

IBM

@server

iSeries

Alapvető rendszerbiztonság és tervezése

V5R3







@server

iSeries

Alapvető rendszerbiztonság és tervezése

*V5R3*

**Megjegyzés**

Mielőtt a jelen leírást és a vonatkozó terméket használná, feltétlenül olvassa el a "Megjegyzések", oldalszám: 129 helyen lévő tájékoztatót.

**ötödik kiadás (2005. augusztus)**

Ez a kiadás a V5R3M0 szintű IBM Operating System/400 (száma: 5722-SS1) termékekre és minden azt követő változatra és módosításra vonatkozik, amíg ez másképpen nincs jelezve. Ez a verzió nem fut minden csökkentett utasításkészletű (RISC) rendszeren és CISC modellen.

© Szerzői jog IBM Corporation 1997, 2005. Minden jog fenntartva

# Tartalom

## Alapvető rendszerbiztonság és tervezése 1

A témakör nyomtatása . . . . .	1
Bevezetés az alapvető rendszerbiztonság témakörébe . . . . .	2
Gyakran ismételt kérdések az alapvető rendszerbiztonságról . . . . .	3
Az alapvető rendszerbiztonság áttekintése . . . . .	4
Beépített rendszerbiztonság . . . . .	4
Alapvető szakkifejezések . . . . .	5
Biztonság a felhasználó szemszögéből . . . . .	5
A rendszer egyéniesítése a felhasználó szemszögéből . . . . .	7
A biztonság és az egyéniesítés rendszereszközei . . . . .	8
Az alapvető rendszerbiztonság tervezésének módszere . . . . .	10
Példa: A JKL Toy Company bemutatása . . . . .	10
A biztonság tervezési folyamatának lépései . . . . .	11
Felhasználói biztonság tervezése . . . . .	12
Fizikai biztonság tervezése . . . . .	12
A rendszeregység fizikai biztonsága . . . . .	13
Példa: JKL Toy Company fizikai biztonság tervezési űrlapja — rendszeregység rész . . . . .	14
Rendszerdokumentációk és tárolási adathordozók fizikai biztonsága . . . . .	14
Példa: JKL Toy Company fizikai biztonság tervezési űrlapja — mentési adathordozók és dokumentációk rész . . . . .	15
Munkaállomások fizikai biztonságának tervezése . . . . .	15
Nyomatatók és nyomtatott listák fizikai biztonsága . . . . .	16
Példa: JKL Toy Company fizikai biztonság tervezési űrlapja — munkaállomás és nyomatató rész . . . . .	17
Biztonsági szabályzat tervezése . . . . .	17
Az alkalmazás biztonságának tervezése . . . . .	18
Alkalmazások leírása . . . . .	18
Példa: JKL Toy Company Alkalmazást leíró űrlap . . . . .	19
Elnevezési szabályok leírása . . . . .	20
Példa: JKL Toy Company Elnevezési szabályok űrlap . . . . .	21
Könyvtári információk leírása . . . . .	21
Példa: JKL Toy Company Könyvtárat leíró űrlap . . . . .	21
Alkalmazási diagram rajzolása . . . . .	22
Átfogó biztonsági stratégia tervezése . . . . .	22
Biztonsági szabályzat írása . . . . .	23
Biztonsági szint kiválasztása . . . . .	24
Bejelentkezést befolyásoló rendszerváltozók kiválasztása . . . . .	25
Bejelentkezési kísérletek számának korlátozása (QMAXSIGN és QMAXSGNACN) . . . . .	25
Felhasználók korlátozása egyidőben egy munkaállomásra . . . . .	27
Inaktív feladatokra vonatkozó rendszerváltozók tervezése . . . . .	27
A biztonsági felelős bejelentkezésének korlátozása . . . . .	29
Jelszavakat befolyásoló rendszerváltozók kiválasztása . . . . .	29

Jelszó élettartam meghatározása . . . . .	30
Jelszavak hosszának meghatározása . . . . .	30
Ismétlődő jelszavak korlátozása . . . . .	31
Rendszer egyéniesítése rendszerváltozókkal . . . . .	31
Példa: JKL Toy Company Biztonsági szabályzat . . . . .	33
Felhasználói csoportok tervezése . . . . .	34
Felhasználói csoportok azonosítása . . . . .	35
Példa: Felhasználói csoportok azonosítása . . . . .	35
A csoportprofil tervezése . . . . .	37
Példa: JKL Toy Company Felhasználói csoportot leíró űrlap . . . . .	38
Bejelentkezést befolyásoló rendszerváltozók kiválasztása . . . . .	39
A felhasználó tevékenységét korlátozó értékek kiválasztása . . . . .	41
A felhasználói környezetet beállító értékek kiválasztása . . . . .	42
Példa: JKL Toy Company Felhasználói csoportot leíró űrlap — második rész . . . . .	43
Egyedi felhasználói profilok tervezése . . . . .	44
Rendszerfunkciókért felelősök meghatározása . . . . .	45
Példa: JKL Toy Company Rendszerfelelőségek űrlapja . . . . .	46
Értékek kiválasztása az egyes felhasználóknak . . . . .	47
Példa: JKL Toy Company Egyedi felhasználói profil űrlap . . . . .	48
Erőforrás biztonság tervezése . . . . .	49
Az erőforrás biztonság céljainak meghatározása . . . . .	50
Példa: JKL Toy Company Biztonsági célkitűzések . . . . .	50
A jogosultság típusainak megértése . . . . .	51
Alkalmazási könyvtárak biztonságának tervezése . . . . .	52
Alkalmazási könyvtárak nyilvános jogosultságának eldöntése . . . . .	53
Példa: JKL Toy Company Könyvtárat leíró űrlap . . . . .	54
Programkönyvtárak nyilvános jogosultságának eldöntése . . . . .	55
Példa: JKL Toy Company Könyvtárat leíró űrlap — nem korlátozó megközelítés . . . . .	55
Példa: JKL Toy Company Könyvtárat leíró űrlap — korlátozó megközelítés . . . . .	56
Könyvtárak és objektumok tulajdonosának meghatározása . . . . .	58
Példa: JKL Toy Company alkalmazásainak tulajdonjoga . . . . .	58
Felhasználói könyvtárak elérésének és tulajdonjogának meghatározása . . . . .	59
Objektumok csoportosítása . . . . .	60
Példa: JKL Toy Company Jogosultsági lista űrlap . . . . .	61
Nyomatatók és nyomtatott listák biztonságának tervezése . . . . .	62
Példa: JKL Toy Company Kimeneti sor és munkaállomás biztonság űrlapja — kimeneti sor . . . . .	63
Munkaállomások biztonságának tervezése . . . . .	64
Példa: JKL Toy Company Kimeneti sor és munkaállomás biztonság űrlapja — munkaállomás . . . . .	65
Erőforrás biztonsági ajánlások összefoglalója . . . . .	65

Alkalmazások telepítésének tervezése . . . . .	66	Nyomatott listák védelme . . . . .	101
Felhasználói profilok és telepítési értékek meghatározása az alkalmazások számára . . . . .	67	Kimeneti sor létrehozása . . . . .	101
Telepítési értékek módosítása az alkalmazások számára . . . . .	67	Nyomatató kimeneti lista hozzárendelése kimeneti sorhoz . . . . .	102
Példa: JKL Toy Company Alkalmazás telepítési űrlap . . . . .	68	Munkaállomások biztonsága . . . . .	103
A felhasználói biztonság beállítása . . . . .	69	Rendszeroperátori üzenetsor elérhetőségének korlátozása. . . . .	104
A teljes környezet beállítása . . . . .	70	Biztonság tesztelése . . . . .	105
Bejelentkezés a rendszerre . . . . .	71	Felhasználói profilok tesztelése . . . . .	105
Megfelelő támogatási szint kiválasztása . . . . .	71	Erőforrás biztonság tesztelése . . . . .	106
Mások bejelentkezésének megakadályozása . . . . .	72	Biztonsági információk módosítása . . . . .	106
Biztonsági rendszerváltozók értékeinek bevitele . . . . .	72	Biztonsági parancsok . . . . .	107
Rendszerváltozók új értékeinek alkalmazása . . . . .	74	Biztonsági információ megtekintése és listázása . . . . .	108
Biztonsági felelős profiljának létrehozása . . . . .	75	Biztonsági információk módosítása . . . . .	108
Biztonsági rendszerváltozók beállítása . . . . .	76	Biztonsági információ törlése . . . . .	108
Biztonsági rendszerváltozók módosítása . . . . .	77	Új felhasználó hozzáadása a rendszerhez . . . . .	109
Egyedi rendszerváltozók módosítása . . . . .	78	Új felhasználói csoport létrehozása . . . . .	109
Biztonság előkészítése az alkalmazások betöltéséhez	79	Felhasználói csoport módosítása . . . . .	109
Tulajdonosi profil létrehozása . . . . .	79	Bővítés új alkalmazással . . . . .	111
Alkalmazás betöltése . . . . .	80	Bővítés új munkaállomással . . . . .	111
Felhasználói csoportok beállítása . . . . .	80	Felhasználói felelősségek módosítása . . . . .	112
Könyvtár létrehozása a felhasználói csoportnak . . . . .	80	Felhasználó eltávolítása a rendszerből . . . . .	112
Jobleírás létrehozása . . . . .	81	Biztonsági információk mentése . . . . .	113
Csoportprofil létrehozása . . . . .	83	Rendszerváltozók mentése . . . . .	113
Egyedi felhasználók beállítása . . . . .	85	Csoport- és felhasználói profilok mentése . . . . .	113
Személyi könyvtár létrehozása . . . . .	86	Jobleírások mentése . . . . .	114
Csoportprofil másolása . . . . .	86	Erőforrás biztonsági információk mentése . . . . .	114
Jelszó beállítása lejáró állapotba . . . . .	88	Alapértelmezett tulajdonosi profil (QDFTOWN) használata . . . . .	115
További felhasználók létrehozása . . . . .	88	Visszaállítás sérült jogosultsági listából . . . . .	115
Felhasználó adatainak módosítása . . . . .	88	Biztonság figyelése . . . . .	116
Felhasználói profilok megjelenítése . . . . .	89	Biztonság figyelésének ellenőrzőlistája . . . . .	116
Erőforrás biztonság beállítása . . . . .	90	Biztonság ellenőrzése . . . . .	117
Tulajdonjog és nyilvános jogosultság beállítása . . . . .	90	Alapvető rendszerbiztonság tervezési űrlapjai . . . . .	117
Tulajdonosi profil létrehozása . . . . .	91	Fizikai biztonság tervezési űrlap . . . . .	118
Könyvtár tulajdonjogának módosítása . . . . .	91	Alkalmazást leíró űrlap . . . . .	119
Alkalmazási objektumok tulajdonjogának beállítása	92	Elnevezési szabályok űrlap . . . . .	119
Work with objects by Owner (WRKOBJOWN) parancs használata . . . . .	92	Könyvtárat leíró űrlap . . . . .	120
Change Object Owner parancs használata . . . . .	93	Rendszerváltozók kiválasztására szolgáló űrlap . . . . .	120
Könyvtár nyilvános jogosultságának beállítása . . . . .	94	Rendszerfelelősségek űrlap . . . . .	122
Nyilvános jogosultság beállítása a könyvtár összes objektumára . . . . .	94	Felhasználói csoportot azonosító űrlap . . . . .	122
Munka ellenőrzése job napló segítségével . . . . .	95	Felhasználói csoportot leíró űrlap . . . . .	123
Új objektumok nyilvános jogosultságainak beállítása	95	Egyedi felhasználói profil űrlapja . . . . .	124
Csoport- és személyi könyvtárak kezelése . . . . .	96	Jogosultsági lista űrlapja . . . . .	125
Jogosultsági lista létrehozása . . . . .	96	Kimeneti sor és munkaállomás biztonság űrlapja . . . . .	125
Objektumok védelme jogosultsági listával . . . . .	97	Alkalmazás telepítési űrlap . . . . .	126
Felhasználók hozzáadása jogosultsági listához . . . . .	97	<b>. Megjegyzések . . . . .</b>	<b>129</b>
Egyedi jogosultságok beállítása . . . . .	98	Védjegyek . . . . .	130
Egyedi jogosultság beállítása könyvtár számára . . . . .	98	A kiadványok letöltésére és kinyomtatására vonatkozó feltételek . . . . .	131
Egyedi jogosultság beállítása objektum számára . . . . .	100		
Jogosultság beállítása egyszerre több objektum számára . . . . .	100		

---

## Alapvető rendszerbiztonság és tervezése

Kiadványunk részletes leírást ad az iSeries biztonság tervezéséről és beállításáról. A témakör a tervezésre helyezi a hangsúlyt, és űrlapokat biztosít, amelyeken megtervezheti és feljegyezheti saját biztonsági döntéseit. Lépésenkénti utasításokat is ad az alapvető rendszerbiztonság beállításához. Mivel a témakör munkafüzet jellegű, szándékában állhat kinyomtatni, hogy többször átnézhesse.

Az iSeries szerver legjobb biztonságának beállítása két fő tevékenységi körből áll: tervezési feladatok és konfigurálási feladatok. Az alábbi tervezési témaköröket nézze át, hogy megbizonyosodjon arról, üzleti igényeit kielégítő biztonságot épít ki.

- A Bevezetés az alapvető rendszerbiztonság témakörébe című rész áttekintést ad az általános biztonsági koncepciókról, és megválaszolja az alapvető rendszerbiztonságról szóló kérdéseket.
- A Felhasználói biztonság tervezése ismerteti a rendszer felhasználóira hatással lévő biztonság tervezését. Ez magában foglalja a fizikai biztonságot, az alkalmazás biztonságot, az átfogó biztonsági stratégiáját és a felhasználói profilokat.
- Az Erőforrás biztonság tervezése leírja, hogyan tervezheti meg a rendszer objektumainak biztonságát, beleértve a könyvtárakat és a bennük lévő objektumokat, a nyomtatókat, a nyomtatott listákat és a munkaállomásokat.


Miután befejezte a tervezési tevékenységeket, átnézheti az alábbi témaköröket, amelyek segítenek a biztonság beállításában a rendszeren:

- A Felhasználói biztonság beállítása részletesen leírja a felhasználói és csoport biztonság beállítását.
- Az Erőforrás biztonság beállítása leírja, hogyan állíthatja be az objektumok tulajdonjogát, a rájuk vonatkozó nyilvános és egyedi jogosultságokat, valamint a nyomtatók és munkaállomások biztonságát.
- A Biztonság tesztelése című rész hasznos információkkal szolgál a biztonság teszteléséről.
- A Biztonsági információk módosítása című rész a felhasználói- és csoportprofilok, valamint az erőforrás biztonság módosításáról és frissítéséről szól.
- A Biztonsági információk mentése tájékoztatást ad a biztonsági információk mentéséről.
- A Biztonság figyelése ellenőrzőlistákat nyújt a biztonság nyomon követésére, valamint tájékoztat az ellenőrzésről.

A témakörökön túlmenően használja fel a tervezési űrlapokat saját stratégiája és biztonsági döntései dokumentálására.

---

## A témakör nyomtatása

A dokumentum PDF változata letölthető megjelenítési vagy nyomtatási céllal. A PDF fájlok megtekintéséhez telepíteni kell az Adobe® Acrobat® Reader programot. A programot letöltheti az Adobe honlapról .

A PDF változat megtekintéséhez vagy letöltéséhez válassza ki az Alapvető rendszerbiztonság és tervezése (950 KB vagy 164 oldal) hivatkozást.

A PDF mentése a munkaállomásra megjelenítés vagy nyomtatás céljából:

1. Nyissa meg a PDF fájlt a böngészőben (kattintson a fenti hivatkozásra).
2. Kattintson a böngésző **Fájl** menüjére.
3. Kattintson a **Mentés másként...** menüpontra.
4. Válassza ki azt a könyvtárat, ahová a PDF fájlt menteni szeretné.
5. Kattintson a **Mentés** gombra.

---

## Bevezetés az alapvető rendszerbiztonság témakörébe

A rendszergazdától a felhasználóig mindenkinek törődnie kell a biztonsággal. A rendszerbiztonság megvédi az iSeries szervert és az érzékeny üzleti adatokat a szándékos és a véletlen biztonsági betörésektől.

A rendszerbiztonságot saját biztonsági környezete és igénye szerint testre szabhatja.

A biztonságot rendszere bejárati ajtajának tekintheti. Alkalmazza a biztonsági elemeket, hogy azok **lezárják** és védjék rendszere információit a jogosulatlan felhasználóktól.

Ugyanakkor a biztonsági elemek használata **megnyitja** az utat a rendszer rugalmassá és egyedivé tételéhez minden jogosult felhasználó számára.

Egy jó biztonsági terv megvédheti a rendszert, de nem tudja garantálni a berendezések és az információ épségét. Meg kell osztani a felelősséget több alkalmazott között azért, hogy ne csak egy személy irányítsa kizárólagosan a rendszert.

Kiadványunk segítségével lépésről-lépésre közelítheti meg a tervezést és az alapvető rendszerbiztonság beállítását. Ez a témakör megpróbálja kihangsúlyozni a rendszerbiztonság tervezésének fontosságát, amihez tervezési űrlapokat biztosít, hogy saját biztonsági döntéseit feljegyezhesse. A könnyebb döntési lehetőség érdekében számos üzleti példát talál a könyvben, amelynek biztonságát is megtervezzük.

Jó és átfogó tervezés szükséges ahhoz, hogy sikeresen teljesítse a rendszerbiztonság követelményeit. Nézze át az alábbi témaköröket, ahol tanulmányozhatja az alapvető biztonsági igényeket és a tervezés fontosságát.

- Gyakran ismételt kérdések az alapvető rendszerbiztonságról
- Az alapvető rendszerbiztonság áttekintése
- Az alapvető rendszerbiztonság tervezésének módszere

Ugyancsak jó tervvel kell rendelkeznie a rendszer összes információjának mentésére és visszaállítására is. Továbbá, ugyancsak tervvel kell rendelkeznie a berendezés cseréjére ill. pótlására katasztrófa esetén. Megfelelő mentési terv elkészítéséről további információt talál az Információs központ Mentés és helyreállítás című témakörében.

### Részletes tervezési információk a felhasználói biztonsághoz

A felhasználói biztonság tervezésének módszereit a következő témakörök ismertetik:

- Alkalmazások biztonságának tervezése
- Biztonsági stratégia tervezése
- Felhasználói csoportok tervezése
- Egyedi felhasználói profilok tervezése

### Részletes tervezési információk az erőforrás biztonsághoz

A felhasználók erőforrás biztonságának tervezéséhez a következő témakörök nyújtanak szisztematikus megközelítést.

- A jogosultság típusainak megértése
- Alkalmazási könyvtárak biztonságának tervezése
- Könyvtárak és objektumok tulajdonosának meghatározása
- Objektumok csoportosítása
- Nyomtatott listák védelme
- Munkaállomások védelme
- Alkalmazások telepítésének tervezése

### Nyomtatható tervezési űrlapok



A kiadvány nyomtatható űrlapokat ad közre, amely lehetővé teszi, hogy feljegyezze saját biztonsági döntéseit. A teljes kiadványt kinyomtathatja PDF-ként, illetve az egyes tervezési űrlapokat a böngésző nyomtatási funkciójával.

### Az alapvető rendszerbiztonság lépésenkénti beállításának utasításai

Miután befejezte a biztonság tervezését, a könyv lépéseket tartalmaz a biztonsági terv gyakorlati megvalósítására is. A következő témakörök nyújtanak segítséget a rendszerbiztonság beállításához.

- Felhasználói biztonság beállítása
- Erőforrás biztonság beállítása

## Gyakran ismételt kérdések az alapvető rendszerbiztonságról

Ha átnézi a biztonságról gyakran feltett kérdésekre adott válaszokat, jobban megértheti a biztonság fontosságát a rendszeren.

### Miért fontos a biztonság?

A rendszeren tárolt információhalmaz az egyik legfontosabb üzleti vagyont. Három fontos szempontot kell szem előtt tartani, mikor az információ-vagyon védelmének mikéntjéről gondolkodik:

- **Bizalmasság:** A jó biztonsági rendszabályok megelőzik a bizalmas és titkos információk feltárását és megtekintését.
- **Sértetlenség:** A rendszer bizonyos kiterjedése esetén az információ pontosságát csak jól megtervezett biztonsági rendszer garantálhatja. Megfelelő biztonsággal megelőzheti az adatok jogosulatlan megváltoztatását vagy törlését.
- **Rendelkezésre állás:** Ha valaki véletlenül vagy szándékosan megrongálja az adatokat a rendszeren, nem fér hozzá ezekhez az erőforrásokhoz, míg helyre nem állítja őket. A jó biztonsági rendszer megakadályozhatja az ilyen jellegű meghibásodásokat.

Mikor az emberek a rendszer biztonságáról gondolkodnak, gyakran csak a cégen kívüli személyek (mint például versenytársak) elleni védelemre gondolnak. Valójában, védelem a kíváncsiság és a rendszerbalesetek ellen - amelyeket a felhasználók okozhatnak - lehet a legnagyobb nyeresége egy jól megtervezett biztonsági rendszernek. Egy rendszerben, ahol a biztonság nincs jól kiépítve, a felhasználó szándékosan törölhet fontos fájlt. Jól megtervezett biztonsági rendszerrel az ilyen balesetek elkerülhetők.

Tegye fel magának az alábbi kérdéseket, amikor meg akarja határozni a szükséges biztonság mértékét:

- Mennyire fontos a számítógép (és az azon tárolt adatok) cége üzletmenete szempontjából?
- Van-e a cégének olyan szabályzata, amely a biztonság bizonyos fokát megköveteli?
- Megköveteli-e a cég felügyeleti szerve a számítógépen tárolt adatok biztonságának valamilyen szintjét?
- Van-e szüksége a biztonság valamilyen fokára a közeljövőben?

### Miért egyéniesítse a rendszert?

Az iSeries a felhasználók széles tartományával rendelkezhet. Egy kis rendszer három - öt felhasználót takarhat, akik kevés alkalmazást futtatnak. Egy nagy rendszer több ezer felhasználót is takarhat nagy kommunikációs hálózaton futó sok alkalmazással.

Az iSeries kivitele rengeteg rugalmasságot biztosít, hogy a rendszer hozzáidomuljon a felhasználók és a helyzetek széles variációjához. Így alkalma van meghatározni és megváltoztatni sok dolgot ahhoz, hogy hogyan is nézzen ki a rendszer a felhasználó számára és hogyan hajtsa végre a feladatokat.

Mikor a rendszer először megérkezik, feltehetően nem kell és nem akar túl sok egyéniesítést realizálni. Az IBM számos paraméter esetében kezdeti beállítással, másnéven **alapértelmezésekkel** szállítja a gépet. Ezek az alapértelmezések a gyakorlat szerint új üzembe helyezés esetén a rendszer legkedvezőbb beállítását jelentik.

**Megjegyzés:** Az összes új rendszert az alapértelmezett **40-es** biztonsági szinttel szállítjuk. Ez a biztonsági szint garantálja azt, hogy csak a megadott felhasználók használhatják a rendszert. Megakadályozza, hogy azok a programok, amelyek kijátszhatják a biztonságot, esetleg kockázatot jelentsenek az integritás szempontjából.

Mégis, ha a rendszert egyéniesíti, egyszerűbbé teheti azt és több hatékony eszközt adhat felhasználóinak. Például, beállíthatja, hogy a felhasználó az általa kívánt képernyőt kapja meg minden bejelentkezéskor. Ugyanígy biztosíthatja, hogy minden felhasználó nyomtatott listája a megfelelő nyomtatón jelenjen meg. Felhasználói nagyobb bizalommal lesznek a rendszer iránt, ha az egyéniesítésnek köszönhetően magukénak látják és érzik azt.

## **Ki legyen a felelős?**

Különböző cégek különböző módon közelítik meg a biztonságot. Néhány esetben a programozók felelősek a biztonság összes aspektusáért. Más esetekben a rendszert kezelő személy is felelős érte. Ha nem biztos benne, hogy kihez és hogyan rendelje a felelősséget a cégen belül, javasoljuk az alábbi megközelítést:

- Az erőforrás biztonság tervezésének módszere attól függ, hogy a vállalat vásárolja az alkalmazásokat vagy maga fejleszti ki őket. Ha az alkalmazás saját fejlesztésű, már a fejlesztés időszakában tisztázza a szükséges erőforrás biztonságot. Ha vásárolt alkalmazással áll szemben, értse meg hogyan működik és éljen az alkalmazás adta lehetőségekkel. Mindkét esetben a tervezőknek figyelembe kell venniük, hogy a biztonság a konstrukció elengedhetetlen része.
- A biztonsági igények összeállítása a biztonsági felelős feladata. Ő határozza meg a felhasználók körét és hozzáférésüket a rendszerhez. A biztonsági felelős kötelezettsége gyakran másra is kiterjed, úgymint az információ mentésére és visszaállítására.
- A biztonsági felelős feladata lehet a rendszer bizonyos mértékű egyéniesítése is, különösen azóta, hogy a biztonsági elemek fontos szerepet játszanak az egyéniesítésben.

Azonban nincs jelentősége, hogy milyen elv alapján rendeli a felelősséget, egyszerűen **kommunikálni kell a biztonsági szabályzatot**. El kell mondani mindenkinek, de még előnyösebb írásban közreadni, hogy a számítógépen található információ fontos vagyton. Ezt az információt ugyanúgy védeni kell, mint ahogy a cég más vagyontárgyait. Tekintse meg a "Példa: JKL Toy Company biztonsági szabályzatát", amely mintául szolgál a biztonsági szabályzat elkészítéséhez.

Most, hogy megértette a biztonság szükségességét a rendszeren, szándékában állhat a rendszerbiztonsági szempontok áttekintése.

## **Az alapvető rendszerbiztonság áttekintése**

Az eredményes tervezéshez meg kell ismernie a rendszer által biztosított és használni kívánt eszközöket. Tudnia kell, hogy hogyan fognak a felhasználók és az általuk elérhető rendszerfunkciók együtt dolgozni.

A következő témakörök a biztonság és az egyéniesítés fontos részeit taglalják és bemutatják, hogyan férnek meg egymás mellett. A témakörök áttekintést szándékoznak adni a tervezés megkezdése előtt. Az összes bemutatásra került koncepció még a tervezési eljárásnál feltételezett mértéknél is részletesebben kerül ebben a részben ismertetésre.

- Beépített rendszerbiztonság
- Alapvető szakkifejezések
- Biztonság a felhasználó szemszögéből
- A biztonság és az egyéniesítés rendszereszközei

## **Beépített rendszerbiztonság**

A biztonság összes rendszeroldali elemét magába foglalja a rendszer. Tehát nem különálló termékek, amit meg kell venni. Az integráltságra törekvés jár néhány előnnyel:

- A biztonság konzisztens az operációs rendszer többi részével. Ugyanazokat a képernyőket, parancsokat és terminológiát használja.
- A felhasználók nem tudják megkerülni a biztonságot, mert az nem egy különálló része a szoftvernek.

- Megfelelően megtervezett biztonság csak minimálisan érinti a teljesítményt.
- A biztonság mindig lépést tart az új szoftver fejlesztésekkel. Amikor új funkciók válnak a rendszer részévé, ezzel egyidőben az ezen funkciókra vonatkozó biztonsági elemek is megtalálhatók.

Az iSeries 40-es biztonsági szinttel érkezik, ami megakadályozza, hogy jogosulatlan felhasználók bejelentkezzenek a rendszerre. Megakadályozza, hogy azok a programok, amelyek kijátszhatják a biztonságot, esetleg kockázatot jelentsenek az integritás szempontjából. Azonban, testre szabhat bizonyos biztonsági beállításokat, illetve megváltoztathatja a biztonsági szinteket. A biztonsági szintek leírását a "Biztonsági szint kiválasztása" című rész tartalmazza.

Most, hogy már jobban megértette a beépített biztonság működését, szándékában állhat megismerkedni az iSeries általános szakkifejezéseivel.

## Alapvető szakkifejezések

Az alábbi szakkifejezések nagyon fontosak az iSeries biztonság megismerése és megértése szempontjából:

### objektum

Az objektum a rendszer olyan névvel rendelkező egysége, amely manipulálható. Az objektumra legáltalánosabb példák a fájlok és a programok. Más típusú objektumok a parancsok, sorok(queues), könyvtárak és mappák. Az objektumok a rendszerben objektumnévvel, objektumtípussal és a tartózkodási helyüket jelentő könyvtárnévvel vannak azonosítva. A rendszerben minden objektumra kiterjeszhető a biztonság.

### könyvtár

A könyvtár az objektumok speciális típusa, amely más objektumokat fog össze egy csoportba. A rendszerben nagyon sok objektum könyvtárban található.

### katalógus

A katalógus az objektumok más módon összerendelt csoportját tartalmazza. Az objektum tartózkodhat egy katalógusban. A katalógus tartózkodhat egy másik katalógusban, formálva ezzel egy hierarchikus struktúrát.

Most, hogy már jobban megismerte az iSeries biztonság alapvető kifejezéseit, szándékában állhat áttekinteni, hogyan látja a felhasználó a biztonságot.

## Biztonság a felhasználó szemszögéből

A felhasználó szemszögéből nézve a biztonság hatással van arra, hogyan tudják elvégezni feladataikat a rendszeren. Ebbe beleértendő az is, hogyan tudnak együttműködni a rendszerrel a feladataik elvégzése érdekében. Nagyon fontos, hogy a felhasználó milyennek látja a biztonságot. Például, a jelszavak 5 naponkénti lejárása idegesítené őket, és zavarná feladataik elvégzésében. Másrészt, a túl laza jelszó politika biztonsági problémákat okozna.

A rendszer megfelelő biztonsága érdekében a biztonságot ossza fel jellemző részekre, amelyeket tervezhet, kezelhet és ellenőrizhet. A felhasználó szemszögéből több részre oszthatja a biztonságot:

### A rendszer fizikai elérése

A fizikai biztonság védi a rendszeregységet, az összes rendszereszközt, valamint a biztonsági mentés adathordozóit (mint például hajlékonylemezek, szalagok vagy CD-k) a véletlenszerű vagy szándékos elvesztéstől vagy sérüléstől.

A legnagyobb mértékben biztosra vehető, hogy a rendszer fizikai biztonsága a külső elemektől függ. Azonban, a rendszer kulcszárral vagy elektronikus kulccsal felszerelve érkezik, ami megelőzi a rendszeregység funkcióinak jogosulatlan használatát.

A "Fizikai biztonság tervezése" című témakör részletes tájékoztatással szolgál a rendszer fizikai biztonságának tervezéséről.

### Felhasználók bejelentkezésének módja

A bejelentkezési biztonság megakadályozza, hogy nem definiált felhasználó bejelentkezhesen a rendszerbe. A bejelentkezés sorrendjének megfelelően, a személynek a felhasználói azonosító és a jelszó érvényes kombinációját kell megadnia.

Mind a rendszerváltozókat, mind az egyedi felhasználói profilokat használhatja azért, hogy meggyőződjön róla, nem sértették-e meg a bejelentkezési biztonságot. Például, kérheti a jelszók szabályos időközönkénti megváltoztatását. Ugyancsak megelőzheti a könnyen kitalálható jelszók használatát.

### **A felhasználóknak engedélyezett tevékenységek**

A rendszerbiztonság és egyéniesítés fontos szerepét jelenti annak meghatározása, hogy mit tehetnek a felhasználók. A biztonság perspektívájából nézve ez gyakran **korlátozó** funkció, úgymint megelőzni azt, hogy az emberek bizonyos nem nekik szánt információt is lássanak. A rendszer egyéniesítés szempontjából ugyanakkor ez egy **feljogosító** funkció. A megfelelően egyéniesített rendszer lehetővé teszi az emberek számára, hogy munkájukat jól végezhessék el, egyúttal kiküszöbölve a szükségtelen feladatokat és információkat.

Néhány módszer annak meghatározására - mit tehetnek a felhasználók - a biztonsági felelős dolga, míg mások a programozók felelőssége. Ez a cikk elsősorban azokra a dolgokra koncentrál, amit a biztonsági felelős tesz. Az összes

rendszerváltozó leírását megtalálja a *Biztonsági szakkönyv* (SC22-0282)  könyv 3. fejezetében (Biztonsági rendszerváltozók).

Paraméterek állnak rendelkezésre az egyedi felhasználói profilokban, a jobleírásokban és az osztályokban arra, hogy a felhasználók mit tehetnek a rendszeren. Az alábbi felsorolás röviden ismerteti a rendelkezésre álló technikákat:

### **Felhasználók korlátozása kevés funkcióhoz**

A felhasználói profil segítségével korlátozhatja a felhasználót úgy, hogy csak megadott programhoz, menühöz vagy menükészlethez, kevés rendszerparancshoz legyen hozzáférése. Általában a biztonsági felelős hozza létre és irányítja a felhasználói profilokat.

### **Rendszerfunkciók korlátozása**

A rendszerfunkciók lehetővé teszik az információk mentését és visszaállítását, a nyomtatandó anyagok kezelését, valamint új felhasználók létrehozását. Minden felhasználói profil megadja azokat a legáltalánosabb rendszerfunkciókat, amelyeket a felhasználó végrehajthat.

Az iSeries rendszeren a rendszerfunkciók vezérlőnyelvi (CL) parancsokkal és alkalmazásprogramozási csatolóval (API) kerülnek végrehajtásra. Mivel minden parancs és API egy-egy objektum, felhasználhatja az objektum jogosultságokat annak vezérlésére, hogy ki használhatja őket és ezáltal a rendszerfunkciókat.

### **Fájlok és programok használatának meghatározása**


Az erőforrás biztonság lehetőséget biztosít a rendszerben minden objektum használatának vezérléséhez. Bármely objektum számára megadható, hogy ki használja és hogyan tudják őt használni. Például megadható, hogy egy felhasználó csak láthatja az adatokat a fájlban, másik felhasználó megváltoztathatja azokat, míg a harmadik megváltoztathatja az adatokat vagy törölheti az egész fájlt.

### **Rendszerforrásokkal való visszaélés megelőzése**

A rendszer feldolgozási teljesítménye ugyanolyan fontossá válhat az üzletmenet szempontjából, mint a rendszer által tárolt adatok. A biztonsági felelős segítségével meggyőződhet arról, hogy a felhasználók nem élnek-e vissza a rendszer erőforrásaival azáltal, hogy munkáikat magas prioritással futtatják, saját riportjaikat nyomtatják ki először illetve túl sok lemeztároló helyet használnak fel.

### **A rendszer kommunikálása más számítógépekkel**

További biztonsági vizsgálatok szükségesek, ha a rendszere más számítógépekkel vagy programozható munkaállomásokkal kommunikál. Ha nem rendelkezik megfelelő biztonsági kontrollal, akkor valaki a hálózat másik számítógépéről elindíthat egy munkát vagy elérhet információt az Ön számítógépén a bejelentkezési procedúra megkerülésével.

Mind a rendszerváltozókat, mind a hálózati attribútumokat használhatja a távoli munkák, távoli adatelérés, távoli PC-elérés engedélyezésére. Ha engedélyezi a távoli elérést, módjában áll meghatározni az érvényrejutó biztonságot. Az összes rendszerváltozó leírását megtalálja a *Biztonsági szakkönyv* (SC22-0282) 

könyv 3. fejezetében (Biztonsági rendszerváltozók). **Biztonsági információk mentése**


Rendszeres időközönként menteni kell a rendszeren lévő információkat. A rendszer adatainak mentésén túlmenően a biztonsági információk mentése is szükséges. Baleset vagy katasztrófa esetén vissza kell állítani a rendszerfelhasználók adatait, a jogosultsági információkat és a tényleges adatokat.

A "Biztonsági információk mentése" című témakör elmagyarázza a biztonsági információk mentését. Az Információs központ Mentés és helyreállítás című témaköre részletes tájékoztatást ad a biztonsági adatok mentéséről és helyreállításáról.

### **Biztonsági terv figyelése**

A rendszer biztosít néhány eszközt a biztonság hatékonyságának figyelésére:

- Üzeneteket küld a rendszeroperátornak a biztonság megsértése esetén.
- Számátalan, biztonsággal kapcsolatos tranzakció jegyezhető fel egy speciális ellenőrzési naplóban.

A "Biztonság figyelése" című rész tárgyalja az eszközök általános használatát. A biztonság ellenőrzéséről további részleteket talál a *Biztonsági szakkönyv* (SC22-0282) könyv 9. fejezetében (Biztonság ellenőrzése a rendszeren). 

A rendszer egyéniesítésének jobb megértéséhez, először ismerje meg a testre szabás felhasználói szempontjait.

**A rendszer egyéniesítése a felhasználó szemszögéből:** A rendszer egyéniesítésével segíthet felhasználóinak, hogy könnyebben elvégezhessék napi munkájukat. Akkor egyéniesítheti legjobban a rendszert, ha arra gondol, hogy mit kell tenniük a felhasználóknak munkájuk sikeres elvégzéséhez. A menük és alkalmazások megjelenítéséhez többféleképpen is egyéniesítheti a rendszert:

### **A felhasználó által látni kívánt dolgok megjelenítése**

Többségünk rendet tart az asztalon és az irodában, így a legfontosabb dolgokat könnyedén elérjük. Ugyanezt az elvet kell biztosítanunk a rendszerbe belépő felhasználó számára is. A rendszerbe történő bejelentkezést követően a felhasználónak az általa leggyakrabban használt menüt vagy képernyőt kell biztosítani. Könnyedén megtervezheti úgy a felhasználói profilt, hogy valóban ez történjen meg.

### **Szükségtelen dolgok eltávolítása**

A legtöbb rendszer számtalan különböző alkalmazást tartalmaz. A felhasználók többsége azonban csak a munkájához nélkülözhetetlen alkalmazásokat szeretné látni. Korlátozva az elérhető rendszerfunkciókat könnyebbé válik munkájuk. A megfelelő felhasználói profilokkal, jobbleírásokkal, menükkal a rendszer egyedi képét adhatja meg mindegyik felhasználónak.

### **Küldés a megfelelő helyre**

Nagyon hasznos, ha a felhasználónak nem kell aggódnia azért, hogy kinyomtatásra szánt riportjai hogyan kerülnek a megfelelő nyomtatóra, illetve kötegelt munkái hogyan futnak. A rendszerváltozók, felhasználói profilok, jobbleírások szabályozzák ezeket az eseményeket.

### **Támogatás biztosítása**

Ne lepődjön meg, ha a rendszer sikeres egyéniesítése ellenére is lesz felhasználó, aki kérdezi: "Hol az én riportom?" vagy "Fut még az én munkám?" Az **Operational Assistant** képernyők egyszerű kapcsolatot biztosítanak a

rendszerfunkciókhoz, amelyek segítenek a felhasználóknak kérdéseik megválaszolásában. A rendszerképernyők különböző szintje biztosítható a **támogatási szint** beállításával a felhasználók számára, technikai gyakorlatosságukkal összhangban. Mikor a rendszer megérkezik, az Operational Assistant képernyők minden felhasználó számára automatikusan rendelkezésre állnak. Azonban, az alkalmazások felépítése megkövetelheti az Operational Assistant menük felhasználói elérésének módosítását.

Az iSeries esetén rendelkezésre állnak olyan rendszereszközök, amelyek lehetővé teszik a rendszerbiztonság testre szabását úgy, hogy az erőforrások védve legyenek, miközben a felhasználók elérik őket.

## A biztonság és az egyéniesítés rendszereszközei

Az eredményes tervezéshez meg kell ismernie a rendszer által biztosított eszközök és a biztonsági célok összefüggéseit. A rendszereszközökkel egyéniesítheti a biztonságot a rendszeren.

### Biztonsági szint

Az IBM az összes új iSeries rendszert 40-es biztonsági szinttel szállítja. A 40-es biztonsági szint jelszavas és erőforrásbiztonságot, valamint sértetlenséget nyújt. Ha meg akarja változtatni az aktív biztonsági szintet a rendszeren, a QSECURITY rendszerváltozót kell megváltoztatni. Azonban az IBM erősen javasolja, hogy hagyja változatlanul a beállított 40-es biztonsági szintet. A biztonsági szint módosításához a felhasználónak \*SECOFR felhasználói osztályban kell lennie vagy \*ALLOBJ és \*SECADM egyedi jogosultsággal kell rendelkeznie.

A rendszer négy biztonsági szintet ajánl fel az alábbi táblázatnak megfelelően:

1. táblázat: Biztonsági szintek a rendszeren

Biztonsági szint	Leírás
20-as biztonsági szint	Csak jelszavas biztonságot nyújt.
30-as biztonsági szint	Jelszavas és erőforrás biztonságot nyújt.
40-es biztonsági szint	Jelszavas és erőforrás biztonságot, valamint sértetlenséget biztosít.
50-es biztonsági szint	Jelszavas és erőforrás biztonságot, valamint továbbfejlesztett sértetlenséget biztosít.

A "Biztonsági szint kiválasztása" című témakör részletekkel szolgál arról, hogy melyik biztonsági szint felel meg legjobban igényeinek.

### Rendszerváltozók

A rendszerváltozók beállításával vezérelheti, hogy az operációs rendszer bizonyos elemei hogyan dolgozzanak az iSeries rendszeren. Tekintse úgy, mintha egy cég belső utasítása lenne. A rendszerváltozók mindenkire érvényesek mindaddig, míg valami további megadás (például: felhasználói profil) nem hatálytalanítja.

A rendszerváltozók meghatároznak olyan dolgokat, mint például az elsődleges nyomtatót, a dátumot, a jelszavak cseréjének gyakoriságát.

### Hálózati tulajdonságok

A hálózati tulajdonságok néhány olyan jellemző meghatározására szolgálnak, amelyek befolyásolják a rendszer kommunikációját más számítógépekkel, beleértve a személyi számítógépeket is. A hálózati tulajdonságok érvényessége kiterjed az egész rendszerre.

### Csoportprofilok

A csoportprofil a felhasználók egy csoportját definiálja. Tekintse a csoportprofilat úgy, mintha egy osztály belső utasítása lenne. A csoportprofilokat használhatja mintaként az egyedi felhasználói profilok előállításához. Ugyancsak

használhatja a csoportprofilokat annak megadására is, hogy a csoport tagjai hogyan érhetnek el objektumokat a rendszerben. A csoportprofilokról a "Felhasználói csoportok tervezése" című részben olvashat.

### Felhasználói profilok

A felhasználói profil a rendszer egyik leghathatósabb és legsokoldalúbb objektuma. Olyan dolgokat tartalmaz, mint például a jelszót, vagy hogy milyen menüt lásson a felhasználó a bejelentkezés után. A felhasználói profil megadja, hogy mit csinálhat és mit nem a felhasználó a rendszerben. Meghatározza a rendszer felhasználó-specifikus képét. A "Felhasználói biztonság tervezése" című témakör javaslatokkal szolgál a felhasználói profilok tervezéséhez.

### Jobleírások

A jobleírás a rendszerváltozókkal és a felhasználói profilokkal együttműködve meghatározza, hogy a rendszer hogyan dolgozza fel a felhasználói jobokat. A jobleírás összeállítja a felhasználó kezdeti könyvtárlistáját, ami meghatározza, hogy mely könyvtárakat éri el automatikusan a felhasználó a bejelentkezést követően.

### Erőforrás biztonság

A biztonsági felelős védi az erőforrásokat (objektumokat) a rendszeren azáltal, hogy meghatározza ki jogosult használatukra és hogyan érhetők el. A biztonsági felelős beállíthatja az objektumjogosultságokat az egyedi objektumokra is, vagy az objektumok egy csoportjára (jogosultsági listák). A fájlok, programok, könyvtárak a legáltalánosabb- és egyben védelmet igénylő objektumok, de a rendszer megengedi, hogy beállítson objektumjogosultságokat a rendszer bármely objektumára.

Egyszerűen és hatékonyan kezelheti az erőforrás biztonságot, ha általános és előremutató tervet készít. Ha az erőforrás biztonság sémájának összeállítása előzetes tervezés nélkül történik, bonyolulttá és alacsony hatékonyságúvá válhat. Az "Erőforrás biztonság tervezése" című rész leírja az erőforrás biztonság tervezésének útját.

A rendszer ajánl néhány olyan eszközt, ami támogatja a megfelelő erőforrás biztonsági terv összeállítását:

- **Csoportprofilok:** Összevonhatja a hasonló felhasználókat egyetlen csoportprofil alá. Azután a felhasználói csoport minden tagja ugyanazon a jogosultságon osztozik az objektumokra vonatkozóan.
- **Jogosultsági listák:** A hasonló biztonsági követelményekkel bíró objektumokat egyetlen listára csoportosíthatja. Azután könnyebben adhat jogosultságot a listához, mint az egyedi objektumokhoz.
- **Objektum tulajdonjoga:** A rendszeren minden objektumnak van tulajdonosa. Csoportprofilok és egyedi felhasználók birtokolhatnak objektumokat. A megfelelő objektum-tulajdonos hozzárendelések segítik az (1) alkalmazások kezelését és a (2) felelősség delegálását az információ biztonsága érdekében.
- **Elsődleges csoport:** Megadhat elsődleges csoportjogosultságot egy objektumra. A rendszer tárolja az elsődleges csoportjogosultságot az objektummal. Az elsődleges csoportjogosultság használata egyszerűsítheti a jogosultság kezelését és növeli a jogosultság ellenőrzésének teljesítményét.
- **Könyvtár jogosultság:** A védelmet igénylő fájlokat és programokat berakhatja egy könyvtárba, és korlátozhatja a kérdéses könyvtár elérését. Ez gyakran egyszerűbb, mint korlátozott hozzáférést rendelni mindegyik objektumhoz külön-külön. A fontos objektumok védelme érdekében védheti mind az objektumot, mind a könyvtárat.
- **Objektum jogosultság:** Azokban az esetekben, mikor a korlátozott könyvtárelérés nem eléggé biztonságos, meghatározhat az egyedi objektumok - például fájlok - használatára vonatkozóan korlátozott jogosultságot.
- **Nyilvános jogosultság:** Minden egyes objektum esetén meghatározhatja az elérhetőség típusát minden olyan felhasználó számára, aki nem rendelkezik semmilyen más jogosultsággal az adott objektumhoz. A nyilvános jogosultság a nem bizalmas objektumok hathatós védelmére szolgál, miközben jó rendszerteljesítményt nyújt.
- **Katalógus jogosultság:** A katalógus jogosultságot ugyanolyan módon használhatja, mint a könyvtár jogosultságot. Könnyebb összerakni az objektumok egy csoportját egy katalógusba és levédeni azt, mint egyedileg az objektumokat.
- **Jogosultság őrző:** Amikor töröl egy objektumot, törli az objektumra vonatkozó jogosultsági információkat is. A jogosultság őrzői megtarthatják a jogosultsági információkat a program által megadott fájlok esetében, amelyeket az alkalmazás töröl, majd újra létrehoz. A jogosultság őrzőkkel segítheti a System/36 rendszerről történő áttelepítést.

## Biztonsági eszközök

A biztonsági eszközökkel kezelheti és figyelheti a biztonsági környezetet az iSeries rendszeren. A felhasználói profil elősegíti a következőket:

- Kitalálhatja, melyik felhasználói profiloknak van alapértelmezett jelszavuk.
- Ütmezheti a felhasználói profilokat, hogy a nap vagy hét bizonyos időszakában ne legyenek használhatók.
- Ütmezheti a törlendő felhasználói profilokat, mikor az alkalmazottak eltávoznak a cégtől.
- Kitalálhatja, hogy melyik felhasználói profilok rendelkeznek speciális jogosultságokkal.
- Kitalálhatja, hogy ki öröklí az objektumokra vonatkozó jogosultságot a rendszeren.

Az objektum biztonsági eszközökkel nyomon követheti a bizalmas objektumokhoz tartozó nyilvános és magán jogosultságokat. A riportok rendszeresen (például havonta) kinyomtathatóak, ami elősegíti, hogy biztonsági erőfeszítéseivel az új fejleményekre koncentráljon. Futtathatja úgy is a riportokat, hogy csak az előző futtatás óta bekövetkezett változásokat jelenítse meg.

További eszközök a figyeléshez:

- Trigger programok
- Biztonsághoz kapcsolódó értékek a kommunikációs bejegyzésekben, alrendszer leírásokban, kimenő sorokban, job várakozási sorokban és leírásokban.
- Megváltozott vagy megváltoztatott programok

Most, hogy megértette a rendszerbiztonság fontosságát, átnézheti a témakörben példaként használt tervezési módszer leírását.

## Az alapvető rendszerbiztonság tervezésének módszere

A témakör kívülről befelé haladva, az általánosságtól a specifikusság irányába menve közelíti meg és tárgyalja a tervezést. Például, a felhasználói profil tervezésénél először arra kell gondolnia, amit a felhasználónak látnia kellene (külső), azután arra, hogyan érzük el mindezt (belső). Először a rendszerváltozókat és a csoportprofilokat tervezzük meg (általános), majd az egyedi felhasználói kivételeket (specifikus). A Felhasználói biztonság tervezése témakörben található tervezési lépéseket a megadott sorrendben hajtjuk végre. A leírások logikailag egymásra épülve ismertetik, hogyan tervezze meg a rendszer használatát, hogyan tegye biztonságossá és egyedivé.

Amikor eltervezi és kivitelezzi a rendszerbiztonságot, az alapokról indulva építkeznek, kezdve a biztonság legalapvetőbb formáival, folytatva a bonyolultabb biztonsági kérdésekkel. Kezdve a rendszer fizikai biztonságával, haladva az alkalmazások és a rendszerváltozók leírása felé. Végül, a felhasználók és a rendszer objektumainak biztonságával kell törődni.

A tervezési témakör egészen példákat mutatunk be egy kitalált vállalat - a JKL Toys - felhasználásával a fent vázolt megközelítési módra. A "JKL Toy Company: A minta vállalat bemutatása" című rész ismerteti a minta vállalatunkat, amelyre mindig visszatérünk a tervezési témakör során.

A "Tervezési folyamat lépései" című témakör rövid leírást ad az egyes lépésekről és azok egymáshoz kapcsolódásáról.

### Példa: A JKL Toy Company bemutatása

A példák könnyebbé teszik mind a magyarázatokat mind a megértést. Ez a témakör a JKL Toy Company nevű vállalatot hozza példaként. A JKL Toy Company kicsi, de gyorsan növekvő, játékgyártó cég, ahol a biztonságot kívánják kialakítani egy iSeries rendszeren. A vállalat elnöke - John Smith - azt akarja, hogy az új iSeries rendszer könnyítsen a JKL Toy Company robbanásszerű növekedésének terhein.

Sharon Jones a cég főkönyvelője kapta meg az elnöktől a biztonsági felelős és a rendszeradminisztrátor feladatkörét. Neki kell zökkenőmentesen lebonyolítani a rendszer teljes telepítését, beleértve a biztonságot is. Sharon hisz a tervezés fontosságában. A cég ma még kicsi és az alkalmazottak többsége hozzáfér az információk túlnyomó részéhez. De Sharon tudja, hogy ez változni fog a növekedéssel összhangban. Már alig várja a feladat korrekt megoldását.



Kezdetben a JKL Toy Company a következő alkalmazások futtatását tervezi a rendszerén: Vevő megrendelések, Készletgazdálkodás, Szerződések és árak, Vevő tartozások. Amint olvassa ezt a tervezési témakört egyre többet fog tudni arról, hogyan kezeli a JKL Toy Company a biztonságot.

A "Tervezési folyamat lépései" című témakör elmagyarázza az egyes lépéseket, amelyeket követni kell a rendszerbiztonság tervezésekor.

## A biztonság tervezési folyamatának lépései

A következő táblázat bemutatja a tervezési folyamat lépéseit és más folyamatokhoz való kapcsolatukat.

2. táblázat: A biztonság tervezési folyamatának lépései

Lépés	Tevékenység ebben a lépésben	Lépések kapcsolódása egymáshoz
Fizikai biztonság tervezése	Ismerteti a rendszeregység, a berendezések és a mentési média védelmének megtervezését.	Ezen információk többsége független a többi eljárástól. A fizikai biztonság tervezési információit nem kell ugyan megadni a rendszeren, azonban bizonyos információkra szükség lesz a rendszerváltozók és az erőforrás biztonság tervezésekor.
Alkalmazások tervezése	Leírja az összes alkalmazás célját, fő menüit és a könyvtárakat.	Biztosítja az alapokat a tervezési folyamat további lépéseire és egyéb döntéseire. Nem kell megadni ezeket az információkat a rendszeren.
Átfogó megközelítés tervezése	Eldönti, milyen módon közelít a biztonsághoz. Kiválasztja a rendszerváltozókat a döntés támogatásához.	Az alkalmazás tervezési információk segítségével határozhatja meg átfogó megközelítésének milyenségét. A kiválasztott rendszerváltozók hatással vannak arra, hogyan tervezzék meg a felhasználói és a csoportprofilokat.
Felhasználói csoportok tervezése	Eldönti, hogyan szervezi felhasználóit csoportokba. Eldönti az egyes csoportok jellemzőit és a rendszerben történő meghatározásukat.	Az alkalmazás leírás segítségével határozhatja meg a csoportokat a rendszeren. A megadott felhasználói csoportok hatással vannak az egyedi felhasználók tervezésére a rendszeren.
Egyedi felhasználói profilok tervezése	Minden felhasználót csoporthoz rendel. Minden felhasználót definiál, beleértve a jellemzőket is, amelyek eltérhetnek a csoport többi tagjától. Például, egyes felhasználóknak eltérő hozzáférésre lehet szükségük az alkalmazáshoz vagy a könyvtárhoz, mint a csoport többi tagjának.	Az alkalmazás- és a felhasználói csoport tervezés adataival határozhatja meg az egyedi felhasználókat.
Erőforrás biztonság tervezése	Eldönti, hogy melyik alkalmazásoknak kell rendelkezésre állni mindenki számára a rendszerben. Ha korlátozni kell bizonyos alkalmazásokat, el kell döntenie, mely felhasználóknak vagy csoportoknak engedi meg a használatukat.	Az alkalmazás- és a csoportprofil tervezés adataival tervezheti meg az erőforrás biztonságát.
Alkalmazások telepítésének tervezése	A tulajdonjogok és a nyilvános jogosultság kialakítása az alkalmazási könyvtárak számára.	Az erőforrás biztonság tervezési adatai segítséget nyújtanak az alkalmazás telepítés tervezéséhez.

A biztonság tervezési folyamatát a Felhasználói biztonság tervezésével kezdje.

---

## Felhasználói biztonság tervezése

A felhasználói biztonság tervezése magában foglalja az összes olyan területet, ahol a biztonság hatással van a felhasználókra a rendszeren. Lényeges, hogy leírja az alábbi területeket:

### Fizikai biztonság

A fizikai biztonság körébe tartozik az iSeries védelme a véletlen (vagy szándékos) sérüléssel vagy lopással szemben. Ezen túlmenően, ide tartozik az összes munkaállomás, nyomtató és tárolóeszköz védelme is. A "Fizikai biztonság tervezése" című rész további tájékoztatást ad a fizikai biztonság tervezéséről, a kockázatokról és az IBM ajánlásokról.

### Alkalmazás biztonság

Az alkalmazás biztonság azzal foglalkozik, hogy mely alkalmazásokat tárolja a rendszeren, és hogyan védje őket, miközben a felhasználók egyidejűleg hozzájuk férhetnek. Az "Alkalmazások biztonságának tervezése" részletekkel szolgál az alkalmazások leírásáról és névadási szabályairól.

### Átfogó biztonsági stratégia

Az átfogó biztonság magában foglalja egy olyan biztonsági terv kidolgozását, amely foglalkozik a pillanatnyi helyzettel és a jövőbeli üzleti tervekkel is. Az "Átfogó biztonsági stratégia tervezése" című rész további tájékoztatást nyújt a biztonsági szabályzatról, a biztonság szintjéről, a jelszavakkal kapcsolatos szempontokról és a rendszerváltozókról.

### Felhasználói csoport biztonsága

A felhasználói csoport a felhasználók olyan csoportja, akiknek ugyanazokat az alkalmazásokat, ugyanazon a módon kell használniuk. A felhasználói csoport biztonsága magában foglalja a rendszert használni kívánó munkacsoportok, valamint a csoportok számára szükséges alkalmazások meghatározását. A "Felhasználói csoportok tervezése" című szakasz részletes tájékoztatást ad a felhasználói csoportok azonosításáról, a rendszerváltozók kiválasztásáról, valamint a felhasználói környezet meghatározásáról.

### Egyedi felhasználói biztonság

Miután eldöntötte, hogy milyen felhasználói csoportokra van szüksége, megtervezheti az egyedi felhasználói profilokat. Az "Egyedi felhasználói profilok tervezése" című szakasz további tájékoztatást nyújt a felhasználók elnevezéséről a rendszeren, az egyedi felhasználók felelősségének megállapításáról, valamint a rendszerváltozók kiválasztásáról.

A könyvben mindenütt talál hivatkozást az űrlapokhoz, amelyekre felírhatja saját tervezési döntéseit.

## Fizikai biztonság tervezése

Az iSeries telepítésének előkészületei során kell elkészíteni a fizikai tervet, amelyben a következő kérdéseket kell feltenni:

- Hova kerül a rendszeregység?
- Hova helyezük el az egyes megjelenítő állomásokat?
- Hova kerülnek a nyomtatók?
- Milyen további eszközökre van szükség, például kábelezésre, telefonvonalakra, bútorra, tároló polcra?
- Milyen mértékű védelmet kíván biztosítani vészhelyzetekre, mint például tűz vagy áramkimaradás?

A fizikai biztonság az átfogó biztonsági tervezés fontos része. Szükség lehet speciális szintű védelemre attól függően, hogy hová helyezi el a rendszert és eszközeit.

A Fizikai biztonság tervezési űrlapra jegyezze fel döntéseit a saját rendszerén megvalósítandó fizikai biztonságról. Nézze át az alábbi témaköröket, hogy ne hagyjon ki semmit a fizikai biztonság szempontjai közül:

- A Rendszeregység fizikai biztonsága magáról a rendszer védelméről ismertet részleteket.
- A Rendszerdokumentációk és tárolási adathordozók fizikai biztonsága tájékoztatást nyújt a dokumentációk és a tároláshoz használt adathordozók védelméről.
- A Munkaállomások fizikai biztonsága a munkaállomások biztonságossá tételének módját tárgyalja.

- A Nyomatók és nyomtatott listák fizikai biztonsága a nyomtatók és a kinyomtatott listák fizikai védelmének részleteit ismerteti.
- A Biztonsági szabályzat tervezése elmagyarázza a felhasználói útmutatók és biztonsági szabályzatok elkészítését.

Minden rendszeregység rendelkezik vezérlőpanellel, amely a berendezés kiszolgálására és speciális rendszerműveletek - mint például a be- és kikapcsolás - végzésére való. A fenti rendszerműveletek jogosulatlan használata ellen véd a gépen található kulcszár kapcsoló vagy az elektronikus kulcsdugó. Bár a kulcszár vagy az elektronikus kulcsdugó adnak bizonyos biztonságot, nem helyettesíthetik a megfelelő fizikai biztonságot.

## A rendszeregység fizikai biztonsága

Az iSeries nem igényel speciális környezeti vezérléssel ellátott számítógéptermet. A rendszert gyakran találhatja egy irodahelyiség közepén, ahol sok ember elérheti. A vásárlók szeretik az iSeries kicsi méretét és minimális karbantartási igényét, azonban ezek a tulajdonságok ugyancsak növelhetik a biztonsági kockázatokat. Például, akár egy személy is könnyen el tudja lopni a rendszeregységet vagy ki tudja venni egy értékes elemét.

Alaposan meg kell tehát vizsgálni, hogy a rendszeregység biztonságos helyen van-e. A legjobb hely egy önálló, zárható terem. A rendszeregységet legalább olyan helyre kell tenni, amely a normál munkaidőn túl zárható.

### Rendszeregységgel kapcsolatos kockázatok

A rendszeregység fizikai biztonságának nem kellő biztosítása az egység és komponenseinek ellophatóságán túl az alábbi kockázatokat is magában rejtí:

#### A rendszerműveletek véletlen megszakítása

Sok biztonsági probléma jöhet a jogosult felhasználóktól. Tételezzük fel, hogy a rendszer egyik megjelenítő állomása leblokkol. A rendszeroperátor nincs elérhető helyen. A leblokkolt állomás kiábrándult felhasználója odasétál a rendszeregységhez, s gondolja, "Lehet, hogy ha megnyomom ezt a gombot megoldódik a problémám...". Az a gomb azonban lehet, hogy kikapcsolja és újratölti a rendszert miközben számtalan munka fut rajta. Esetleg több órába telik a részlegesen frissített állományok helyreállítása. Ennek megelőzésére használhatja a kulcszár kapcsolót.

#### A biztonság megkerülése a Kijelölt szervizeszközök (DST) funkcióval

A biztonság nem irányítja a rendszer által végrehajtott szerviz funkciókat, mivel a rendszerszoftver lehet, hogy nem működik megfelelően, amikor ezeket a funkciókat végre kell hajtania. Egy jól informált személy, aki tudja vagy kitalálja a Szervizeszközöknél használt felhasználói azonosítót és jelszót, a rendszer figyelemre méltó sérülését okozhatja. A Szervizeszközökről az Információs központ Szervizeszközök című témakörében olvashat.

### Javaslatok

- Ideális esetben tartsa a rendszeregységet egy zárt teremben. Ha erre nincs lehetősége, tegye olyan helyre, ahová idegenek nem juthatnak be. Továbbá, válasszon olyan helyet, ahol a felelős alkalmazottak figyelem alatt tarthatják. A fizikai biztonság következő eszközeivel védheti a rendszert a véletlen vagy szándékos beavatkozástól:
- Használja az elektronikus kulcsot vagy kulcszárát:
  - Tegye "Normal" állásba a működési üzemmód kapcsolóját, ha a rendszert a kulcs használata nélkül kívánja indítani.
  - Tegye "Auto" állásba a működési üzemmód kapcsolóját, ha használni akarja az "Automatic Power On/Off" funkciót a rendszer indítására és leállítására.
  - Vegye ki a kulcsot és tegye biztonságos helyre.
- Rögtön változtassa meg a Szervizeszközök (DST) felhasználói azonosítóját és jelszavát, amint telepítette a rendszert, és amint a szerviz személyzet használta. Az Információs központ Szervizeszközök témaköre részletesen tárgyalja, hogyan tudja ezt megtenni.

Szándékában állhat példaként megtekinteni a JKL Toy Company egység biztonságra vonatkozó tervét, mielőtt megtervezné a Rendszerdokumentációk és tárolási adathordozók fizikai biztonságát.

**Példa: JKL Toy Company fizikai biztonság tervezési űrlapja — rendszeregység rész:** Az alábbi példában a Fizikai biztonság tervezési űrlap rendszeregységre vonatkozó részét ismerheti meg, amelyet Sharon Jones állított össze a saját rendszeréhez:

3. táblázat: JKL Toy Company Fizikai biztonság tervezési űrlap: rendszeregység példa

Fizikai biztonság tervezési űrlap	
Készítette: Sharon Jones	Dátum: 9/2/99
<b>Rendszeregység:</b>	
A rendszeregység biztonságáról végzett vizsgálatok eredménye (például zárt terem):	A rendszeregység a számviteli részleg területén van. Munkaidő alatt a számviteli alkalmazottak mindig ott tartózkodnak és figyelemmel kísérik a rendszeregységet. A számviteli alkalmazottak ugyancsak felelősek csekély készpénzért és fontos iratokért is. Szabályos munkaidőn túl a terület zárva van.
Melyik kulcsár pozíció legyen használva?	Normal
Hol legyen a kulcs tárolva?	Kicsi széfben, Sharon irodájában.
További megjegyzések a rendszeregységhez:	A rendszeregység könnyen hozzáférhető lesz. A területen dolgozókat figyelmeztetni kell, hogy a rendszeregységben illetéktelenek nem kontárkodhatnak.

Miután megtervezte a rendszeregység fizikai biztonságát, megtervezheti a rendszer dokumentációk és adathordozók fizikai biztonságát.

## Rendszerdokumentációk és tárolási adathordozók fizikai biztonsága

A fizikai biztonság terv egyik része a fontos rendszer dokumentációk és tárolási adathordozók tárolásával törődik. A rendszerdokumentáció magában foglalja az IBM által a rendszerrel küldött egyéb információkat, jelszavakat, tervezési űrlapokat és a rendszer által generált riportokat.

A rendszertől függően a biztonsági mentés adathordozója lehet szalag, CD-ROM, hajlékonylemez vagy DVD tároló. A rendszerdokumentációt, valamint a biztonsági mentés adathordozóit tárolja a telephelyén és külső helyszínen is. Katasztrófa esetén szüksége van ezekre az anyagokra a rendszer helyreállításához. Az alábbiakban javaslatot talál a rendszerdokumentáció és az adathordozók tárolási módjára. Miután döntött a saját módszeréről, jegyezze fel választását a Fizikai biztonság tervezési űrlap Biztonsági mentés adathordozója és dokumentációk című szakaszában.

### Rendszerdokumentációk biztonságos tárolása

A Szervizeszközök és a biztonsági felelős jelszavai igen fontosak a rendszer működéséhez. Írja fel ezeket a jelszókat és tárolja őket egy széfben, biztonságos helyen. Továbbá, tartson egy másolatot a jelszavakról külső helyszínen is, hogy elérhetőek legyenek katasztrófa helyreállítás során.

Más fontos rendszerdokumentumokat, mint például a konfigurációs beállításokat és a fő alkalmazási könyvtárakat, is érdemes a helytől távol tartani, ami katasztrófa esetén segíthet a helyreállításban.

### Tárolási adathordozók biztonságos tárolása

Amikor telepíti a rendszert, tervet kell készítenie a rendszer információinak szabályos időközönkénti szalagra vagy más adathordozóra mentéséről. Ezek a biztonsági mentések lehetővé teszik a rendszer helyreállítását szükség esetén. Az ilyen biztonsági mentéseket ugyancsak külső, biztonságos helyszínen kell tárolni.

### Kockázatok

- Biztonsági mentés adathordozója megsérül: Ha katasztrófa vagy vandalizmus miatt megrongálódik a biztonsági mentés adathordozója, a rendszer információit nem tudja visszaállítani, kivéve a nyomtatott riportokat.

- A biztonsági mentés adathordozóját vagy a jelszavakat ellopják: Üzleti szempontból fontos és bizalmas információk lehetnek a mentési adathordozókon. Képzett szakember képes lehet az adatokat másik számítógépen betölteni és kinyomtatni vagy feldolgozni.

#### Javaslatok

- Az összes jelszót és mentési adathordozót tárolja zárható, tűzbiztos szekrényben.
- Szabályos időközönként (legalább hetente) vigye a mentési adathordozók egy másolatát külső helyre.

Szándékában állhat példaként átnézni a JKL Toy Company rendszerdokumentáció tárolására vonatkozó tervét, mielőtt megtervezné a Munkaállomások fizikai biztonságát.

**Példa: JKL Toy Company fizikai biztonság tervezési űrlapja — mentési adathordozók és dokumentációk rész:**  
Sharon Jones az alábbi táblázat szerint készítette el a JKL Toy Company Fizikai biztonság tervezési űrlapjának Mentési adathordozók és dokumentációk című részét:

4. táblázat: JKL Toy Company Fizikai biztonság tervezési űrlap: mentési adathordozók és dokumentációk példa

Fizikai biztonság tervezési űrlap	
Készítette: Sharon Jones	Dátum: 9/2/99
<b>Mentési adathordozók és dokumentációk:</b>	
Hol legyenek a mentési szalagok a munkahelyen tárolva?	A cég számviteli alkalmazottainak irodájában egy tűzbiztos széfben.
Hol legyenek a mentési szalagok távolabbi helyen tárolva?	A cég egy másik irodájában egy tűzbiztos széfben.
Hol legyenek a jelszavak (biztonsági felelős, szerviz és DST) tárolva?	Széfkombinációval John Smith irodájában.
Hol legyenek a fontos rendszerdokumentumok (szériaszám, konfiguráció) tárolva?	Egy távoli nagy széfben és a számviteli alkalmazottak irodájában.

Miután megtervezte a tárolási adathordozók és a dokumentációk biztonságát, megtervezheti a munkaállomások fizikai biztonságát.

### Munkaállomások fizikai biztonságának tervezése

A legtöbb esetben szeretnénk ha minden felhasználó bármelyik munkaállomásról bejelentkezhetne és végrehajthatná a megengedett funkciókat. Azonban, ha vannak olyan munkaállomásai, amelyek nagy nyilvánosságú vagy nagyon eldugott helyen vannak, speciális óvintézkedéseket tehet. Például, a billentyű leütéseket tárolni képes megjelenítő állomások és személyi számítógépek is speciális körülményt igényelnek. Az itt leírtak segítséget nyújtanak a Fizikai biztonság tervezési űrlap 2. részének (Munkaállomások és nyomtatók fizikai biztonsága) kitöltéséhez.

#### Munkaállomásokkal kapcsolatos kockázatok

##### Munkaállomás jogosulatlan használata nyilvános helyen

Ha a dolgozókon kívül más emberek is könnyen bejuthatnak az adott helyszínre, esély van arra, hogy bizalmas információkhoz jutnak. Ha a felhasználó otthagyja a munkaállomást bejelentkezve, külső ember könnyedén odasétálhat és elérhet bizalmas információkat.

##### Munkaállomás jogosulatlan használata eldugott helyen

Egy nagyon eldugott helyen lévő munkaállomás lehetőséget ad a betolakodásra. Túl sok idő állhat rendelkezésre a biztonság becsapására az észrevétlenség következtében.

##### Visszajátszás funkció vagy PC bejelentkezési program használata a munkaállomáson a biztonsági szabályok kijátszása érdekében

Számos megjelenítő állomás rendelkezik rögzítő és visszajátszó funkcióval, amely megengedi a felhasználónak a sűrűn előforduló billentyűleütések tárolását és ismétlésüket egy gomb lenyomásával. Amikor személyi számítógépet használ munkaállomásként az iSeries rendszeren, írhat egy programot, amely

automatizálja a bejelentkezési folyamatot. Mivel a felhasználók gyakran használják a bejelentkezési folyamatot, a felhasználók dönthetnek úgy, hogy inkább letárolják azonosítójukat és jelszavukat, mintsem begépeljék minden alkalommal.

## Javaslatok

Fontolja meg az alábbi ajánlásokat, amikor összeállítja a munkaállomások fizikai biztonságára vonatkozó tervét:

- Ha lehetséges, kerülje a munkaállomások elhelyezését nagy nyilvánosságú vagy eldugott helyeken.
- Hangsúlyozza a felhasználóknak a kijelentkezés fontosságát a munkaállomás elhagyásakor. A biztonsági szabályzatban térjen ki a kijelentkezési folyamatra.
- Hangsúlyozza, hogy a jelszó rögzítése a megjelenítő állomáson vagy PC programban sérti a rendszer biztonságát. A biztonsági szabályzatban térjen ki a jelszó rögzítésére.
- Az inaktivitást figyelő rendszerváltozók (QINACTIV és QINACTMSGQ) használatával megelőzheti, hogy a felhasználó kijelentkezés nélkül magára hagyja a munkaállomást nyilvános helyen.
- Korlátozza a nyilvános munkaállomáson végrehajtható funkciókat és csak az őket használó felhasználókat jogosítsa fel korlátozott jogosultsággal az ilyen munkaállomások használatára.
- Előzze meg az eldugott munkaállomásról a bejelentkezést biztonsági felelősi és szervizjogosultságú profillal. A QLMTSECOFR rendszerváltozóval megadhatja, hogy honnan jelentkezhet be a felhasználó ilyen jogosultságokkal.
- Tiltsa meg, hogy a felhasználók egy időben több állomásról is bejelentkezzenek. A QLMTDEVSSN rendszerváltozóval korlátozva az eszközzetekciókat vezérelheti, hogy honnan jelentkezzenek be a felhasználók.

Az itteni ajánlások megvalósításához olvassa el a "Bejelentkezést befolyásoló rendszerváltozók kiválasztását" és a "Munkaállomások erőforrás biztonságának tervezését".

A Fizikai biztonság tervezése űrlapon meg kell határoznia, hogy melyik munkaállomás fizikai elhelyezése jelent biztonsági kockázatot. Szándékában állhat példaként átnézni, hogy Sharon Jones hogyan tervezte meg a JKL Toy Company munkaállomásainak fizikai biztonságát.

Miután megtervezte a munkaállomás biztonságát, megtervezheti a Nyomatatók és nyomtatott listák fizikai biztonságát.

## Nyomatatók és nyomtatott listák fizikai biztonsága

Ha egyszer az információ nyomtatása megkezdődik, a rendszerbiztonság tovább nem tudja kontrollálni, ki látja a listát. Védeni kell a nyomtatót és a nyomtatott listákat, hogy minimalizálja a veszélyét annak, hogy valaki betekintést nyer az érzékeny üzleti adatokba. Készítsen egy szabályzatot, amely a bizalmas üzleti információk kinyomtatásáról rendelkezik.

### Nyomatatókkal és nyomtatott listákkal kapcsolatos kockázatok

A következő kockázatok jelentkezhetnek az üzletmenetében. Ezek a leggyakoribb biztonsági kockázatok, amelyek a nyomtatókkal és a nyomtatott listákkal kapcsolatban előfordulhatnak. Azonban meg kell vizsgálni az egyéb kockázatokot is, amelyek egy adott üzletmenetben jelentkezhetnek.

- Ha a nyomtató nyilvános helyen van, esetleg jogosulatlan személy bizalmas információ birtokába juthat.
- A nyomtatott lista asztalon hagyásával az adatok szem elé kerülhetnek.
- A rendszer lehet, hogy csak egy vagy két nyomtatóval rendelkezik. Lehet, hogy olyan értékes vagy bizalmas információt - úgymint fizetescédula - kellene kinyomtatnia, amit nem kellene másoknak látni.

## Javaslatok

A következő ajánlások révén csökkentheti a nyomtatókkal és a kinyomtatott listákkal kapcsolatos biztonsági kockázatokot.

- Hangsúlyozza a felhasználóknak a bizalmas adatokat tartalmazó listák védelmének fontosságát. Írja bele a biztonsági szabályzatba a nyomtatók fizikai biztonságára vonatkozó döntéseit.
- Kerülje el a nyomtató nyilvános helyen való elhelyezését.

- Időzítse a szigorúan bizalmas listák nyomtatását és gondoskodjon arról, hogy egy jogosult személy tartózkodjon a nyomtatónál ez idő alatt.

A "Nyomtatók és nyomtatott listák biztonságának tervezése" című rész tárgyalja a bizalmas nyomtatott listák kezelésére vonatkozó javaslatokat.

Szándékában állhat példaként megtekinteni a JKL Toy Company nyomtató biztonságára vonatkozó tervét, mielőtt megtervezné a Biztonsági szabályzatot.

**Példa: JKL Toy Company fizikai biztonság tervezési űrlapja — munkaállomás és nyomtató rész:** Az alábbi példában a Fizikai biztonság tervezési űrlap második részét ismerheti meg, amelyet Sharon Jones állított össze a JKL Toy Company számára:

5. táblázat: JKL Toy Company Fizikai biztonság tervezési űrlap: munkaállomás és nyomtató példa

Fizikai biztonság tervezési űrlap			Második rész
Munkaállomások és nyomtatók fizikai biztonsága			
Munkaállomás vagy nyomtató neve	Helye vagy leírása	Biztonsági helyzete	Védelem mértéke
DSP06	Fogadó raktár	Túl nyilvános	Automatikus kijelentkezés. Munkaállomásról elvégezhető funkciók korlátozása.
DSP09	Ügyfélszolgálati pult	Túl nyilvános	Automatikus kijelentkezés. Munkaállomásról elvégezhető funkciók korlátozása.
RMT12	Távoli értékesítőhely	Túl eldugott	Ne engedjen biztonsági felelősi bejelentkezést onnan.
PRT02	Számviteli részleg, a rendszerhez közel	Érzékeny információk (például árlisták) láthatók	Valaki kinevezése a nyomtatott anyag figyelésére

Miután befejezte a Fizikai biztonság tervezési űrlapot, folytassa a biztonsági szabályzat tervezésével.

## Biztonsági szabályzat tervezése

Hasznosnak találhatja, hogy minden alkalmazottnak elküldje a biztonsági irányelveket, ezzel is kihangsúlyozva a fizikai- és a rendszerbiztonsággal kapcsolatos útmutatásokat. Ugyanazt az útmutatót adhatja oda a rendszerbe később belépő új felhasználóknak is.

Ennek az útmutatónak tartalmaznia kell néhány általános utasítást a rendszer biztonságának megőrzésével kapcsolatban, mint például a kijelentkezés szükségessége vagy a jelszó meg nem oszthatósága. Ugyancsak tartalmaznia kell a saját döntései eredményeképpen született egyedi előírásokat is.

A cikk olvasása közben készítsen jegyzetet arról, amit a saját útmutatójába belevesz. Lehet, hogy Ön is tesz megjegyzést biztonsági szabályzatához.

Például, Sharon Jones a JKL Toy Company felelőse a következő megjegyzéseket fűzte saját útmutatójához, amikor a rendszer fizikai biztonságát tervezte:

Kihangsúlyozni a kijelentkezés fontosságát az anyagszállítás, az ügyfélszolgálat, az eladóhely számára. A könyvelésen dolgozók tartják szemmel a rendszerezésüket.

Miután kitöltötte a Fizikai biztonság tervezési űrlapját, készen áll az Alkalmazások biztonságának tervezésére.

## Az alkalmazás biztonságának tervezése

Az alkalmazások megfelelő biztonságának tervezéséhez a következőket kell tudni:

- Milyen információkat kíván tárolni a rendszeren?
- Kinek szükséges ezen információk elérése?
- Milyen típusú elérésre van szükség? A felhasználóknak változtatni is kell az információt vagy csak megtekinteni?

Ahogy végighalad az alkalmazás tervezési témakörein, először az első kérdésre fog válaszolni, vagyis arra, hogy milyen információkat kíván tárolni a rendszeren. A többi kérdéssel kapcsolatos döntését a az ezt követő témakörökben leírtakat alapul véve hozhatja meg. Az alkalmazás biztonságának tervezési információit nem kell ugyan megadni a rendszeren, azonban bizonyos információkra szükség lesz a felhasználók és az erőforrás biztonság tervezésekor.

### Mi az alkalmazás?

Az alkalmazások biztonságának tervezésében első lépésként a rendszeren futtatni kívánt alkalmazásokat kell leírni. Az alkalmazás logikailag egymáshoz tartozó funkciók egy csoportja. Például, a JKL Toy Company cégnél a rendelések felvétele, rendelések kiszállítása, számlák nyomtatása mind a Vevő rendelések nevű alkalmazás egyes funkciói.

Általában két különböző típusú alkalmazás fut az iSeries rendszeren:

- **Üzleti alkalmazások:** Vásárolt vagy fejlesztett alkalmazások adott üzleti funkciók elvégzésére, mint például rendelésfeldolgozás, készletgazdálkodás.
- **Speciális alkalmazások:** Az ilyen alkalmazások a legkülönbézetbb vállalati tevékenységeket támogathatják, amelyek nem kifejezetten az üzleti folyamathoz tartoznak.

### Milyen űrlapra van szükség?

Az alkalmazás biztonságának tervezéséhez használja a következő űrlapokat:

- Alkalmazást leíró űrlap
- Könyvtárat leíró űrlap
- Elnevezési szabályok űrlap

Az űrlapok nyomtatásához kattintson a hivatkozásra, válassza ki a jobboldali keretet, majd kattintson a **Nyomtat** ikonra a böngészőben.

A tervezési űrlapok kitöltéséhez olvassa el az alábbiakat:

- Alkalmazások leírása
- Elnevezési szabályok leírása
- Könyvtári információk leírása
- Alkalmazási diagram rajzolása

## Alkalmazások leírása

Ennél a pontnál össze kell gyűjteni néhány általános ismeretet az összes üzleti alkalmazásáról. Az alábbiak szerint írja be alkalmazásainak adatait az Alkalmazást leíró űrlap megfelelő mezőibe. Később felhasználhatja az ismeretet a felhasználói csoportok és az alkalmazás biztonságának tervezésekor:

### Alkalmazás neve és rövidítése

Adjon az alkalmazásnak rövid nevet és rövidítést a kezelés egyszerűsítéséért, és az alkalmazás által használt objektumok elnevezéséhez.

### Leíró információ

Rövid leírás az alkalmazás funkciójáról.

### Elsődleges menü és könyvtár

Határozza meg az alkalmazás elérhetőségét adó elsődleges menüt. Jelezze a könyvtárat, ahol a menü található. Általában az elsődleges menü vezeti a specifikus alkalmazói funkciókat tartalmazó többi képernyő sorát. A felhasználók az alkalmazásuk elsődleges menüjét rögtön a bejelentkezést követően szeretik látni.



## Kezdeti program és könyvtár

Néha az alkalmazások lefuttatnak egy kezdeti programot a háttér feltérképezése vagy a biztonság ellenőrzése végett. Ha az alkalmazásnak van kezdeti- vagy beállító programja, jelezze az űrlapon.

## Alkalmazás könyvtárak

Általában minden alkalmazásnak van egy könyvtára fájljai részére. Az összes könyvtárat vegye számításba, amelyeket az alkalmazás használ, beleértve a programkönyvtárakat és a többi alkalmazás könyvtárát is. Például, a JKL Toy Company cég Vevő rendelések alkalmazása használja a készlet könyvtárat a tételek leírása és a raktári készletérték végett.

A könyvtárak és az alkalmazások közötti kapcsolatok felhasználhatók annak megállapítására, hogy kinek milyen könyvtárakat kell elérni.

## Alkalmazások információinak fellelhetősége

Ha még nem állnának rendelkezésére az alkalmazások információi, lépjen kapcsolatba a programozókkal vagy az alkalmazások szállítóival.

Az alábbiakban ismertetett mód segíthet a rendszeren futó alkalmazások információinak saját erőnkől történő összegyűjtésében, ha ezek eléréséhez más út nem áll rendelkezésünkre.

- Az alkalmazás felhasználói feltehetően meg tudják mondani az elsődleges menü és könyvtár nevét, vagy meg tudja nézni bejelentkezéskor.
- Ha a felhasználók rögtön látják az alkalmazást a bejelentkezés után, megnézheti az **Initial program** mezőt a felhasználói profiljukban. Ez a mező tartalmazza az alkalmazás kezdeti programját. A DSPUSRPRF parancs segítségével megtekintheti a kezdeti programot.
- Kिलistáztathatja a rendszer összes könyvtárának nevét és leírását. Ehhez használja a DSPOBJD \*ALL \*LIB parancsot. Megjelenik a rendszer összes könyvtára.
- Megnézheti az aktív munkákat, míg a felhasználók az alkalmazást futtatják. A Work with Active Jobs (WRKACTJOB) parancsot közepes támogatási szinttel használja, hogy részletes információt nyerjen az interaktív munkákról. Jelenítse meg a munkákat és tekintse meg a könyvtárlistákat, valamint azok blokkolt objektumait a használatban lévő könyvtárak megállapításához.
- Egy adott alkalmazás köteget munkáit a Work with User Jobs (WRKUSRJOB) paranccsal jelenítheti meg.

A folytatás előtt hajtsa végre az alábbi feladatokat, hogy bizonyos legyen afelől, minden szükséges információt összegyűjtött az alkalmazás biztonságának tervezéséhez:

- Töltse ki az Alkalmazást leíró űrlapot minden üzleti alkalmazására. Töltse ki az egész űrlapot a biztonsági követelmények rész kivételével. Az alkalmazás erőforrás biztonságának tervezéséhez használja fel az "Erőforrás biztonság tervezése" című témakör megfelelő szakaszát.
- Töltse ki az Alkalmazást leíró űrlapot minden speciális alkalmazására. Az űrlap használata segítségre van az alkalmazás elérésének meghatározásakor.

**Megjegyzés:** Az IBM által szállított speciális alkalmazásokra, mint például az IBM Query for iSeries termékre, választható, hogy kitölti-e az Alkalmazást leíró űrlapot. Ezen alkalmazások által használt könyvtárak elérése nem igényel speciális tervezést. Ennek ellenére hasznosnak tűnik az információk összegyűjtése és az űrlap kitöltése.

Szándékában állhat példaként megtekinteni a JKL Toy Company Alkalmazást leíró űrlapját, mielőtt az Elnevezési szabályok leírására kerülne sor.

**Példa: JKL Toy Company Alkalmazást leíró űrlap:** Sharon Jones felsorolta a társaság összes alkalmazását rövidítésekkel együtt a saját Alkalmazást leíró űrlapján. Leírta röviden azt is, hogyan dolgoznak a felhasználók ezekkel az alkalmazásokkal.

## Vevő rendelések (CO)

Rendelésfelvétel, követés és szállítás. Számlák nyomtatása.

### **Készletgazdálkodás (IC)**

Felügyeli mind a késztermékek, mind az anyagok rendelkezésre álló szintjét. Feldolgozza az összes raktári mozgást.

### **Szerződések és árak (CP)**

Felügyeli az ügyfelekkel kötött speciális szerződéseket és árakat.

### **Vevő tartozások (AC)**

Nyomon követi a vevők számláinak pillanatnyi egyenlegét. A havi állapotot nyomtatja.

Az alábbi táblázat tartalmazza Sharon Jones leírását a Vevő rendelések alkalmazásról. Szisztematikusan készítette el űrlapjait, kezdve az első alkalmazással, majd leírva a többit is.

#### *6. táblázat: JKL Toy Company Alkalmazást leíró űrlap: példa*

Alkalmazást leíró űrlap	
Készítette: Sharon Jones	Dátum: 9/3/99
Alkalmazás neve: Vevő rendelések	Rövidítés: CO
Az alkalmazás rövid leírása:	Vásárlói megrendelések bevitel, szállítás előtti követésük, leszállításuk, szállítólevelek és számlák kinyomtatása.
Elsődleges menü: COMAIN	Könyvtár: COPGMLIB
Kezdeti program neve: NA	Könyvtár: NA
Fájlok és programok részére használt könyvtárak listája: <ul style="list-style-type: none"><li>• CUSTLIB</li><li>• ITEMLIB</li><li>• CONTRACTS</li><li>• COPGMLIB</li></ul>	
Határozza meg az alkalmazás biztonsági elemeit, vajon van-e titkos információ:	

A Vevő rendelések alkalmazáson túl, Sharon Jones elkészítette az Alkalmazást leíró űrlapokat a JKL Toy Company rendszerének alábbi alkalmazásaira is:

- Készletgazdálkodás
- Szerződések és árak
- Vevő tartozások

Következő lépésként leírhatja az elnevezési szabályokat a rendszer objektumaira vonatkozóan.

### **Elnevezési szabályok leírása**

A rendszerben lévő objektumok neveinek ismeretében tervezheti és figyelheti a biztonságot, megoldhatja a problémákat, megtervezheti a mentést és a visszaállítást. Az alkalmazások többsége megfelelő szabály szerint rendel nevet a könyvtárakhoz, fájlokhoz, programokhoz. Ha az alkalmazások különböző forrásokból valók, feltételezhetően egyedi elnevezési szabályokkal rendelkeznek.

Mindenképpen jegyezze fel az alkalmazásokra és objektumokra vonatkozó összes elnevezési szabályt az Elnevezési szabályok űrlapján. Az űrlap kitöltésével írja le az alkalmazások könyvtárainak és fájljainak elnevezési szabályait. Használhatja az üres sorokat más objektumok elnevezési szabályai számára, mint például programok és menük részére. Ha az alkalmazások különböző forrásokból valók, feltételezhetően egyedi elnevezési szabályokkal rendelkeznek. Írja le az elnevezési szabályokat mindegyik alkalmazásra. Lehet, hogy egynél több űrlap kitöltésére lesz szükség.

Szándékában állhat példaként megtekinteni a Sharon által a JKL Toy Company rendszerén lévő objektumokra alkalmazott elnevezési szabályokat, mielőtt a Könyvtári információk leírására kerülne sor.

**Példa: JKL Toy Company Elnevezési szabályok űrlap:** Az alábbi táblázat csak a könyvtárakra és fájlokra vonatkozó elnevezési szabályokat mutatja be. Természetesen, a rendszer más objektumaira is le kell írni az elnevezési szabályokat. Az Elnevezési szabályok űrlap tartalmaz néhány általános objektumot ugyan, de lehetnek más objektumai, amelyeket Önnek kell felvenni.

7. táblázat: JKL Toy Company Elnevezési szabályok űrlap: példa

Elnevezési szabályok űrlap	
Készítette: Sharon Jones	Dátum: 9/3/99
Objektum típusa	Elnevezési szabály
Könyvtárak	A fájlokot tartalmazó könyvtárak nevei értelmes jelentésűek, úgymint CONTRACTS vagy ITEMLIB. A programkönyvtárak nevei az alkalmazás rövidítését használják a PGMLIB előtt, úgymint ICPGMLIB.
Fájlok	A fájlok többségének értelmes neve van, úgymint CUSTMAST a Customer Master fájl- vagy ITEMMAST az Item Master fájl számára. Az alkalmazás többi fájljának neve (ezek elsősorban a programozók számára érthető) áll az alkalmazás rövidítéséből a FILE előtt és egy számból, úgymint az ICFILE14.

Miután befejezte az Elnevezési szabályok űrlapot, elkezdheti a könyvtárak leírását.

## Könyvtári információk leírása

Miután leírta az elnevezési szabályokat, a rendszeren lévő könyvtárak leírása következik. A könyvtárak azonosítják és szervezik a rendszeren található objektumokat. A hasonló állományok könyvtárba helyezése lehetővé teszi a felhasználóknak, hogy könnyedén elérjék a fontos alkalmazásokat és fájlokat. A felhasználók jogosultságát is testre szabhatja így, hiszen bizonyos könyvtárakat elérhetnek, míg másokat nem. Írja le az egyes alkalmazások könyvtárait, amelyek a rendszeren találhatóak. Lehet, hogy egynél több Könyvtárat leíró űrlapra lesz szükség.

**Megjegyzés:** Csak a könyvtárat leíró információt töltsse ki. A Könyvtárat leíró űrlap maradék részeit akkor fogja kitölteni, amikor a könyvtár erőforrás biztonságát tervezi. A könyvtárakra vonatkozó jogosultsági információkat később írja be. A Könyvtárat leíró űrlap befejezésével kapcsolatban olvassa el az "Alkalmazási könyvtárak biztonságának tervezése" című részt.

Mielőtt folytatná, mindenképpen fejezze be a következőket:

- Töltse ki az Elnevezési szabályok űrlap könyvtár és fájl részeit.
- Töltse ki a Könyvtárat leíró űrlap leíró mezőit minden egyes alkalmazási könyvtárra.

Szándékában állhat példaként megtekinteni Sharon leírását a JKL Toy Company könyvtárainról, mielőtt az Alkalmazási diagram rajzolására kerülne sor.

**Példa: JKL Toy Company Könyvtárat leíró űrlap:** Az alábbi két táblázat két könyvtárat ír le, amelyeket a Vevő rendelések nevű alkalmazás használ a JKL Toy Company esetében. Az első táblázat a fájlokat, míg a második a programokat tartalmazó könyvtárat írja le.

8. táblázat: JKL Toy Company Könyvtárat leíró űrlap: példa fájlokat tartalmazó könyvtárra

Könyvtárat leíró űrlap	
Készítette: Sharon Jones	Dátum: 9/3/99
Könyvtár neve: CUSTLIB	Leírónév (szöveg): Vásárlói bejegyzések könyvtára
A könyvtár funkciójának rövid leírása:	Őrzi az összes vásárló adatait, beleértve a rendeléseket és követeléseket.

9. táblázat: JKL Toy Company Könyvtárat leíró űrlap: példa programokat tartalmazó könyvtárra

Könyvtárat leíró űrlap	
Készítette: Sharon Jones	Dátum: 9/3/99

9. táblázat: JKL Toy Company Könyvtárak leíró űrlap: példa programokat tartalmazó könyvtárra (Folytatás)

Könyvtár neve: COPGMLIB	Leírónév (szöveg): Vásárlói bejegyzések programkönyvtára
A könyvtár funkciójának rövid leírása:	A Vevő rendelések alkalmazás összes programját tárolja.

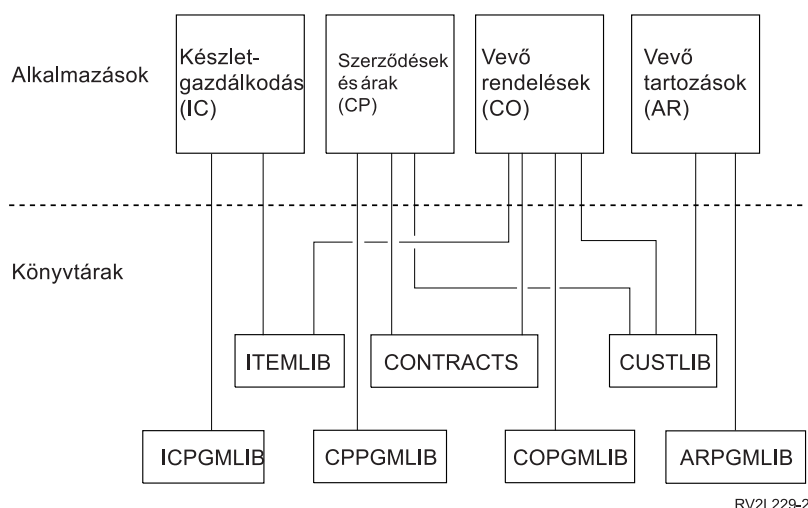
Miután leírta a könyvtárakat, rajzolja meg a rendszer alkalmazási diagramját.

## Alkalmazási diagram rajzolása

Az Alkalmazást és a Könyvtárak leíró űrlapok kitöltése kapcsán esetleg hasznosnak fogja itélni, ha az alkalmazások és a könyvtárak kapcsolatát egy diagram segítségével szemléletesebbé tesszük. A diagram segítséget jelent a felhasználói csoportok és az erőforrás biztonság tervezésében.

Az alábbi ábra Sharon Jones diagramját mutatja a JKL Toy Company alkalmazásairól és könyvtárainról.

### JKL Toy Company alkalmazásainak és könyvtárainak diagramja



Az alkalmazások és a könyvtárak információinak összegyűjtése nagyban segít a szükséges biztonsági döntések meghozatalában. Tekintse ezt úgy, mint egy esélyt tudása növelésére rendszeréről és az alkalmazásokról.

Az alábbiakat tegye meg, ha bizonyos akar abban lenni, hogy összegyűjtötte az alkalmazások információit:

- Töltse ki az Alkalmazást leíró űrlapot a rendszeren lévő minden üzleti alkalmazására.
- Nem kötelező jelleggel töltse ki az Alkalmazást leíró űrlapot a rendszeren lévő minden speciális alkalmazására.
- Töltse ki az Elnevezési szabályok űrlap könyvtár és fájl részeit.
- Készítse el a Könyvtárak leíró űrlapot minden alkalmazási könyvtárra.
- Rajzolja meg a diagramot az alkalmazások és a könyvtárak egymás közötti kapcsolatáról.

Mikor befejezte az űrlapokat, elkezdheti az Átfogó biztonsági stratégia tervezését.

## Átfogó biztonsági stratégia tervezése

Miután az Alkalmazások biztonságát megtervezte, készen áll az átfogó biztonsági stratégia kidolgozására. Először is döntést kell hozni a rendszer biztonságának általános megközelítési módjáról. Mikor e döntéseket hozza, teremtse meg az egyensúlyt a vállalat jelenlegi és jövőbeni igényei között.

Az itt leírtak elősegítik a tervezési folyamatot, valamint a biztonsági szabályzat és a célok meghatározását. Továbbá, segítségükkel kiválaszthatja az alapvető rendszerváltozókat, amelyek befolyásolják a rendszer összes felhasználóját.

### Milyen űrlapra van szükség?

Az alkalmazások tervezésének befejezéséhez használja a Rendszerváltozók kiválasztására szolgáló űrlapot.

A rendszerváltozók értékeinek eldöntéséhez használja fel a kitöltött Fizikai biztonság tervezése és Alkalmazást leíró űrlapokat, valamint az itt leírtakat.

A biztonsági stratégia tervezéséhez az alábbi témaköröket nézheti át:

- Biztonsági szabályzat írása
- Biztonsági szint kiválasztása
- Bejelentkezést befolyásoló rendszerváltozók kiválasztása
- Jelszavakat befolyásoló rendszerváltozók kiválasztása
- Rendszer egyéniesítése rendszerváltozókkal

## Biztonsági szabályzat írása

A tervezés megkezdése előtt, készítse el a rendszer biztonságára vonatkozó vállalati szabályzat kivonatát. Ez a kivonat egy megállapodás tulajdonképpen Ön és a felsőszintű vállalatvezetés között. Ez segít Önnek a döntéshozatalban és meghatározza a fontos feladatokat. A biztonsági szabályzat ki kell, hogy fejezze az Ön általános megközelítési módját és a védeni kívánt információ-vagyon meghatározását.

Minden rendszernek kell bizonyos biztonsággal rendelkeznie. A következő megközelítések egyikét alkalmazhatja a biztonságra:

- **Szigorú:** Egyes emberek "csak amit szükséges tudni" elnevezéssel is illetik ezt a biztonsági sémát. Az ilyen szigorú környezetben a felhasználók csak azokhoz az információkhoz és funkciókhoz kapnak hozzáférést, amely munkájukhoz elengedhetetlen. Minden más ki van zárva. Számos felügyelet javasolja az ilyen megközelítési módot.
- **Átlagos:** Az átlagos biztonsági környezetben a felhasználók a hozzájuk rendelt jogosultságok alapján férnek hozzá az objektumokhoz.
- **Laza:** Laza biztonsági környezetben megengedik a jogosult felhasználóknak a rendszeren található objektumok többségének elérését. A hozzáférést csak fontos és bizalmas erőforrások esetén korlátozzák. Az ilyen megközelítést általában csak részlegek vagy kicsi cégek alkalmazzák.

A kérdés általános megközelítése segít a konkrét biztonsági döntések meghozatalában. A rendszerbiztonság megközelítési módja összhangban kell, hogy legyen a vállalaton belüli egyéb információk elérési filozófiájával. Ha nem biztos abban, hogy milyen megközelítést alkalmazzon, próbálja meg a következőket:

- Döntse el a kitöltött Alkalmazást leíró űrlap segítségével, hogy kinek kell hozzáférnie és kinek nem az alkalmazásokhoz.
- Vizsgálja meg a vállalatnál bevezetendő technológiákat. Például, ha a rendszert vagy a hálózatot az Internethez kívánja kapcsolni, korlátozottabb biztonsági környezetet kíván kialakítani, hogy védje a rendszert az Internet külső felhasználóitól.
- Beszélgessen a szervezet más tagjaival is erről, például biztonsági ellenőrökkel, hogy jobban meg tudja határozni biztonsági szükségleteit.

Ne felejtse el, hogy szabályzatát mindig megváltoztathatja. A vállalatok többsége úgy találja, hogy a szigorúság fokozására van szükség növekedésük esetén. Az itt leírtak segítenek abban is, hogy olyan biztonsági sémát állítson össze, amely lehetővé teszi a szigorúság fokozását kevés változtatás mellett, az alkalmazások ismételt vizsgálata nélkül.

## Mit védjünk?

A biztonsági szabályzatban megfogalmazott általános megközelítésen túlmenően meg kell határozni a vállalat fontos információ-vagyonának körét. A rendszer biztonságát úgy kell megterveznie, hogy ez az információ-halmaz meg legyen védve. Használhat néhány követelményt a kritikus vagyon meghatározásához:

- **Bizalmasság:** Olyan információ, amely általában nem elérhető az emberek számára a vállalaton belül. Például ebbe a körbe tartozik a fizetési jegyzék.
- **Versenyképesség:** Olyan információ, amely a versenyben előnyös helyzetbe juttat, úgymint termékspecifikációk, minták, receptek.

- **Működés:** Olyan információk a számítógépen, amelyek nélkülözhetetlenek az üzletmenet napi műveleteihez, úgmint ügyféllista, raktárkészlet-nyilvántartás.

Sharon Jones biztonsági felelős és John Smith, a vállalat elnöke együtt dolgozták ki és készítették el a biztonsági szabályzatot. John Smith felhasználta az alábbi megjegyzéseket a JKL Toy Company biztonsági szabályzatához. Átnézheti a biztonsági szabályzatot, amelyet a JKL Toy Company megküldött minden alkalmazottnak, miután befejezték a biztonság tervezését és beállítását. Ne felejtse el a témakör feldolgozása során leírni megjegyzéseit arról, hogy mit akar belevenni a saját biztonsági szabályzatába.

10. táblázat: JKL Toy Company biztonsági szabályzata - példa

<p><b>Általános megközelítés</b> Laza: Az emberek többségének hozzá kell férni a legtöbb információhoz.</p> <p><b>Fontos információk</b></p> <ul style="list-style-type: none"> <li>• Szerződések és speciális árak</li> <li>• Bérlista</li> <li>• Vevői és leltári adatok csak a cég alkalmazottai számára</li> </ul> <p><b>Általános szabályok</b></p> <ul style="list-style-type: none"> <li>• Minden felhasználónak felhasználói profilja lesz. A felhasználók nem oszthatják meg profiljaikat és jelszavaikat egymással.</li> <li>• A felhasználóknak 60 naponként meg kell változtatni jelszavukat.</li> </ul>
--

Miután elkészítette megjegyzéseit a biztonsági szabályzattal kapcsolatban, kiválaszthatja a biztonsági szintet.

## Biztonsági szint kiválasztása

A QSECURITY rendszerváltozó biztosítja a rendszeren megvalósítandó biztonság mértékének beállítását. A biztonsági szintek működésének megértéséhez képzelje el egy épületként a rendszert, ahova az emberek megpróbálnak bemenni.

### 20-as szint: Jelszavas védelem

A 20-as szint beállításával bizonyos védelemhez jut. Az ajtónál álló őr az épületbe lépőktől azonosítót és egy titkos jelszót kér. Csak azok az emberek léphetnek az épületbe, akik mindkettővel rendelkeznek. De az emberek ha már bent vannak, azt csinálnak és oda mennek amit és ahova akarnak.

Ha valaki meghallja vagy tudja a titkos jelszót és használja a tulajdonosa helyett, a belépése ellen nincs védelem.

### 30-as szint: Jelszavas és erőforrás védelem

A 30-as szint adja mindazt, amit a 20-as tud, plusz Ön tudja irányítani, hogy kik mehetnek az épület bizonyos részeibe és mit csinálhatnak, ha ott vannak. Kijelölheti az épület néhány részét nyilvánosnak, míg más részeket korlátozottaknak, örökkel az ajtók előtt.

Engedélyezheti, hogy a korlátozott területeket elérők azt csinálhassák, amit akarnak, vagy kérheti, hogy igényeiket nyújtsák be az információjogosultság nyilvántartóhoz (programok). A betolakodó, aki valaki más jelszavát használja, még lehet, hogy el tudja érni a védett területeket az őrök mögött.

### 40-es szint: Integritás védelem

A 40-es szintnél mindazt megkapja, amit a 30-as szintnél, de a rendszer ellenőrzi a felhasználók hozzáférési jogát. Az épületen belül az ajtóknál álló őrök ellenőrzik a jelszavakat és beírják a naplóba a terembe belépő összes felhasználót.

### 50-es szint: Fejlett integritás védelem

Az 50-es szintnél az őrök olyan szigorú szabályokat alkalmaznak, amellyel megelőzhető a speciális tudással rendelkező személy bejutása a korlátozott részhez és ezáltal annak megsértése. Az őrök ehhez ellenőrzik az azonosságát annak, aki aláírja a naplót.

## Javaslatok

Az iSeries rendszert 40-es biztonsági szinttel szállítjuk. A 40-es biztonsági szint a legjobb választás a telepítések többségénél, akár szigorú, akár közepes vagy laza a biztonsági szabályzata. Ha laza megközelítést választ, beállíthatja a nyilvános elérést az erőforrások többségénél a rendszeren. Ha a 40-es biztonsági szintet a kezdetektől használja, a rendszer biztonsága rugalmasan fokozható a jövőben nem túl sok változtatással.

Ha alkalmazási programokat vásárol, győződjön meg róla, hogy a programok tesztelve vannak 40-es biztonsági szinttel. Néhány alkalmazás használ olyan műveletet, amely hibát okoz 40-es biztonsági szintnél. Ha az alkalmazások nem voltak tesztelve 40-es és 50-es szinttel, kezdjen 30-as szinttel. Használja az ellenőrzési napló funkciót az alkalmazások biztonsági hibáiról történt bejegyzések ellenőrzésére. Ha nincs bejegyzés, változtassa a szintet 40-re vagy 50-re.

Az 50-es szint olyan események megelőzésére szolgál, amely a rendszerek többségénél normális körülmények között nem történhet meg. A rendszer további ellenőrzést végez minden programfutásnál. Ez a további vizsgálat negatív hatással lehet a teljesítményre.

Miután beírta a kiválasztott biztonsági szintet a Rendszerváltozók kiválasztására szolgáló űrlapon, kiválaszthatja a bejelentkezést befolyásoló rendszerváltozókat.

## Bejelentkezést befolyásoló rendszerváltozók kiválasztása

Miután kiválasztotta a biztonsági szintet, a rendszerváltozókkal egyéniesítheti, hogy mit lássanak a felhasználók a képernyőn, és hogyan működjenek együtt a rendszerrel. Tervezze meg a rendszerváltozókat, és választásait írja le a Rendszerváltozók kiválasztására szolgáló űrlapon.

Az alábbi táblázat ismerteti a témakörben tárgyalt rendszerváltozókat.

11. táblázat: iSeries rendszerváltozók és leírásuk

Rendszerváltozó	Leírás
QMAXSIGN	Korlátozza az egymás után következő bejelentkezések számát.
QMAXSGNACN	Kijelöli azt a műveletet, amelyet a rendszer végrehajt, amikor az egymást követő bejelentkezések száma eléri a megadott értéket.
QLMTDEVSSN	Meghatározza azt, hogy a felhasználó bejelentkezhet-e egynél több munkaállomásról ugyanazzal a felhasználói profillal.
QINACTITV	Meghatározza, hogy mikor fog a rendszer műveletet végezni az inaktív jobokon.
QINACTMSGQ	Meghatározza a műveletet, amit a rendszer végrehajt, amikor a feladat a QINACTITV rendszerváltozóban megadott ideig inaktív állapotban van.
QDSCJOBITV	Vezérli, hogy az ideiglenesen felfüggesztett munkát a rendszer befejezze-e és mikor.
QLMTSECOFR	Egy adott eszközre korlátozza a biztonsági felelőst, akinek a rendszer összes objektumához jogosultsága van.

**Bejelentkezési kísérletek számának korlátozása (QMAXSIGN és QMAXSGNACN):** Két rendszerváltozó határozza meg a bejelentkezési kísérletek számát, ahányszor a felhasználó megpróbálhat bejelentkezni, és azt, hogy mit tegyen a rendszer a korlát elérésekor.

A Maximum sign on attempts (QMAXSIGN) rendszerváltozó korlátozza az egymás után következő érvénytelen bejelentkezési kísérletek számát, amelyet a rendszer még megenged, mielőtt bizonyos műveleteket elkezdene. Az érvénytelen bejelentkezési kísérletek azt jelentik, hogy valaki megpróbál használni egy adott felhasználói profilt érvénytelen jelszóval, vagy nem megfelelő jogosultsága van a munkaállomáshoz.

A Maximum sign on action (QMAXSGNACN) rendszerváltozó megmondja, hogy mit csináljon a rendszer, ha valaki túl sokszor próbált bejelentkezni egymásután. A lehetséges értékek:

- 1 További próbálkozások megelőzése az egységről. Ez az egység letiltását jelenti. Senki sem tud az egységről

mindaddig bejelentkezni, míg egy jogosult személy a WRKCFGSTS paranccsal az egységet újra nem aktivizálja. Ez az opció általában nem elégséges a védelemre, különösen akkor, ha a bejelentkezési kísérletek személyi számítógépről vagy távoli rendszerről történnek.

A rendszeroperátor vagy valaki az egységre vonatkozó \*USE jogosultsággal az egységet ismét engedélyezheti.

- 2 További próbálkozások megelőzése az egységről. Ez az egység letiltását jelenti. Senki sem képes a kísérletezett profillal mindaddig bejelentkezni, míg egy jogosult személy a Change User Profile (CHGUSRPRF) paranccsal a profilt nem engedélyezi újra.

A felhasználói profil engedélyezéséhez (az állapot megváltoztatásához) biztonsági adminisztrátornak kell lenni, és jogosultsággal kell rendelkezni a profil használatához.

- 3 Mind a profil, mind az egység letiltása.

### **Kockázatok és javaslatok**

Néhány bajkeverő élvezi a kihívást, hogy kitalálja a jelszavakat és feltörésükkel belépjen a rendszerbe. A bejelentkezési kísérletek számának korlátozásával csökkentheti sikerük esélyeit.

A Maximum not valid sign on (QMAXSIGN) rendszerváltozó határozza meg, hogy mennyi bejelentkezési kísérletet engedélyez. Állítsa elég magas értékre, kerülve a felhasználók kétségbeesését. Állítsa elég alacsonyra ahhoz, hogy észrevegye a túl figyelmetlen felhasználókat és erősen korlátozza a potenciális behatolók kísérletezgetését. A bejelentkezési kísérletek maximális számát állítsa 3 és 5 közé.

A maximum sign on action (QMAXSGNACN) ajánlott értéke 3, bár az eszköz és a felhasználói profil letiltása kényelmetlen lehet a felhasználóknak. Ha egy munkaállomás túlzottan eldugott helyen van, lehetőséget ad a behatolónak, hogy kipróbáljon számtalan különböző profil és jelszó kombinációt. Ha a rendszerben nincs olyan munkaállomás, amely elhelyezésénél fogva veszélyt jelent, feltételezhetően a felhasználói profil letiltása elégséges védelmet jelent.

Ellenőrizze a kitöltött Fizikai biztonság űrlapot. Ha vannak munkaállomásai távoli helyeken, illetve távoli felhasználói (olyan felhasználók, akik telefonvonalon vagy VPN kapcsolaton keresztül érik el a rendszert), esetleg még szigorúbban kívánja korlátozni a bejelentkezési kísérleteket. Adja meg a QMAXSIGN és a QMAXSGNACN változókra vonatkozó értékeit a Rendszerváltozók kiválasztására szolgáló űrlap második részében.

Hasznosnak veheti, ha áttekinthet egy példát, amely azt illusztrálja, hogy a rendszerváltozók együttműködésével hogyan korlátozhatja a bejelentkezési kísérleteket, mielőtt kiválasztaná azt a rendszerváltozót, amely egyidejűleg egy munkaállomásra korlátozza a felhasználókat.

*Példa: Bejelentkezési kísérletek korlátozása:* Sharon Jones a bejelentkezési kísérletek számát 3-ra (QMAXSIGN=3) korlátozta, és úgy döntött, hogy a korlát elérésekor mind a profil, mind az egység letiltásra kerül (QMAXSGNACN=3). Az alábbi események történhetnek meg, amikor a fenti értékeket eléri:

1. Roger kétszer tévesen adja meg a jelszavát.
2. A második kísérlet után figyelmeztető üzenet jelenik meg, hogy a következő sikertelen kísérlet esetén a profilja letiltásra kerül.
3. Még egy hibát követ el.
4. A rendszer letiltja a profilját és a munkaállomáson megszűnik a bejelentkezési képernyő. Ha Roger egy másik munkaállomáson próbál bejelentkezni, hibaüzenet fog megjelenni.
5. Most meg kell kérnie Sharont, hogy engedélyezze ismételten a profilját. Sharon vagy a rendszeroperátor kell ahhoz is, hogy Roger munkaállomása ismét engedélyezve legyen. Ha Roger nem emlékszik a jelszavára, Sharon adhat részére egy ideiglenest, melyet Roger a következő bejelentkezéskor meg tud változtatni.

A következőkben áttekintheti azt a rendszerváltozót, amely egyidőben egy munkaállomásra korlátozza a felhasználókat.



**Felhasználók korlátozása egyidőben egy munkaállomásra:** A limit device sessions (QLMTDEVSSN) rendszerváltozó határozza meg, hogy egy adott felhasználó egyidőben több munkaállomárról be tud-e jelentkezni. A lehetséges értékek:

- 0** A rendszer engedélyezi korlátlan számú felhasználónak a bejelentkezését egyidőben, ugyanazzal a profillal.
- 1** A felhasználói profil csak egy egységen engedélyezett egyidőben. A felhasználó több szekcióval is rendelkezhet ugyanazon az egységen.

### **Kockázatok és javaslatok**

Egyidőben egy munkaállomásra korlátozva a bejelentkezés lehetőségét jó módszernek tűnik a megfelelő biztonsági szokások eléréséhez. Hanyag biztonsági szokások növelik a biztonsági kockázatokat:

- Ha a felhasználók csak egy-egy egységet használhatnak, ez a tény elveszi a kedvüket az azonosító és a jelszó másokkal való megosztásától. Ha az emberek megosztják egymás között azonosítójaikat, elveszti a kontrollt és a számonkérhetőséget. A továbbiakban nem tudja megmondani, valójában ki milyen funkciókat hajtott végre a rendszerben.
- A felhasználóknak emlékezniük kell arra, hogy ki kell jelentkezniük a használt munkaállomárról, mielőtt egy másikhoz mennek. A bejelentkezve hagyott, de nem használt munkaállomások biztonsági kockázatot jelentenek.

A QLMTDEVSSN javasolt értéke 1, amely a felhasználók részére egy egységet engedélyez. Adjon minden felhasználónak egyedi azonosítót és jelszót megfelelő jogosultságokkal, majd korlátozza őket egy munkaállomás használatára egyidőben. Adja meg a QLMTDEVSSN változóra vonatkozó értékét a Rendszerváltozók kiválasztására szolgáló űrlap második részében.

Ezután elkezdheti az inaktív feladatokra vonatkozó rendszerváltozók tervezését.

**Inaktív feladatokra vonatkozó rendszerváltozók tervezése:** Három rendszerváltozó együttes munkája határozza meg a rendszer reakcióját, amikor a felhasználók elfelejtkeznek kijelentkezni a munkaállomárról.

#### **Inactive job time-out interval (QINACTITV)**

A QINACTITV rendszerváltozó határozza meg a rendszer reakciójának bekövetkeztét, ha a bejelentkezett munkaállomáson az időkorlát alatt semmilyen munka nem folyik.

**Megjegyzés:** Az **Inactive** állapot azt jelenti, hogy a felhasználó sem Enter-, sem funkcióbillentyűt nem nyomott le az időintervallum alatt.

#### **Inactive job message queue (QINACTMSGQ)**

A QINACTMSGQ rendszerváltozó határozza meg a rendszer reakcióját, ha a QINACTITV rendszerváltozó által definiált idő letelik. Ha az ENDJOB opciót választotta, a rendszer a QINACTITV időértéknél hosszabb ideig passzív munkákat befejezi. Ha a DSCJOB opciót választotta, a rendszer felfüggeszti a passzív munkákat. Ha megadja egy üzenetsor nevét, a rendszer figyelmeztető üzenetet küld oda, ha egy munka túl sokáig passzív.

Mikor a rendszer **felfüggeszt** egy munkát a munkaállomárról, az a munka ideiglenes szüneteltetését jelenti. A munkaállomás visszatér a bejelentkezési képernyőhöz. A rendszer akkor folytatja a felfüggesztett munkát, amikor ugyanaz a felhasználó ugyanazon a munkaállomáson ismét bejelentkezik.

#### **Disconnected job time-out interval (QDSCJOBITV)**

A QDSCJOBITV rendszerváltozó irányítja, hogy a felfüggesztett munkát a rendszer befejezze-e és mikor. A rendszer a munkákat automatikusan függeszti fel a QINACTITV és a QINACTMSGQ rendszerváltozók eredménye alapján. A felhasználók is kérhetik munkájuk ideiglenes felfüggesztését (szüneteltetését) az Operational Assistant\* menü megfelelő opciójával vagy a Disconnect Job (DSCJOB) paranccsal.

### **Kockázatok és javaslatok**

Ha Sharon elfelejti a kijelentkezést a munkaállomásáról, John odasétál és végrehajt egy olyan funkciót, amelyhez Sharon rendelkezik jogosultsággal.

Szabályozni kell az inaktív állomásokat különösen két okból:

- Szigorú biztonsági környezet megléte mellett a rendszeren bizalmas információk vannak tárolva.
- A munkaállomások olyan helyen vannak telepítve, ahol külső emberek könnyen hozzáférhetnek.

Normál munkavégzés során gyakran meg kell szakítani a munkánkat a munkaállomásokon. Előnyös, ha a három rendszerváltó együttes munkája következtében a normál megszakítások megengedettek, de a rendszerbiztonság védelme is megvalósul.

Az ilyen kockázatok kiküszöbölése érdekében az IBM az QINACTITV, a QINACTMSGQ és a QDSCJOBITV rendszerváltók együttes munkáját ajánlja, hogy a normál megszakítások megengedettek legyenek, de a rendszerbiztonság védelme is megvalósuljon.

**Inactive job time-out interval (QINACTITV):** Állítsa olyan kicsire az intervallumot, ami biztosítja a magára hagyott állomások észrevételét, de ne olyan rövidre, hogy kényelmetlen legyen a felhasználóknak. A javasolt beállítás 30 perc. Mikor egy munka 30 perccig passzív, a rendszer az Inactive job message queue (QINACTMSGQ) változóban megadott módon reagál.

**Inactive job message queue (QINACTMSGQ):** Válassza a job felfüggesztését. A rendszer felfüggeszti azokat a munkákat, amelyek az Inactive job time-out interval (QINACTITV) változóban megadott intervallumnál hosszabb ideig passzívak. A rendszer felfüggeszti a jobot és kijelentkezteti a képernyős állomást. Mikor ugyanaz a felhasználó ismét bejelentkezik, a munkája ott folytatódik, ahol abbahagyta.

Ez sokkal kényelmesebb a felhasználóknak, mivel a munkájuk csak felfüggesztésre kerül, nem pedig befejezésre. A passzív munkák felfüggesztése több védelmet jelent a rendszer számára, mint a munkák befejezése a tényleges végrehajtás előtt.

**Megjegyzés:** A rendszer nem tud minden jobot szüneteltetni. Ha a rendszer nem képes felfüggeszteni egy munkát, akkor valójában befejezi. Ez esetleg információ veszteséget okozhat. Érdemes a QINACTMSGQ beállításánál megadni a rendszeroperátor üzenetsorát üzenet küldése céljából.

**Disconnected job time-out interval (QDSCJOBITV):** Bízassa arra a rendszer felhasználókat, hogy ideiglenesen jelentkezzenek ki a rendszerről, amikor rövid időre el kell hagyniuk a munkaállomást, míg ha hosszabb időre kell elmenniük, fejezzék be a munkát és úgy jelentkezzenek ki.

Használja a QDSCJOBITV változót a felfüggesztett munkák befejezéséhez mielőtt a rendszer az éjszakai eljárásokat (pl. Automatic Cleanup) elkezdene. Állítsa olyan nagyra, hogy a felhasználó a munkaidőn belül visszatérhessen a munkaállomáshoz, de elég rövidre ahhoz, hogy a munkák véget érjenek az éjszakai eljárások előtt. Válassza a 300 perces (öt órás) intervallumot, ami elegendő időt ad az éjszakai feldolgozások befejezéséhez anélkül, hogy zavarná a felhasználói jobokat.

**Megjegyzés:** Annak megelőzésére, hogy két felhasználó egyidőben ugyanazt az információt módosítsa, a rendszer **zárolja** a rekordot a módosítás előtt. Az erőforrások zárolása fennmarad a felhasználói munka felfüggesztése idejére is. Az alkalmazás kivételétől és a rendszer felhasználóinak számától függően, a zárolások okozhatnak teljesítmény problémát a rendszeren. Ellenőrizze a programozókkal vagy az alkalmazás szállítójával, hogy befolyásolja-e a zárolás a teljesítményt.

Szándékában állhat áttekinteni egy példán a fenti rendszerváltók együttes munkáját, ami kezeli az inaktív jobokat a rendszeren.

Miután leírta az inaktív jobokra vonatkozó döntését a Rendszerváltók kiválasztására szolgáló űrlapon, eldöntheti, hogyan korlátozza a biztonsági felelős bejelentkezését.

*Példa: Inaktív feladatok kezelése a QINACTITV, QINACTMSGQ és QDSCJOBITV rendszerváltókkal:* Tétélezzük fel, hogy az inaktív feladatok időkorlátja (QINACTITV) 30 percre van beállítva. A rendszer felfüggeszti az inaktív feladatokat (QINACTMSGQ rendszerváltó beállítása DSCJOB). A QDSCJOBITV 300 percre (5 órára) van beállítva. Például, ha Sharon elfelejt kilépni délelőtt 9:30-kor, a rendszer felfüggeszti munkájának futását délelőtt 10:00-kor, és befejezi délután 3:00-kor.

Adja meg saját választását a QINACTITV, QINACTMSGQ és QDSCJOBITV rendszerváltóokra a Rendszerváltók kiválasztására szolgáló űrlap második részében.

Miután leírta döntését a Rendszerváltók kiválasztására szolgáló űrlapon, döntse el, hogyan korlátozza azt, honnan jelentkezessen be a biztonsági felelős.

**A biztonsági felelős bejelentkezésének korlátozása:** Esetleg bizonyos munkaállomásokra kívánja korlátozni azoknak a felhasználóknak a bejelentkezését, akik jogosultak a biztonság és a vezérlő objektumok megváltoztatására. Ezzel megakadályozza, hogy ezek a felhasználók bejelentkezzenek távoli helyen lévő munkaállomásokról az Ön tudta nélkül. A QLMTSECOFR rendszerváltó (limit security officer) engedélyezi ezt a lehetőséget. A QLMTSECOFR változót 1-be állítva, az (\*ALLOBJ) vagy (\*SERVICE) speciális jogosultságú személy csak a konzolon vagy egy kijelölt másik munkaállomáson jelentkezhet be.

QLMTSECOFR a konzolhoz korlátozza a biztonsági felelőst, a szerviz szakembert és a speciális jogosultságú felhasználókat. A Grant Object Authority (GRTOBJAUT) parancs segítségével adhat elérést más eszközökhöz az ilyen felhasználóknak.

**Megjegyzés:** A QLMTSECOFR rendszerváltó működéséhez 30-as vagy magasabb biztonsági szint kell a rendszeren.

### **Kockázatok és javaslatok**

A QLMTSECOFR rendszerváltót 1 értékre kell beállítani. Ha valaki meghallja vagy kitalálja a biztonsági felelős jogosultságaival rendelkező személy jelszavát, ahhoz az eszközökhöz is hozzá kell férnie, amelyről az ilyen felhasználók bejelentkezhetnek.

Miután kitöltötte a QLMTSECOFR változóra vonatkozó választását a Rendszerváltók kiválasztására szolgáló űrlap második részében, kiválaszthatja a jelszavakat befolyásoló rendszerváltókat.

### **Jelszavakat befolyásoló rendszerváltók kiválasztása**

Inkább hagyja, hogy a jelszavakat a felhasználók maguk hozzák létre, mintsem a biztonsági felelős adjon nekik jelszót. Ha maguk hozzák létre a jelszavakat, várhatóan nem kell leírniuk. A leírt jelszavak kézenfekvő helyen való tárolása biztonsági kockázatot jelent.

### **Ötletek jelszavak létrehozásához**

A felhasználók gondban lehetnek a megfelelő jelszó kitalálásakor. Javasoljuk a következő technikát: Segítségképpen vegyünk egy könnyen eszünkbe jutó mondatot nehezen kitalálható jelszó létrehozásához. Például, nyaralás után használhatja a "Július 4-i hal rossz volt" mondatot a J4HRV jelszó képzéséhez.

Néhány rendszerváltó szabályozza a jelszavakat. Be tudja állítani, hogy a felhasználóknak milyen gyakran kell cserélni jelszavaikat. Ön is alkothat sok szabályt a könnyen kitalálható jelszavak használatának megelőzésére. Ezen rendszerváltók többsége nagy szervezetek számára fontos. Kevesebb része pedig mindenki számára.

Az ASSIST menü opciójának, vagy a Change Password (CHGPWD) parancs használatával a felhasználók létrehozhatják jelszavaikat. Mikor a felhasználók cserélik jelszavaikat, a rendszer ellenőrzi az új jelszót a rendszerváltók előírása szerint. Ha a felhasználó a CHGUSRPRF paranccsal módosította jelszavát, a rendszer nem ellenőrzi az új jelszót a rendszerváltókhöz viszonyítva.

**Megjegyzés:** Ha beállította a jelszavakat befolyásoló rendszerváltókat, a rendszer nem engedi a felhasználói profillal azonos jelszót, hacsak a CHGUSRPRF paranccsal be nem állítja.

A táblázat a jelszavakat befolyásoló rendszerváltozókat és meghatározásaikat mutatja:

12. táblázat: iSeries jelszavakkal kapcsolatos rendszerváltozók

Rendszerváltozó	Leírás
QPWDEXPITV	Megköveteli a felhasználóktól, hogy megadott idő után változtassák meg jelszavaikat.
QPWDMAXLEN	Lehetővé teszi, hogy megadja a jelszavak maximális karakterhosszát.
QPWDMINLEN	Lehetővé teszi, hogy megadja a jelszavak minimális karakterhosszát.
QPWDRQDDIF	Megakadályozza, hogy a felhasználók két különböző jelszót változtassanak.

A jelszavakkal kapcsolatos rendszerváltozókról az alábbi témakörök szolgálnak további részletekkel:

- Jelszó élettartam meghatározása
- Jelszavak hosszának meghatározása
- Ismétlődő jelszavak korlátozása

A WRKSYSVAL \*SEC parancs begépelésével megnézheti a rendszerváltozókra vonatkozó online segítséget a QPWD karakterekkel kezdődően.

**Jelszó élettartam meghatározása:** A QPWDEXPITV rendszerváltozó határozza meg a felhasználóktól megkívánt jelszócsere gyakoriságát.

A rendszer figyelmezteti a felhasználókat a jelszólejárati naphoz közeledve. Ha a jelszó lejár, a rendszer kérni fogja a felhasználót a következő bejelentkezéskor, hogy változtassa meg jelszavát.

### Javaslatok

A felhasználók szabályos időközönként változtassák meg jelszavaikat. Ez kedvét szegi a jelszavakat megosztani kívánó felhasználóknak. Mint ahogy azon jogosulatlan felhasználóknak is, akik mások jelszavát megtanulva akarják azt felhasználni. A jelszó élettartama legyen elég hosszú, hogy ne irritálja a felhasználókat, de legyen elég rövid a megfelelő biztonság garantálásához. Az ilyen problémák elkerülése érdekében állítson be 45 - 60 napos periódust.

Miután leírta a QPWDEXPITV rendszerváltozóra vonatkozó értékét a Rendszerváltozók kiválasztására szolgáló űrlapon, meghatározhatja a jelszavak hosszát.

**Jelszavak hosszának meghatározása:** Több felhasználó nem szívesen gépel. Ha hagyja őket, egybetűs vagy kezdőbetűikből álló jelszavakat fognak választani. Sajnos a rövid jelszavak megkönnyítik a behatolónak a sikeres kitalálást. A QPWDMINLEN rendszerváltozó meghatározza az összes jelszó minimális hosszát.

Ha a rendszere kommunikál más rendszerekkel is, a felhasználók kicserélhetik a jelszavakat a két számítógép között. Néhány kommunikációs módszer a jelszavakat maximum 8 karakterre korlátozza. A QPWDMAXLEN rendszerváltozó lehetővé teszi, hogy meghatározza a jelszavak maximális hosszát.

### Javaslatok

A jelszó minimális hosszát állítsa 6-ra. Ez megszünteti a kezdőbetűk használatát és több kreativitásra sarkallja a felhasználókat a jelszó kialakításakor. Állítsa a jelszó maximális hosszát 8-ra, ha rendszere más rendszerekkel is kommunikál.

Miután leírta a QPWDMINLEN és a QPWDMAXLEN rendszerváltozókra vonatkozó értékeit a Rendszerváltozók kiválasztására szolgáló űrlap második részében, elhatározhatja mennyire korlátozza a jelszavak ismétlődését.

**Ismétlődő jelszavak korlátozása:** A Change Password (CHGPWD) parancs megköveteli, hogy az új jelszó eltérjen a régítől. Azonban, egy felhasználó cserélgethet két jelszót egymás között oda-vissza mindaddig, míg a QPWDRQDDIF rendszerváltó használataival meg nem előzi ezt. Az alábbi táblázat bemutatja a lehetséges választásokat a QPWDRQDDIF rendszerváltóra:

13. táblázat: QPDRQDDIF rendszerváltó értékei

Érték	Ismétlődésre ellenőrzött jelszavak száma
0	0 Ismétlődő jelszavak engedélyezve vannak.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

### Javaslatok

Használja a jelszó lejáratási intervallumot és az ismétlődő jelszó értéket az egy évre szükséges egyedi jelszavak definiálásához. Például, ha a jelszavak 60 nap alatt járnak le, akkor QPWDRQDDIF értékének válassza a 7-et.

Miután leírta a QPWDRQDDIF rendszerváltóra vonatkozó értékét a Rendszerváltók kiválasztására szolgáló űrlap második részében, elhatározhatja hogyan használja fel a rendszerváltókat a rendszer egyéniesítéséhez.

### Rendszer egyéniesítése rendszerváltókkal

Az iSeries rendszernek vannak olyan rendszerváltói és hálózati tulajdonságai, amelyek számtalan dolgot jobban irányítanak, mint a biztonságot. A rendszer- és alkalmazás programozók használják az ilyen rendszerváltók és tulajdonságok többségét. A biztonsági felelős csak kevés rendszerváltó és hálózati attribútum beállítását végzi az egyéniesítés folyamán.

### Rendszer névadás

Használja a SYSNAME hálózati tulajdonságot a rendszernev hozzárendelésére. A rendszernev a bejelentkezési képernyő és a rendszerriportok jobb felső sarkában látható. A rendszernev lesz használva akkor is, ha a rendszer egy másik rendszerrel, vagy iSeries Access for Windows révén személyi számítógéppel kommunikál.

Mikor a rendszer más rendszerekkel vagy személyi számítógépekkel kommunikál, a rendszernev azonosítja és megkülönbözteti a rendszert a hálózat többi rendszerétől. A számítógépek minden kapcsolatfelvételkor kicserélik azonosítóikat. Ha egyszer hozzárendelt nevet, ne változtassa, mert a változás hatással van a hálózat többi rendszerére is.

### Javaslatok

Válasszon értelmes és egyedi nevet a rendszernek. Még ha most nem is kommunikál más számítógépekkel, később szándékában állhat. Ha a rendszere egy hálózat része, feltehetően a hálózati menedzser fogja megmondani milyen rendszernevet adjon neki.

Például, a JKL Toy Company esetében Sharon Jones a JKLTOY nevet választotta a rendszernek.

### Dátum és idő kijelzése a rendszeren

Beállíthatja az év, hónap, nap sorrendjét, mikor dátumot jelenít meg képernyőn, vagy mikor kinyomtatja. Ugyancsak definiálhatja a köztük lévő elválasztó karaktert.

A QDATFMT rendszerváltozó határozza meg a dátum formátumát. A következő ábra mutatja be 2000. június 16-i időpont nyomtatási eredményeit a különböző választási lehetőségek esetén:

14. táblázat: QDATFMT (System Date formats)

Saját választás	Leírás	Eredmény
YMD	Év, Hónap, Nap	00/06/16
MDY	Hónap, Nap, Év	06/16/00
DMY	Nap, Hónap, Év	16/06/00
JUL	Julián féle dátum	00/168

**Megjegyzés:** A fenti példákban a dátumelválasztó karakter a "slash" (/).

A QDATSEP határozza meg a dátumelválasztó karaktert az év, hónap, nap között. Az alábbi táblázat a választásait mutatja. Választását számmal tudja azonosítani:

15. táblázat: QDATSEP (System Date Separator)

Elválasztó karakter	QDATSEP érték	Eredmény
/ (per)	1	16/06/00
- (kötőjel)	2	16-06-00
. (pont)	3	16.06.00
, (vessző)	4	16,06,00
(üres)	5	16 06 00

**Megjegyzés:** A fenti példák a DMY dátumformátumot használják.

A QTIMSEP rendszerváltozó meghatározza az óra, perc, másodperc elválasztására szolgáló karaktert az idő megjelenítésekor. Választását számmal tudja azonosítani. A lenti táblázat bemutatja a délelőtti 10:30 időpont megjelenítését különböző választás esetén:

16. táblázat: QTIMSEP (System Time Separator)

Elválasztó karakter	QTIMSEP	Eredmény
: (kettőspont)	1	10:30:00
. (pont)	2	10.30.00
, (vessző)	3	10,30,00
(üres)	4	10 30 00

## Döntés a rendszeregységek elnevezéséről

A rendszer automatikusan konfigurálja az új megjelenítő állomásokat és nyomtatókat, amit hozzákapcsol. A rendszer nevet ad minden új egységnek. A QDEVNAMING rendszerváltozó determinálja a nevek hozzárendelését. Az alábbi ábra mutatja be a nevek hozzárendelését harmadik megjelenítő állomás és második nyomtató csatlakoztatásakor:

17. táblázat: Rendszeregység elnevezése

Saját választás	Elnevezési formátum	Megjelenítő állomás neve	Nyomtató neve
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Egység címe	DSP010003	PRT010002

**Megjegyzés:** A fenti példában mindkét periféria az első kábelhez csatlakozott.

## Javaslatok

Alkalmazza az iSeries elnevezési szabályokat, ha csak nem futtat olyan szoftvert, amely S/36 elnevezést igényel. Az iSeries megjelenítő állomás- és nyomtatónévek kevésbé kényelmetlenek, mint az egység címét igénylő elnevezések. A megjelenítő állomás és a nyomtató neve néhány Operational Assistant képernyőn tűnik fel. A nyomtatónévek a nyomtatott listák menedzselésénél kerülnek felhasználásra.

Miután a rendszer konfigurálta az új egységet, használja a Change Display Device (CHGDEVDS) parancsot, vagy a Change Printer Device (CHGDEVPR) parancsot az egység értelmes leírásának beviteléhez. A leírásba beletartozik mind a fizikai cím, mind a fizikai hely, úgymint *John Smith iroda, vonal 1 cím 6*.

## Rendszernyomtató kiválasztása

Használja a QPRTDEV rendszerváltozót a rendszernyomtató kijelölésére. A rendszerváltozó, a felhasználói profil és a jobleírás együttesen határozza meg, hogy a job melyik nyomtatót használja. A job a rendszernyomtatót használja, ha csak a felhasználói profil vagy a jobleírás ki nem jelöl egy másikat.

## Javaslatok

Normál esetben a rendszer leggyorsabb nyomtatója a rendszernyomtató. A rendszernyomtató hosszú listák és rendszeradatok kinyomtatására szolgál.

**Megjegyzés:** Nem tudja a nyomtatók neveit addig, amíg nem telepíti és konfigurálja a rendszert. Jegyezze fel a rendszernyomtató helyét. Töltse ki a nyomtatónévet később.

## Nyomtatott anyagok listájának megjelenítése

A rendszer lehetőséget ad a felhasználók nyomtatott listáinak nyomon követésére. A Work with Printer Output képernyő mutatja az összes nyomtatás alatt lévő vagy arra váró listát. Ugyancsak engedélyezheti a már kinyomtatott listák megjelenítését is. Ez a képernyő mutatja meg a kinyomtatott listát és azt, hogy melyik nyomtatón lett kinyomtatva. Ez nagyon hasznos az elveszett riportok fellelése végett.

A kinyomtatott listák megjeleníthetők a munka felügyelő funkció és a QACGLVL rendszerváltozó segítségével. A QACGLVL változó \*PRINT opciója biztosítja a kinyomtatott lista tárolását.

## Javaslatok

A kinyomtatott listák tárolása tárolókapacitást igényel. Ameddig a felhasználók nem nyomtatnak sok riportot, feltehetően, ezt a funkciót nem kell használni. Írjon NEM-et a Rendszerváltozók kiválasztására szolgáló űrlapon. Ez beállítja a munka felügyelő szintet \*NONE értékre.

- Győződjön meg róla, hogy elkészítette a cégére vonatkozó saját biztonsági szabályzatot, hasonlóan a Sharon Jones és John Smith által a JKL Toy Company számára írt példához.
- Győződjön meg róla, hogy leírta a rendszerváltozókra vonatkozó választásait a Rendszerváltozók kiválasztására szolgáló űrlapon.
- Írja le a biztonsági feljegyzésbe beépítendő gondolatokat.

Miután beírta az összes rendszerbeállítást a Rendszerváltozók kiválasztására szolgáló űrlapon, és megírta a biztonsági szabályokat, megtervezheti a felhasználói csoportokat.

**Példa: JKL Toy Company Biztonsági szabályzat:** Az alábbi feljegyzés illusztrálja azokat a biztonsági szabályokat, amelyeket John Smith, a JKL Toy Company elnöke adott ki az alkalmazottaknak. Felhasználta azokat a megjegyzéseket is, amelyeket ő és Sharon készített a biztonsági szabályzat kialakításakor.

18. táblázat: Példa: JKL Toy Company Biztonsági szabályzat

Kiadja: John Smith, Elnök
---------------------------

<b>JKL Toy Company</b>	
Címzettek:	JKL Toy Company összes alkalmazottja
Tárgy:	Az új rendszer biztonsága
<p>Mindannyian részt vettek az új rendszerről szóló tájékoztató megbeszélésen. A rendszer felhasználóinak kiképzése elkezdődött és a vevő rendelések gépi feldolgozása is a jövő héten indul. Úgy ítéljük meg, hogy a rendszer már a közeljövőben üzleti sikereink meghatározó elemévé válik.</p> <p>Ismertetem az új rendszerre vonatkozó biztonsági előírásokat és döntéseket, továbbá kiemelem fontosságukat. Ezeket az előírásokat üzleti tevékenységünk fontos információinak megvédése érdekében adom ki.</p> <ul style="list-style-type: none"><li>• Sharon Jones fog felelni a rendszer biztonságáért. Helyettese Ken Harrison lesz. Velük vegye fel a kapcsolatot, ha bármilyen kérdése van, vagy biztonsági problémákat gyanít.</li><li>• A rendszerfunkciókat végrehajtó személyekről szóló döntéseinket az információ kezeléssel kapcsolatos jelenlegi szabályaink alapozták meg. Például:<ul style="list-style-type: none"><li>– A szerződés- és speciális ár információk bizalmas adatoknak minősülnek. Ezeket nem szabad felfedni cégen kívüli személy előtt.</li><li>– Csak a számviteli részleg állíthatja be és módosíthatja ügyfeleink számlalimitjét.</li></ul></li><li>• Mindenki, akinek használnia kell a rendszert, kapni fog egy felhasználói azonosítót és egy jelszót. A jelszó módosítását az első bejelentkezéskor, majd azt követően hatvan naponként igényli a rendszer. Válasszon olyan jelszót, amelyet könnyen megjegyez, de ne legyen nyilvánvaló. A felhasználói azonosító mellé adott űrlapon talál néhány jó tanácsot a jelszó létrehozásához.</li><li>• <i>Jelszavát ne ossza meg senkivel.</i> Mindenki képes lesz a munkájához szükséges összes gépi művelet elvégzésére. Ha szüksége van valamilyen információ elérésére, lépjen kapcsolatba Sharon vagy Ken kollégával. Ha elfelejti jelszavát, Sharon vagy Ken azonnal újat tud beállítani a részére. Senkinek sem lehet semmi oka arra, hogy más azonosítóját és jelszavát használja a bejelentkezéshez.</li><li>• Megtanulhatta a tárolás és visszajátszás funkció használatát munkaállomásán a gépelés csökkentése végett. <i>Ne használja</i> ezt a funkciót a jelszó tárolásához.</li><li>• Ne hagyja a munkaállomását bejelentkezve, mikor távozik asztalától. A kiképzés során megtanulta, hogyan kell ideiglenesen kijelentkezni a munkaállomáson. Használja ezt a funkciót, ha rövid időre kell elhagynia asztalát. Ha hosszabb időszakra távozik, fejezze be a munkáját és használja a szabályos kijelentkezést.<p>A munkaállomás elhagyásakor történő kijelentkezés különösen fontos azokon a helyszíneken, amelyek nagy nyilvánosság számára elérhetők, mint például a raktár rakodási területe, ügyfélszolgálat területe, és a távoli üzlethelyiség.</p></li><li>• Habár a rendszeregység nagyon szilárd, ütögetése és a tetejére pakolás kerülendő. Az egység vezérlőpultja normál esetben nem aktív, ne tapogassa. A számviteli osztály dolgozói felelnek annak biztosításáért, hogy senki ne kontárokodhasson bele a rendszeregységbe.</li></ul> <p>Emlékezzen mindig rá, hogy az új rendszer célja munkánk könnyítése és üzleti teljesítményünk fokozása. Biztonsági előírásaink munkáját segítik és nem hátráltatják. Ha kérdése, vagy javaslata van, azonnal vegye fel a kapcsolatot Sharon vagy Ken kollégákkal, illetve velem.</p>	

Miután elkészítette saját biztonsági irányelveinek vázlatát, elkezdheti a felhasználói csoportok tervezését.

## Felhasználói csoportok tervezése

A tervezési folyamat első lépése biztonsági stratégia eldöntése, mely a vállalati biztonsági szabályzatban realizálódik. Most készen állunk a felhasználói csoportok kialakítására, mely a gyakorlatban az osztály szabályzataként ismert.

### Mi a felhasználói csoport?

A felhasználó csoport értelmét a neve hüen kifejezi: emberek olyan csoportja, akiknek ugyanazokat az alkalmazásokat, ugyanazon a módon kell használniuk. Egy felhasználói csoport tipikusan ugyanazon osztály dolgozóiból áll össze, akik hasonló feladatokért felelősek. Egy felhasználói csoportot csoportprofil létrehozásával definiálhat.

### Mit csinál a csoportprofil?



A csoportprofil két célt szolgál a rendszeren:

- **Biztonsági eszköz:** A csoportprofil egyszerű módot biztosít annak megszervezéséhez, hogy bizonyos objektumokat ki használhat a rendszeren (objektum jogosultság). Sokkal egyszerűbben definiálhat objektum jogosultságot az egész csoportra, mint a csoport egyes tagjaira külön-külön.
- **Egyéniesítő eszköz:** A csoportprofil mintaként használhatja egyedi felhasználói profilok létrehozásához. Egyazon csoport legtöbb tagjának ugyanazok az egyéniesítési igényei, mint például kezdeti menü, vagy alapértelmezett nyomtató. Mindezeket definiálhatja a csoportprofilban és csak másolni kell az egyedi felhasználói profilokba.

A csoportprofilok könnyebbé teszik az egyszerű, konzisztens séma kialakítását mind a biztonsághoz, mind az egyéniesítéshez.

### Milyen űrlapra van szükség?

A felhasználói csoportok tervezéséhez ezek az űrlapok szükségesek:

- Felhasználói csoportot azonosító űrlap
- Felhasználói csoportot leíró űrlap

**Megjegyzés:** Minden egyes felhasználói csoportra kell egy Felhasználói csoportot leíró űrlap.

Az űrlapok kitöltéséhez nézze át a következő témaköröket:

- Felhasználói csoportok azonosítása.
- Csoportprofilok tervezése.
- Bejelentkezést befolyásoló rendszerváltozók kiválasztása.
- Felhasználó tevékenységét korlátozó értékek kiválasztása.
- Felhasználói környezetet beállító értékek kiválasztása.

### Felhasználói csoportok azonosítása

Amikor tervezi felhasználói csoportjait, először állítsa össze a csoportokat a rendszeren. Ez lehetővé teszi, hogy megtervezze a csoportok számára szükséges erőforrásokat. Próbáljon meg egyszerű eljárást alkalmazni felhasználói csoportjainak kialakítására. Gondoljon az osztályokra, vagy munkacsoportokra, akik a terv szerint használni fogják a rendszert. Nézze át az alkalmazási diagramot, amelyet korábban készített alkalmazásairól. Vegye figyelembe az alkalmazások és a munkacsoportok közötti természetes kapcsolatokat:

- Betud azonosítani elsődleges alkalmazást minden munkacsoportnak?
- Ismeri minden csoport alkalmazási igényét? Melyik alkalmazásokra nincs szükségük?
- Megtudja-e mondani, melyik csoport legyen az egyes alkalmazási könyvtárak információinak gazdája?

Ha "Igen" választ tud adni a kérdésekre, elkezdheti a felhasználói csoportok tervezését. Ha csak "talán" vagy "lehet" válaszokat tud adni, akkor hasznosnak ítélni a felhasználói csoportok azonosításának módszeres megközelítését.

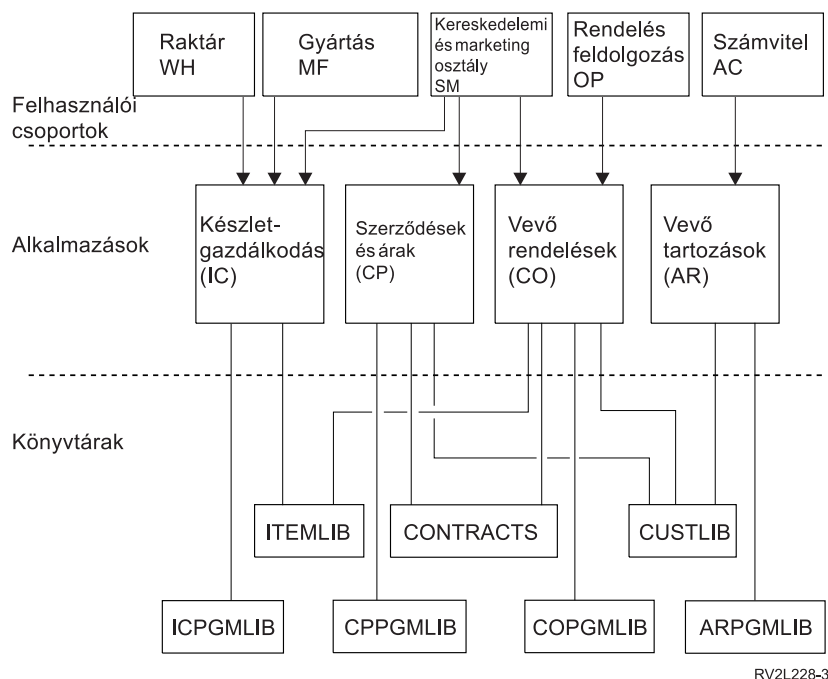
Szándékában állhat, hogy inkább egy példán tekintené át a felhasználói csoportok kialakításának módszerét.

**Megjegyzés:** A biztonság felügyeletét egyszerűsíti, ha minden felhasználó csak egy csoportprofilnak tagja. Habár, néhány esetben előnyösebb, ha a felhasználók egyszerre több csoportprofilhoz tartoznak.

Sokszor könnyebb felügyelni a több csoportprofilhoz tartozó felhasználókat, mintha az egyedi profiloknak kellene különböző magán-jogosultságokat adni.

**Példa: Felhasználói csoportok azonosítása:** Ha az alkalmazások és a munkacsoportok közötti kapcsolatok bonyolultak vagy tisztázatlanok, használja a Felhasználói csoportot azonosító űrlaphoz hasonló mátrix technikát a dolgok tisztázására. A rendszerfelhasználók és alkalmazási igényeik megszerkesztéséhez egy mátrixra van szüksége - nézzen meg hasonló, felmerült mintákat. A felhasználói csoportot azonosító űrlap kitöltésén túlmenően Sharon Jones felhasználta saját alkalmazási diagramját is ahhoz, hogy meghatározza, mely felhasználói csoportoknak kell elérniük az alkalmazásokat.

Az alábbi ábra szemlélteti a JKL Toy Company alkalmazási diagramját.



Ha laza biztonsági környezetet céltott meg, egy X-el jelölje, hogy a felhasználónak kell alkalmazás. Ha korlátozott környezetet céltott meg, vegye figyelembe hogyan használják az emberek az alkalmazásokat. Jobb, ha X helyett V (view) jelzést használ, ha valakinek csak megtekinteni kell az alkalmazás információit. Használja a C (change) jelzést, ha valakinek változtatnia kell az információt. Használja az O (owner) jelzést, ha valaki az adott információknak elsődleges felelőse.

Például a JKL Toy Company esetében különböző csoportok használják a "Szerződések és árak" alkalmazást:

- A Kereskedelmi és Marketing osztály képi az árakat és köti a vásárlói szerződéseket. Ők a *gazdái (own)* a "Szerződések és árak" alkalmazás információinak.
- Az ügyfélrendelések osztály indirekt úton módosítja a szerződési információkat. Mikor egy rendelést elfogadnak, a szerződésben lévő mennyiséget megváltoztatják. Ők *változtatják (change)* a "Szerződések és árak" információit.
- A rendelésfeldolgozás embereinek csak megtekinteni kell a számla-limit értékeket munkájuk tervezéséhez, de nem változtathatják meg azokat. Nekik csak *látni (view)* kell a számla-limit fájlt.

19. táblázat: JKL Toy Company Felhasználói csoportot azonosító űrlap - példa

Felhasználói csoportot azonosító űrlap					
Készítette: Sharon Jones			Dátum: 9/2/99		
Alkalmazások elérési módja					
Felhasználó neve	Osztály	Alk: CO	Alk: IC	Alk: PC	Alk: AR
Ken H.	Rendelés feldolgozás (OP)	O	C	C	C
Karen R.	Rendelés feldolgozás (OP)	O	C	C	C
Kris T.	Számvitel (AC)	V		V	O
Sandy J.	Számvitel (AC)	V	C	V	O
Peter D.	Számvitel (AC)	C		V	O
Ray W.	Raktár (WH)	V	O	V	
Rose Q.	Raktár (WH)	V	O	V	

19. táblázat: JKL Toy Company Felhasználói csoportot azonosító űrlap - példa (Folytatás)

Roger T.	Kereskedelmi és marketing oszt. (SM)	C	C	O	C
Sharon J.	Menedzserek (MG)	C	C	C	C
<p><b>Megjegyzés:</b></p> <ul style="list-style-type: none"> <li>Ha biztonsági környezete <i>laza</i>, jelölje X betűvel mely alkalmazásokat igénylik a felhasználók.</li> <li>Ha biztonsági környezete <i>átlagos</i>, jelölje meg A betűvel, hogy mely felhasználóknak lesz jogosultsága mely alkalmazásokhoz.</li> <li>Ha biztonsági környezete <i>korlátozott</i>, használja a C (change), a V (view) és az O jelölést arra, hogy a felhasználók <i>hogyan</i> használják az alkalmazást.</li> </ul>					

Sharon Jones a mátrix készítésekor az alábbi megjegyzéseket fűzte döntéséhez:

- Az OP és az AC osztályok háttérrel biztosítanak egymásnak. Ezért ma még hasonló alkalmazásokat igényelnek. Azonban, előbb-utóbb külön csoportokká válnak, amikor létszámnövekedés folytán tevékenységük tovább specializálódik.
- Annak ellenére, hogy az OP osztály közvetlenül nem változtathatja meg a készlet- és szerződési információkat, a változások automatikusan megtörténnek, amikor felviszik a rendeléseket. Szükség van-e biztonsági intézkedésre később?
- Az SM dolgozói minden alkalmazásba és az üzletmenet minden részébe be vannak vonva. Ők állítják össze az árakat és a termékleírásokat. Ők állítják össze az ügyfelek listáját, míg az AC osztály a számla-limiteket. Ők a felelősek az összes szerződési feltételért és az áráért.

Döntsön arról, hogyan kerüljenek a felhasználók csoportokba. Töltse ki a Felhasználói csoportot azonosító űrlapot, ha segítségre van szüksége a döntéshez.

Miután felvitte a felhasználókat a Felhasználói csoportot azonosító űrlapra, megtervezheti a csoportprofil.

## A csoportprofil tervezése

Ha egyszer meghatározta a felhasználói csoportokat, készen áll az egyes csoportok profiljainak megtervezésére. Sok döntés hatással van mind a biztonságra, mind az egyéniesítésre. Például, mikor egy kezdeti menüt definiál, lehet, hogy korlátoz egy felhasználót éppen ehhez a menühöz. De, ugyanakkor biztos lehet benne, hogy a felhasználó a megfelelő menüt látja a bejelentkezést követően.

Példaként készítsen elő egy Felhasználói csoportot leíró űrlapot egy felhasználói csoportra. Az első űrlap végén térjen vissza és töltse ki az űrlapot a többi csoportra is, amelyekre szükséges.

Az iSeries rendszer biztonsága és egyéniesítése a tervezés folytán nagyfokú rugalmasságot mutat. Az itt leírt módszer jó megoldást jelent a csoportprofilok és a jobleírások tervezéséhez, de programozója vagy alkalmazás szolgáltatója javasolhat más módszert is.

## Csoportprofilok elnevezése

Mivel a csoportprofil egy speciális típusú felhasználói profil, szándékában állhat könnyebben kialakítani a csoportprofilokat listákon és megjelenítőkön. Speciális neveket rendeljen hozzájuk. A csoportprofilok együttes megjelenítése érdekében a nevüknek ugyanazon betűkkel kellene kezdődnie, úgymint csoport GRP (group esetén) vagy osztály DPT (department esetén). Az alábbi irányelveket kövesse a felhasználói csoportok elnevezésekor:

- A csoport neve legfeljebb 10 karakter hosszú lehet.
- A név tartalmazhat betűket, számokat, speciális karaktereket: pound (#), dollar (\$), underline (\_).
- A név nem kezdődhet számmal.

**Megjegyzés:** A rendszer hozzárendel egy azonosító számot (*gid*) minden egyes csoportprofilhoz. Normál esetben hagyhatja, hogy a *gid* értéket a rendszer generálja. Azonban ha a rendszer hálózatban működik, lehet, hogy Önnek kell hozzárendelnie a meghatározott *gid* azonosítókat a csoportprofilokhoz. Egyeztessen a hálózati adminisztrátorral, hogy kell-e *gid* azonosítókat hozzárendelnie vagy sem.

Adja meg a csoportprofilokra vonatkozó elnevezési szabályát az Elnevezési szabályok űrlap megfelelő mezőjében. Például, Sharon Jones a DPT betűket választotta a csoportprofilok elnevezéséhez. Kitöltötte az Elnevezési szabályok űrlap megfelelő szekcióját.

20. táblázat: JKL Toy Company Elnevezési szabályok űrlap: csoportprofil példa

Objektum típusa	Elnevezési szabályok
Csoportprofilok	Használja a DPT karaktereket, majd az osztály nevének rövidítését. A csoportprofil leíró (description) mezője az osztály nevét tartalmazza.

### Felhasználói csoportok számára szükséges alkalmazások és könyvtárak meghatározása

Ha még nem tette volna meg, adja hozzá felhasználó csoportjait az alkalmazás diagramhoz és a könyvtárakhoz. Ez a vizuális kép segítséget nyújt az egyes csoportok számára szükséges erőforrások és alkalmazások eldöntéséhez.

A Felhasználói csoportot leíró űrlap első részében jelezhető a csoport elsődleges alkalmazása, amelyet a leggyakrabban használ. Készítsen listát a csoport egyéb alkalmazási igényéről.

Nézze meg az Alkalmazásokat leíró űrlapokat és a diagramot az egyes csoportok számára szükséges könyvtárak definiálásához. A könyvtárak legjobb elérési módszerének megtalálása érdekében konzultáljon a programozókkal vagy az alkalmazás szállítójával. A legtöbb alkalmazás az alábbi technikák egyikét használja:

- Az alkalmazás tartalmazza a könyvtárakat a felhasználó kezdeti könyvtárlistájában.
- Az alkalmazás lefuttat egy beállító programot, amely hozzáadja a könyvtárakat a felhasználó könyvtárlistájához.
- A könyvtáraknak nem kell a listában lenniük. Az alkalmazási programok mindig megadják a könyvtárat.

A könyvtárlistát az alkalmazások futtatásakor a rendszer használja a szükséges programok és fájlok megtalálásához. A **könyvtárlista** a könyvtárak olyan listája, amit a rendszer az objektumok keresésekor használ fel. Két részből áll:

1. **Rendszer rész:** QSYLIBL rendszerváltozó adja meg, OS/400 könyvtárak esetén használatos. A rendszerváltozó alapértelmezésének módosítására nincs szükség.
2. **Felhasználói rész:** QUSRLIBL rendszerváltozó biztosítja a könyvtárlista felhasználói részét. A felhasználói job leírása vagy a bejelentkezés utáni parancsok határozzák meg a kezdeti könyvtárlistát. Ha van kezdeti könyvtárlistája a QUSRLIBL rendszerváltozó felülbírálja. Az alkalmazási könyvtárak a könyvtárlista felhasználórészében vannak megadva.

### Jobleírás használata

Amikor a felhasználó bejelentkezik a rendszerbe, a jobleírás meghatározza a munka számtalan jellemzőjét, beleértve a nyomtatás milyenségét, a kötegelt munkák futását és a kezdeti könyvtárlistát. A rendszer alapértelmezésben a QDFTJOBID nevű jobleírással érkezik, amelyet felhasználhat a csoportprofilok létrehozásakor. Habár a QDFTJOBID a QUSRLIBL rendszerváltozót definiálja kezdeti könyvtárlistaként. Ha azt szeretné, hogy különböző csoportok különböző könyvtárakat érjenek el bejelentkezéskor, létre kell hozni egyedi jobleírásokat a csoportok részére.

Sorolja fel a csoportok könyvtárigényeit a Felhasználói csoportokat leíró űrlapon. Ha a könyvtárnak a csoportra vonatkozó jobleírás kezdeti könyvtárlistájában kell lenni, jelölje be a könyvtárat az űrlapon.

Szándékában állhat példaként átnézni, hogy Sharon Jones hogyan írta le felhasználói csoportjait a JKL Toy Company esetében, mielőtt kiválasztaná a bejelentkezést befolyásoló rendszerváltozókat.

**Példa: JKL Toy Company Felhasználói csoportot leíró űrlap:** Az első táblázat mutatja be a Felhasználói csoportot leíró űrlap első részét, amelyet Sharon Jones készített el a Kereskedelmi és marketing osztály számára. Ne felejtse el, hogy Sharon nem tette bele a CONTRACTS és CPPGMLIB könyvtárakat a csoport kezdeti könyvtárlistájába. Az alkalmazás automatikusan hozzáadja őket a listához, nem kell, hogy a DPTSM kezdeti könyvtárlistán legyenek. Amikor a felhasználó kilép az alkalmazásból, a rendszer eltávolítja a könyvtárakat a listából. Ez további biztonságot jelent a könyvtárak számára, hiszen csak az alkalmazási programokon keresztül érhetők el.

21. táblázat: JKL Toy Company Felhasználói csoportot leíró űrlap: példa leíró információkra

Felhasználói csoportot leíró űrlap	Első rész
Készítette: Sharon Jones	Dátum: 9/5/99
Csoportprofil neve: DPTSM	
A csoport leírása: Kereskedelmi és marketing osztály	
Csoport elsődleges alkalmazása: Szerződések és árak	
További alkalmazások listája: Készletgazd. (tételleírások és árak), Vevő rendelések	
A csoport könyvtárigényének listája. Tegyen jelet (✓) minden olyan könyvtár elé, melynek a kezdeti könyvtárlistában kell szerepelnie:	
<ul style="list-style-type: none"> <li>• ✓CUSTLIB</li> <li>• ✓ITEMLIB</li> <li>• ✓COPGMLIB</li> <li>• ✓ICPGMLIB</li> <li>• CPPGMLIB</li> <li>• CONTRACTS</li> </ul>	

Továbbá, Sharon ugyancsak belekezdett a Raktár osztály Felhasználói csoportot leíró űrlapjába is.

22. táblázat: Felhasználói csoportot leíró űrlap: leíró információk

Felhasználói csoportot leíró űrlap	Első rész
Készítette: Sharon Jones	Dátum: 9/5/99
Csoportprofil neve: DPTWH	
A csoport leírása: Raktár osztály	
Csoport elsődleges alkalmazása: Készletgazdálkodás	
A csoport számára szükséges további alkalmazások: nincs	
A csoport könyvtárigényének listája. Tegyen jelet (✓) minden olyan könyvtár elé, melynek a kezdeti könyvtárlistában kell szerepelnie:	
<ul style="list-style-type: none"> <li>• ✓ITEMLIB</li> <li>• ✓ICPGMLIB</li> </ul>	

Miután befejezte a Felhasználói csoportot leíró űrlap első részét, elkezdheti a bejelentkezést befolyásoló értékek kiválasztását.

## Bejelentkezést befolyásoló rendszerváltozók kiválasztása

Miután megtervezte a csoportprofilokat a rendszeren, ki kell választani a bejelentkezésre hatással lévő rendszerváltozókat. Írja le választását a Felhasználói csoportokat leíró űrlap második részében. Ne felejtse el, hogy most olyan értékeket választ, amelyeknek másolásával fogja a csoporttagok egyedi profiljait előállítani. Kezdje a kiválasztott csoportprofilnév bevitelével és a csoportra vonatkozó rövid leírással.

Ha megfelelően van a rendszer egyéniesítve, a felhasználóknak csak saját azonosítójukat és jelszavukat kell megadni a bejelentkezési képernyőn. Minden más bejelentkezési értéket profiljuk ad meg.

### Jelszó

Állítsa a csoportprofil jelszavát \*NONE értékre. Ez megakadályozza azt, hogy valaki bejelentkezzen a profillal. Később, mikor a csoportprofil másolásával előállította az egyedi profilokat, be kell állítani a jelszót minden felhasználónak.

## Kezdeti program és kezdeti eljárás

A felhasználó kezdeti programja (más néven **bejelentkezési programja**) lefut, mielőtt a rendszer megjeleníti az első menüt. Írja be a csoportprofilba mind a program, mint a könyvtár nevét, még akkor is, ha a könyvtár rajta van a kezdeti könyvtárlistán. Mindkettő megadásával biztos lehet benne, hogy a rendszer megfelelő programot futtat és nem kell aggódnia a könyvtárlista megváltozásától.

Az alábbi okok egyike miatt kerül sor kezdeti program vagy eljárás használatára:

- Néhány alkalmazás használ kezdeti programot az alkalmazási környezet kialakítása céljából.
- Ha azt akarja, hogy egy felhasználó csak egy programot futtasson és sose lássa a menüt. Például, a JKL Toy Company cégnél a fogadó raktár dolgozói csak a bejövő áruk nyilvántartását feldolgozó programot futtathatják. Ez kiküszöböli a nyilvános helyen lévő munkaállomás okozta biztonsági kockázatot.

Ha beállítja a **Korlátolt képesség** mezőt \*YES vagy \*PARTIAL értékre, a felhasználó nem tudja a kezdeti programot megváltoztatni a bejelentkezési képernyőn.

Ellenőrizze a programozókkal, hogy az alkalmazás igényel-e kezdeti programot vagy eljárást.

## Kezdeti menü és kezdeti menükönyvtár

A kezdeti menü, vagy más néven **első menü**, valóban az első menü, amit a felhasználó a bejelentkezést követően lát. A kezdeti program lefut a kezdeti menü megjelenése előtt. Ha a kezdeti program megjelenít képernyőt, akkor azokat látja a felhasználó a kezdeti menü előtt.

Normál esetben a csoport fő alkalmazásának elsődleges menüje a kezdeti menü. Adja meg mind a menü, mind a könyvtár nevét.

Ha beállítja a **Korlátolt képesség** mezőt \*YES értékre, a felhasználó nem tudja a kezdeti menüt megváltoztatni a bejelentkezési képernyőn. Ha beállítja a *Korlátolt képesség* mezőt \*PARTIAL értékre, a felhasználó megtudja változtatni a kezdeti menüt a bejelentkezési képernyőn.

## Aktuális könyvtár

Az aktuális könyvtár másik neve **alapértelmezett könyvtár**. Történik néhány dolog, mikor aktuális könyvtárat definiál egy felhasználó számára:

- Ha a felhasználó létrehoz valamilyen objektumot (például lekérdező programot), a rendszer az aktuális könyvtárba helyezi el, hacsak a felhasználó más könyvtárat nem ad meg.
- A rendszer automatikusan hozzáadja az aktuális könyvtárat a könyvtárlista felhasználórészéhez. Benne lehet a jobbleírás kezdeti könyvtárlistájában is, de nem szükségszerű.
- Az aktuális könyvtár az első helyre kerül a könyvtárlista felhasználórészben. A rendszer az aktuális könyvtárban keresi először a fájlokat, s csak azután keresi a könyvtárlista további könyvtáraiban.
- Ha nincs a felhasználónak definiálva aktuális könyvtár, a rendszer a QGPL (general purpose) könyvtárat rendeli hozzá.

## Javaslatok

Az aktuális könyvtár különösen fontos, ha IBM Query for iSeries vagy más hasonló program használatát tervezi. Alkalmazza az alábbi megközelítések egyikét:

- Hozzon létre a csoporttagok részére egy közös könyvtárat. Az összes query programot és fájlt töltsse ebbe a könyvtárba. Adja ugyanazt a nevet neki, mint a csoportprofil és állítsa be a csoport aktuális könyvtárának.
- Adjon minden Query felhasználónak személyi könyvtárat. Adja a könyvtárnak ugyanazt a nevet, mint a felhasználói profilnak. Majd adja meg aktuális könyvtárként a csoporttagok egyedi profiljaiban, és ne a csoportprofilban tegye ezt meg.

Töltse ki a bejelentkezést befolyásoló mezőket saját adataival a Felhasználót leíró űrlap második részében.

Miután kiválasztotta a bejelentkezést befolyásoló értékeket, kiválaszthatja a felhasználó tevékenységét korlátozó értékeket.

### A felhasználó tevékenységét korlátozó értékek kiválasztása

Miután leírta saját választását a bejelentkezést befolyásoló értékekkel kapcsolatban a Felhasználói csoportot leíró űrlap második részében, elgondolkozhat azon, hogy milyen mértékben korlátozza a felhasználók tevékenységét a rendszeren. Lehet, hogy korlátozni akarja a felhasználók tevékenységét néhány okból kifolyólag:

- Megelőzni a CL parancsok használatát. Nagy a csábítás a kísérletezésre és meggondolatlan hibák okozására.
- Elérni, hogy a felhasználók csak a megadott alkalmazásokat és funkciókat használják.
- Olyan egyszerű környezetet biztosítani, amelyben a felhasználó nem tud téveszteni felesleges választások miatt.

Sok tényező határozza meg, hogy mennyi mindent tehet a felhasználó:

- Alkalmazás felépítése
- Rendszerváltozók
- Forrásbiztonság
- Csoportprofilok
- Felhasználói profilok
- Jobleírások

A csoport vagy a felhasználói profil két mezője, a **Korlátolt képességek (Limit capabilities)** és a **Felhasználói osztály (User Class)** határozzák meg, hogy a felhasználó hány Ön által hozott döntést bírálhat felül.

### Korlátolt képességek

A **Korlátolt képességek** mezőt hívhatjuk **Restricted command line use**-nak is. Korlátozhatja, hogy a felhasználók megváltoztassák a bejelentkezési képernyő értékeit, a Figyelem-gomb kezelő programjukat, valamint korlátozhatja a parancsbevitelt is. Erős korlátozást jelent a (\*YES) érték, átlagosat a (\*PARTIAL) érték, és nincs korlátozás (\*NO) esetén. A következő táblázat ismerteti, hogy mit engedélyeznek ezek az értékek:

23. táblázat: Megengedett funkciók a Korlátolt képességek értékeinél

Korlátolt képesség értéke	Kezdeti program megváltoztatás	Kezdeti menü megváltoztatás	Aktuális könyvtár megváltoztatás	Figyelem program megváltoztatás	Enter parancsok
*YES	Nem	Nem	Nem	Nem	Kevés <sup>1</sup>
*PARTIAL	Nem	Igen	Nem	Nem	Igen
*NO	Igen	Igen	Igen	Igen	Igen
<b>1</b>	Engedélyezett parancsok: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG és STRPCO. A felhasználó nem használhatja az F9-et a parancssor megjelenítésére egyetlen Operational Assistant menüből és képernyőből sem.				

### Felhasználói osztály

A felhasználói osztály, másnéven a **felhasználó típusa**, határozza meg, hogy az Operational Assistant és a rendszermenük milyen opcióit látja a felhasználó. Ugyancsak meghatározza azt is, hogy mit tehet a felhasználó, hacsak nincs jogosultsági lista megadva a **Speciális jogosultság** mezőben.

### Javaslatok a korlátolt képességekre és a felhasználói osztályokra

A felhasználók többségének nem szükséges vagy nem akarja elérni a CL parancsokat vagy a rendszerfunkciókat. Az Operational Assistant képernyők elég információt és vezérlési lehetőséget adnak a felhasználónak saját munkájához. Az alábbi ajánlások garantálják azt, hogy a felhasználók csak azokat a rendszer erőforrásokat érik el, amelyek feladataik elvégzéséhez szükségesek:

- Minden csoportprofilban állítsa be a **Korlátozott képességek** mezőt \*YES értékre. Állítsa a *Felhasználói osztály* mezőt \*USER értékre.
- Írja át ezeket a specifikációkat a rendszerfunkciókat igénylő felhasználóknál.
- Győződjön meg róla, hogy a menük biztosítják a mozgást az alkalmazások között, ha ez kell a felhasználónak.

Miután leírta saját választását a felhasználói osztályra és a korlátozott képességekre a Felhasználói csoportot leíró űrlap második részében, válassza ki a felhasználói környezetet beállító értékeket.

## A felhasználói környezetet beállító értékek kiválasztása

Miután leírta, hogyan korlátozza a felhasználók tevékenységét a rendszeren a Felhasználói csoportot leíró űrlap második részében, választhat a felhasználói környezetet meghatározó értékek közül. A felhasználói profil számos mezője meghatározza a felhasználó működési környezetét: melyik nyomtatót használja, hova menjenek az üzenetek, milyen prioritású munkák fussanak. A mezők többségére az alapértelmezett beállítások javasoltak. Néhány mező leírását megtalálhatja a következő bekezdésben.

- **Jobleírás és jobleírás könyvtár:** A profil ezen mezői megmondják a rendszernek, hogy milyen jobleírást használjon a felhasználó bejelentkezése esetén. A jobleírás tartalmazza a kezdeti könyvtárlistát. Minden csoportnak profiljuk nevével azonos nevű jobleírással kell rendelkeznie. A jobleírások általában a QGPL könyvtárban vannak.
- **Nyomtató eszköz és kimeneti sor:** A felhasználó által előállított nyomtatandó lista a profiljában megadott nyomtatóra megy mindaddig, míg egy adott nyomtatási job másik nyomtatóra nem irányítja. Egy adott csoport tagjai általában egy helyen vannak és ugyanazt a nyomtatót használják. Megadhatja a nyomtatót a csoportprofilban és másolhatja minden egyes egyedi profilba. A felhasználó nyomtató eszközének neve **alapértelmezett nyomtató**. A kimeneti sor tartalmazza a kinyomtatandó listát a nyomtatás előtt. Általában minden nyomtatónak van kimeneti sora a saját nevével. Megadhatja a \*DEV opciót a kimeneti sor részére tudatva a rendszerrel, hogy használhatja az egység kimeneti sorát.  
Töltse ki a jobleírás és könyvtárának nevét, az alapértelmezett nyomtatót, valamint a kimeneti sort a Felhasználói csoportot leíró űrlapon.
- **Operational Assistant kezelőfelület beállítása:** A rendszer leszállításakor az Operational Assistant menü a Figyelem gomb kezelőprogramja. Amikor a felhasználó megnyomja a Figyelem gombot az Operational Assistant (ASSIST) menüjét fogja látni. Ha az alkalmazási programok eltérő Figyelem gomb kezelő programot használnak, akkor más eljárást kell biztosítani az Operational Assistant menü eléréséhez:
  - Adja meg az Operational Assistant menüt, mint az alkalmazás egyik opcióját annak főmenüjén a GO ASSIST vagy CALL QEZAST használatával.
  - A felhasználók gépeljék be a GO ASSIST parancsot a parancssorban.

Ha a **Korlátozott képesség** mező beállítása \*YES a felhasználói profilban, akkor a GO parancs nem használható a menü megjelenítéséhez. Valamilyen más módszert kell biztosítani az Operational Assistant felhasználóknak az ASSIST menü elérésére.

Szándékában állhat egy példán áttekinteni, hogy Sharon Jones milyen értékeket választott ki a JKL Toy Company számára a Felhasználói csoportot leíró űrlapon.

A tervezési lépések elvégzéséhez:

- Töltse ki a Felhasználói csoportot leíró űrlapot a vállalat minden egyes felhasználói csoportjára.
- Írja le a felhasználói csoportok neveit az Elnevezési szabályok űrlapon.
- Rendelje hozzá a felhasználói csoportokat az alkalmazások és könyvtárak diagramjához.

Miután végzett a feladatokkal, elkezdheti az Egyedi felhasználói profilok tervezését.



**Példa: JKL Toy Company Felhasználói csoportot leíró űrlap — második rész:** Sharon Jones készített néhány megjegyzést a Kereskedelmi és marketing osztályról (SM), valamint a Raktár osztályról (WH), amikor készítette a Felhasználói csoportot leíró űrlapot a Kereskedelmi és marketing osztály személyzetéről:

- Az SM osztály személyzete erős felhasználója az IBM Query for iSeries programnak. Mindegyik felhasználónak saját könyvtárat kell biztosítani. A Raktár osztálynak megfelel egy csoportkönyvtár.
- A fogadó térben dolgozó Raktári személyzetnek kezdeti program kell kezdeti menü helyett.

Sharon elkészítette a Felhasználói csoportot leíró űrlap második részét két osztály számára.

24. táblázat: JKL Toy Company felhasználói csoportot leíró űrlapja: Kereskedelmi és marketing osztály

Mező neve	Ajánlott érték	Saját választás
Csoportprofil neve		DSTSM
Jelszó	*NONE	*NONE
Felhasználói osztály	*USER	*USER
Aktuális könyvtár	<i>mint a csoportprofil neve</i>	(üresen hagyva, csak az egyedi profilokban kitöltve)
Hívandó kezdeti program (bejelentkezési program)		
Kezdeti programkönyvtár		
Kezdeti menü		CPMAIN
Kezdeti menü könyvtára		CPMAINLIB
Korlátolt képességek (korlátolt parancssor haszn.)	*YES	*PARTIAL
Szöveg (felhasználó leírás)		Kereskedelmi és marketing osztály
Jobleírás	<i>mint a csoportprofil neve</i>	DPTSM
Jobleírás könyvtára		QGPL
Csoportprofil neve	*NONE <sup>1</sup>	*NONE
Nyomtató egység		PRT03
Kimeneti sor	*DEV	*DEV

25. táblázat: JKL Toy Company felhasználói csoportot leíró űrlapja: Raktár osztály

Mező neve	Ajánlott érték	Saját választás
Csoportprofil neve		DPTWH
Jelszó	*NONE	*NONE
Felhasználói osztály	*USER	*USER
Speciális környezet		
Aktuális könyvtár	<i>mint a csoportprofil neve</i>	DPTWH
Hívandó kezdeti program (bejelentkezési program)		
Kezdeti program könyvtára		
Kezdeti menü		ICMAIN
Kezdeti menü könyvtára		ICPGMLIB
Korlátolt képességek (korlátolt parancssor haszn.)	*YES	*YES
Szöveg (felhasználó leírás)		Raktár osztály
Jobleírás	<i>mint a csoportprofil neve</i>	DPTWH

25. táblázat: JKL Toy Company felhasználói csoportot leíró űrlapja: Raktár osztály (Folytatás)

Mező neve	Ajánlott érték	Saját választás
Jobleírás könyvtára		QGPL
Csoportprofil neve	*NONE <sup>1</sup>	*NONE
Nyomtató egység		PRT04
Kimeneti sor	*DEV	*DEV
<b>1</b> A csoportprofil nevének *NONE értékűnek kell lenni. A csoportprofil nem lehet egy másik csoport tagja.		

Most elkezdheti az egyedi felhasználói profilok tervezését.

## Egyedi felhasználói profilok tervezése

Most, hogy döntött az átfogó biztonsági stratégiáról, és megtervezte a felhasználói csoportokat, készen áll az egyedi felhasználói profilok tervezésére.

### Milyen űrlapra van szükség?

Az alábbi űrlapokat használja fel az egyedi felhasználói profilok tervezéséhez:

- Egyedi felhasználói profil űrlapja
- Rendszerfelelősségek űrlap

Az alábbi kitöltött űrlapokra is szüksége lesz:

- Felhasználói csoportot azonosító űrlap
- Elnevezési szabályok űrlap
- Saját alkalmazási diagramja

### Felhasználói profilok elnevezése

A felhasználói profil nevét a felhasználónak a rendszer felé történő azonosítása adja. A bejelentkezési képernyő **User ID** mezőjében megadott érték maga a profil neve. Minden munkához, nyomtatáshoz, amit végez, a rendszer hozzárendeli profilja nevét.

A felhasználói profilok elnevezésekor legyen tekintettel az alábbiakra:

- A profil neve maximum 10 karakter hosszúságú lehet. Bizonyos kommunikációs módszerek 8 karakterre korlátozzák a felhasználói azonosítót.
- A felhasználói profil neve tartalmazhat betűket, számokat és speciális karaktereket: font (#), dollár (\$), aláhúzás (\_), és "at" jel (@). Viszont nem kezdődhet számmal vagy aláhúzással (\_).
- A rendszer nem tesz különbséget a kis- és nagybetűk között a felhasználói profilban. A rendszer a kisbetűs karaktereket nagybetűkké konvertálja.
- A rendszer a felhasználói profilok listáját a nevük ábécé sorrendjében jeleníti meg.
- Minden IBM által szállított profil Q betűvel kezdődik. A saját profilok elnevezésére az IBM profiloktól eltérő kezdőbetűt használjon, hogy elkerülje a hozzárendelési hibákat.

### Javaslatok

Egy lehetséges technika a felhasználói nevek kialakítására, mikor a családnév első 7 karakterét a keresztnév első karaktere követi. Az alábbi táblázatban láthatja Sharon elnevezési szabályát, amelyet a felhasználói profilok elnevezésére alkalmazott a JKL Toy Company-nál:

26. táblázat: JKL Toy Company Elnevezési szabályok űrlap: felhasználói profil példa

Felhasználó neve	Felhasználói profil neve
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

Ez a módszer könnyen megjegyezhetővé teszi a profilok neveit. Egyúttal a profilok nevének listája a családi nevek sorrendjével fog megegyezni.

Például, a JKL Toy Company esetében Sharon Jones ezt az elnevezési szabályt kívánja alkalmazni. Kitöltötte az Elnevezési szabályok űrlap megfelelő szekcióját.

27. táblázat: JKL Toy Company Elnevezési szabályok űrlap: felhasználói profil példa

Objektum típusa	Elnevezési szabályok
Felhasználói profilok	Használja a felhasználó családi nevének első 7 karakterét és azt követve a keresztnév első karakterét. A felhasználói profil leírása a felhasználók családi és utónevét tartalmazza.

Írja le az Elnevezési szabályok űrlapon, hogyan kívánja elnevezni a felhasználói profilokat, majd meghatározhatja, hogy ki feleljen a rendszerfunkciókért és kiválaszthatja az értékeket minden egyes felhasználó számára.

## Rendszerfunkciókért felelősök meghatározása

Az Egyedi felhasználói profilok tervezéséhez először meg kell határozni a rendszer egyedeinek felelősségét. A rendszer hatékony működéséhez szükség van olyan személyekre, akik szabályos időközönként elvégzik a kezelési és karbantartói funkciókat. Az ilyen feladatokat ellátó személyeknek megfelelő jogosultsággal kell rendelkezniük.

A felhasználó tevékenységét korlátozó értékek kiválasztása című rész tárgyalta a **Felhasználói osztály** és a **Korlátozott képességek** mezők értékeinek hatását az elvégezhető rendszerfunkciók szempontjából. A felhasználók többségének rendszerint nem kell engedélyezni a rendszerfunkciók elvégzését (felhasználói osztály \*USER értékre, míg a korlátozott képességek \*PARTIAL vagy \*YES értékre állítva). Azonban, néhány felhasználónak további jogosultságot kell adni, hogy a rendszer hatékonyan működjön.

Az alábbi táblázat felsorol néhány fontos rendszerkezelési feladatot. Jelzi a Felhasználói osztályt és az egyedi jogosultságokat, amelyeket hozzárendelhet az ilyen felelősséggel rendelkező személyekhez. A lista elősegítheti annak meghatározását, hogy mely felhasználóknak milyen speciális jogosultságot kell adni. Azonban ez a táblázat nem szándékozik komplett tervezési eszköz lenni a saját rendszer működésére és karbantartására. A táblázat olyan felhasználói osztályokat és egyedi jogosultságokat tartalmaz, amelyek a legtöbb rendszeren működnek. Lehet, hogy eltérő jogosultságokat kell hozzárendelnie, a rendszertől függően.

Mikor a profilban a \*USER osztálytól eltérőt ad meg, a felhasználó automatikusan megkapja a speciális jogosultságok adott készletét a rendszerfunkciók végrehajtásához. Hozzárendelhet felhasználói egyedi jogosultságokat is, amelyek eltérnek a felhasználói osztály mezőben megadottaktól, de erre nem biztos, hogy szükség van.

28. táblázat: Rendszerfelelősség, felhasználói osztály és egyedi jogosultság

Rendszerfunkció <sup>1</sup>	Leírás	Szükséges felhasználói osztály <sup>2</sup>	Szükséges egyedi jogosultság <sup>3</sup>
Rendszerműveletek	Nyomatott listák kezelése, válaszolás rendszerüzenetekre, műveletek követése, kezdeti programbetöltés (IPL) végrehajtása.	*SYSOPR	*JOBCTL
Rendszertakarítás	Rendszertakarítási funkciók végrehajtása, úgymint az automatikus takarítás beosztása és a diszkhasználat követése.	*SYSOPR	*JOBCTL

28. táblázat: Rendszerfelelősség, felhasználói osztály és egyedi jogosultság (Folytatás)

Rendszerfunkció <sup>1</sup>	Leírás	Szükséges felhasználói osztály <sup>2</sup>	Szükséges egyedi jogosultság <sup>3</sup>
Rendszer biztonsági mentés	Alkalmazási könyvtárak, rendszerkönyvtárak és a biztonsági információk letárolása szabályos időközönként. A funkciók részletes leírását az Információs központ Mentés és visszaállítás című témakörében olvashatja el.	*SYSOPR	*SAVSYS
Profil adminisztráció	Új felhasználói profilok felvétele, meglévők karbantartása.	*SECADM	*SECADM
Erőforrás biztonság adminisztráció	Objektumjogosultságok karbantartása a rendszerben.	*SECOFR	*ALLOBJ
Program karbantartás	Program változások (PTF) periodikus hozzáadása az IBM könyvtárakhoz. Alkalmazási könyvtárak módosítása.	*SECOFR	*ALLOBJ
Biztonsági ellenőrzés	Biztonsági felülvizsgálati funkciók összeállítása. Események, felhasználók, objektumok kijelölése vizsgálatra.		*AUDIT <sup>4</sup>
Rendszer konfigurálás	Egységek felvétele, módosítása, eltávolítása a rendszerből.		*IOSYSCFG <sup>5</sup>
1	Állítsa a Korlátolt képességek mezőt *NO értékre a feladatért felelős felhasználóknak.		
2	Minimum ez a felhasználói osztály szükséges. A felhasználói osztály biztosítja a funkció elvégzéséhez szükséges parancsok és menüopciók használatának jogosultságát. Az erőforrás biztonságtól függően további objektumjogosultsági igény merülhet fel.		
3	A feladat adta felelősség ezeket a speciális jogosultságokat igényli. A felhasználói osztály adhat további speciális jogosultságot.		
4	Az *AUDIT speciális jogosultságnak nincs megfelelő felhasználói osztálya. A *SECOFR felhasználói osztályban van az *AUDIT speciális jogosultság. Habár, a felülvizsgálónak valószínűleg nem szükséges a *SECOFR osztály adta egyéb jogosultságok. Egyszerűbb az *AUDIT speciális jogosultságot beállítani a rendszert felülvizsgálók egyedi profiljaiban.		
5	Az *IOSYSCFG speciális jogosultságnak nincs megfelelő felhasználói osztálya. A *SECOFR felhasználói osztályban van az *IOSYSCFG speciális jogosultság. Egyszerűbb az *IOSYSCFG speciális jogosultságot beállítani a rendszert felülvizsgálók egyedi profiljaiban. Az egyének képesek létrehozni vonalakat, vezérlőket és egységeket, vagy TCP/IP -t konfigurálni. Habár, a rendszert konfigurálónak nincs szüksége a *SECOFR osztály adta többi jogosultságra.		

## Javaslatok

Használja a fenti táblázatot a rendszerfunkciókat végrehajtók megnevezésére. Legalább két embert jelöljön ki a rendszerbiztonság kezelésére, és két másik személyt a működés és a biztonsági mentések felügyeletére.

A Rendszerfelelősségek űrlapja jó eszköz a rendszer irányítására és felügyeletére. Segítségével nyomon követheti mindazokat, akiknek egyedi jogosultsága van a rendszeren, és azt is megtudhatja, miért szükséges számukra az egyedi jogosultság.

Szándékában állhat példaként megtekinteni Sharon döntését a felhasználói felelőségekről, mielőtt kiválasztaná az egyes felhasználókat befolyásoló értékeket.

**Példa: JKL Toy Company Rendszerfelelőségek űrlapja:** Az alábbiakban a Rendszerfelelőségek űrlapjára lát példát, amelyet Sharon Jones állított össze:

29. táblázat: JKL Toy Company Rendszerfelelősségek űrlapja: példa

Elsődleges biztonsági felelős Sharon Jones			
Másodlagos biztonsági felelős Ken Harrison			
Profil neve	Felhasználó neve	Osztály	Megjegyzések
JONESS	Sharon Jones	*SECOFR	Sharon az elsődleges biztonsági felelős és rendszerirányító.
HARRISOK	Ken Harrison	*SECOFR	Ken helyettesíti Sharont, mint általános rendszerirányító.
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy felel elsősorban a rendszerműveletekért és a biztonsági mentésekért.
ROGERSK	Karen Rogers	*SYSOPR	Karen segíti Sandyt feladata elvégzésében.
WILLISR	Rose Willis	*SYSOPR	Rose lesz az operátor a második műszakban.

Miután elkészítette a Rendszerfelelősségek űrlapját, megkezdheti az értékek kiválasztását az egyes felhasználók számára.

### Értékek kiválasztása az egyes felhasználóknak

Miután meghatározta a felhasználók felelősségét a rendszeren, megkezdheti az értékek kiválasztását az egyes felhasználók számára. A csoportprofilok - melyek mintaként szolgálnak az egyedi profilokhoz - megtervezésével a munka többségét elvégezte. Az Egyedi felhasználói profil nevű űrlap segítségével rendelje hozzá a felhasználókat a megfelelő csoporthoz és definiálja a csoporton belüli különbségeket. Mintaként töltsön ki egy Egyedi felhasználói profil űrlapot az egyik felhasználói csoportra vonatkozóan, majd térjen vissza az Egyedi felhasználói profil készítéséhez, ha további felhasználói csoportokra vonatkozóan is el kívánja készíteni.

Töltse ki a csoportprofil nevét és a többi leíró információt az Egyedi felhasználói profil űrlap felső részén.

#### Példa: JKL Toy Company Egyedi felhasználói profil űrlapjának leíró információi

Itt található meg, Sharon Jones hogyan töltötte ki az Egyedi felhasználói profil űrlapot.

30. táblázat: JKL Toy Company Egyedi felhasználói profil űrlap: példa leíró információkra

Egyedi felhasználói profil űrlapja	
Készítette: Sharon Jones	Dátum: 9/5/99
Csoportprofil neve: DPTOP	
Létrehozott obj. gazdája:	Csoportjogosultság az objektumokhoz:
Csoport jogosultság típusa:	

### Értékek meghatározása a csoporttagok számára

Az Egyedi felhasználói profil űrlapon töltsön ki a csoport minden tagjára vonatkozóan a profil nevét és leírását (felhasználó neve). Az alábbi paragrafus ismerteti más értékek meghatározását a csoport tagjai számára.

Emlékezzen rá, hogy a csoportprofil mintaként szolgál az egyedi profilok elkészítéséhez. Ezért az Egyedi felhasználói profil űrlapon csak a csoporttól eltérő értékeket kell definiálnia.

- **Jelszavak hozzárendelése:** A legegyszerűbb, ha kezdeti jelszóként a profil nevét adja meg. A kezdeti jelszó lejártságát beállítva elérheti, hogy a felhasználó az első bejelentkezésekor mindenképpen megváltoztatja azt. A Jelszó beállítása lejárt állapotba című részben fog olvasni arról, hogyan történik ez automatikusan a csoportprofil másolásakor. Ha ezt a módszert követi nem kell a jelszavakat felírni az Egyedi felhasználói profil űrlapján.

- **Felhasználói osztály és Korlátolt képességek:** Nézze meg a Rendszerfelelősségek űrlapján, hogy a csoportok mely tagjainak kell a többiektől eltérő értéket adni a **Felhasználói osztály** és a **Korlátolt képességek** mezőkre. Töltse ki a megfelelő információt az Egyedi felhasználói profil űrlapon azoknak, akiknek az értékei eltérnek a csoportprofilban lévőktől.
- **Egyéb értékek megadása:** Ellenőrizze azokat a felhasználókat, akiknek a Felhasználói csoportot leíró űrlapon megadottól eltérő értékeket kell adni. A Felhasználói csoportot leíró űrlapon a **Felhasználói osztály** és a **Korlátolt képességek** mezők a lap felső részén találhatóak, mivel ezek az értékek gyakran eltérhetnek a csoport néhány tagjánál. Jegyezzen fel minden olyan mezőt, amely a felhasználónál eltér a csoport többi tagjától.

A tervezési lépés befejezéséhez feltétlenül végezze el a következőket:

- Töltse ki a Rendszerváltozók kiválasztása űrlapot.
- Írja le az Elnevezési szabályok űrlapján, hogyan kívánja elnevezni a felhasználói profilokat.
- Készítse el az Egyedi felhasználói profilok űrlapját a cég mindegyik csoportjára.

Szándékában állhat példaként megtekinteni Sharon adatait az egyedi felhasználókról, mielőtt megtervezné az erőforrás biztonságot.

**Példa: JKL Toy Company Egyedi felhasználói profil űrlap:** Például a JKL Toy Company esetében a raktárban dolgozók csak egy programot tudnak futtatni. Sharon néhány funkcióra korlátozta tevékenységüket, mert munkahelyük jellege miatt munkaállomásaik túl nyilvános helyen vannak. Ezért a Raktár osztály tagjainak nincs kezdeti menüjük, csak kezdeti programjuk. A Rendelésfeldolgozó osztálynak két helyi és egy távoli nyomtatója van. Ezért Sharon néhány felhasználónak - a csoporttól eltérően - más nyomtatót jelölt ki.

Sharon Jones az alábbi Egyedi felhasználói profil űrlapot töltötte ki a JKL Toy Company Raktár és Rendelésfeldolgozó osztályai számára. Ne felejtse el, hogy csak azokat a mezőket töltötte ki, amelyek értéke eltér a csoportprofilban megadottól.

31. táblázat: JKL Toy Company egyedi felhasználói profil űrlapja: Raktár osztály

Csoportprofil neve: DPTWH					
A csoport minden tagját jegyezze fel:					
Felhasználói profil	Szöveg (leírás)	Felhasználói osztály	Korlátolt képesség	Kezdeti program/ Könyvtár	Kezdeti menü/ Könyvtár
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ ICPGMLIB	nincs
AMESJ	Ames, Janice			ICRCPT/ ICPGMLIB	nincs
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

32. táblázat: Egyedi felhasználói profil űrlapja: Rendelésfeldolgozó osztály

Csoportprofil neve: DPTOP				
A csoport minden tagját jegyezze fel:				
Felhasználói profil	Szöveg (leírás)	Felhasználói osztály	Korlátolt képesség	Nyomtató egység
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

Következő lépésként elkezdheti az erőforrás biztonság tervezését.

## Erőforrás biztonság tervezése

Most, hogy befejezte a felhasználók tervezését, megtervezheti az erőforrás biztonságot, amely az objektumokat védi a rendszeren. Az "Erőforrás biztonság beállítása" című részben tanulmányozhatja az erőforrás biztonság beállítását a rendszeren.

A rendszerváltozók és felhasználói profilkok vezérlik a rendszer elérését és megelőzik a jogosulatlan bejelentkezéseket. Az erőforrás biztonság vezérli azokat a műveleteket, amelyeket a jogosult rendszerfelhasználók végrehajthatnak, miután sikeresen bejelentkeztek. Az erőforrás biztonság támogatja a rendszerbiztonság fő célját, azaz védelmezi:

- Az információ titkosságát
- Az információ pontosságát a jogosulatlan módosítások megakadályozásával
- Az információ használhatóságát a véletlen és a szándékos adatsérülés megelőzésével

Az erőforrások biztonságának tervezése eltérő lehet attól függően, hogy a cég az alkalmazásokat vásárolta vagy azok saját fejlesztésűek. Az alkalmazások saját fejlesztése esetén a programozókkal kell kommunikálnia már a tervezési fázisban az információ biztonsági igényeinek tisztázása érdekében. Vásárolt alkalmazás esetén Önnek kell meghatározni a biztonsági igényeket és összevetni az alkalmazás struktúrája adta lehetőségekkel. Az alábbiakban ismertetésre kerülő technikák mindkét esetben segítséget nyújtanak.

Ez a témakör az erőforrás biztonság tervezésének alapvető elemeit ismerteti. Bemutatja a főbb módszereket és azok használatát. Az itt leírt technikákat nem szükségszerű alkalmazni minden cégre és alkalmazásra. Konzultáljon a programozóval vagy az alkalmazás szállítójával az erőforrás biztonság tervezése kapcsán.

Az erőforrás biztonság tervezéséhez az alábbi témaköröket nézheti át:

- Az erőforrás biztonság céljainak meghatározása
- A jogosultság típusainak megértése
- Alkalmazási könyvtárak biztonságának tervezése
- Könyvtárak és objektumok tulajdonosának meghatározása
- Objektumok csoportosítása
- Nyomtatott listák védelme
- Munkaállomások védelme
- Erőforrás biztonsági ajánlások összefoglalója
- Alkalmazások telepítésének tervezése

### Milyen űrlapra van szükség?

A következő űrlapokról készítsen másolatot és töltsse ki a témakör olvasása során. Dolgozza fel az egész eljárást egy alkalmazásra, majd ismételje meg az eljárást az összes többire.

33. táblázat: Erőforrás biztonság tervezéséhez szükséges űrlapok

Űrlap neve	Szükséges másolatok száma
Jogosultsági lista űrlapja	Néhány
Nyomtatott listák és munkaállomás biztonság űrlapja	Egy

Kiegészíti a következő űrlapokat, amelyekkel már korábban dolgozott:

34. táblázat: Űrlapok, amelyek változni fognak

Űrlap neve	Előkészítés fázisa
Könyvtárat leíró űrlap	Könyvtári információk leírása

34. táblázat: Űrlapok, amelyek változni fognak (Folytatás)

Űrlap neve	Előkészítés fázisa
Felhasználói csoportot leíró űrlap	Csoportprofilok tervezése

Hivatkozás korábban előkészített űrlapokra:

35. táblázat: Erőforrás biztonság tervezésének befejezéséhez szükséges űrlapok

Űrlap neve	Előkészítés fázisa
Könyvtárat leíró űrlap	Alkalmazási diagram rajzolása és Felhasználói csoportok azonosítása
Alkalmazást leíró űrlap	Alkalmazási információk leírása
Egyedi felhasználói profil űrlapja	Értékek kiválasztása az egyes felhasználóknak
Felhasználói csoportot azonosító űrlap	Felhasználói csoportok azonosítása
Rendszerfelelősségek űrlap	Rendszerfunkciókért felelősök meghatározása
Fizikai biztonság tervezési űrlap	Fizikai biztonság tervezése

## Az erőforrás biztonság céljainak meghatározása

Az Erőforrás biztonság tervezésének elkezdéséhez először meg kell határozni a célokat. Az iSeries rugalmasan valósítja meg az erőforrás biztonságot. Jó teljesítménnyel védi a kritikus erőforrásokat, pontosan azon a módon, ahogy Ön akarja. De az erőforrás biztonság egyúttal további terhelést jelent az alkalmazásoknak. Például, minden alkalommal, ha az alkalmazásnak egy objektumra van szüksége, a rendszernek ellenőriznie kell a felhasználó jogosultságát az objektumhoz. Örökké egyensúlyozni kell a bizalmasság és a teljesítmény költsége között. Az erőforrás biztonsággal kapcsolatos döntések meghozatalakor a biztonság egyes elemeinek értékét össze kell vetni az árával.

Annak megelőzésére, hogy az erőforrás biztonság komolyan csökkentse az alkalmazások teljesítményét, kövesse az alábbi szempontokat.

- Legyen az erőforrás biztonság sémája egyszerű
- Csak azokat az objektumokat védje, amelyeknek valóban biztonságosaknak kell maradni.
- Kiegészítésként használja az erőforrás biztonságot, de ne más információvédő eszköz helyett, mint például:
  - Felhasználók korlátozása megadott menükhöz és alkalmazásokhoz.
  - Felhasználói parancsbevitel megakadályozása (korlátolt képességek a felhasználói profilban).

Kezdje az erőforrás biztonság tervezését a célok meghatározásával. A biztonsági célokat megadhatja az Alkalmazást leíró űrlapon vagy a Könyvtárat leíró űrlapon.

Hogy melyik űrlapot használja, az attól függ, hogyan vannak az információk szervezve a könyvtárban.

Szándékában állhat példaként átnézni a JKL Toy Company biztonsági célkitűzéseit, mielőtt áttekinti a jogosultságok típusait, amelyeket az erőforrás biztonsághoz használhat.

### Példa: JKL Toy Company Biztonsági célkitűzések

Sharon Jones a Könyvtárat leíró űrlapot használta fel a Customer Records (CUSTLIB) könyvtár biztonsági követelményeinek leírására:

36. táblázat: JKL Toy Company Könyvtárat leíró űrlap: Biztonsági célkitűzések példa

Könyvtárat leíró űrlap	Első rész
Határozza meg a könyvtár biztonsági elemeit, vajon van-e titkos információ:	Ma még minden alkalmazott látja az ügyfél információkat és a vevő rendeléseket. Az információ pontosságának védelme érdekében irányítanunk kell, hogy kik változtathatják meg.



Sharon az Alkalmazást leíró űrlapot használta a Szerződések és árak alkalmazásra, hogy leírja az alkalmazás biztonsági célkitűzéseit

37. táblázat: JKL Toy Company Alkalmazást leíró űrlapja: Biztonsági célkitűzések példa

Alkalmazást leíró űrlap	Első rész
Határozza meg a könyvtár biztonsági elemeit, vajon van-e titkos információ:	<p>Az információk a szerződésekről és a speciális árakról titkosak. Csak kevés embernek van joga megtekinteni és változtatni:</p> <ul style="list-style-type: none"> <li>A Kereskedelmi és marketing osztály dolgozói és az összes vezető létrehozhatja, módosíthatja, elemezheti a szerződéseket. Nekik mind a programokat, mind a fájlokat használniuk kell.</li> <li>A Rendelésfeldolgozási osztály dolgozói a rendelések felvételekor és leszállításakor indirekt módon módosítják a szerződéseket és látják az árakat. A szerződéseket és árakat csak rendelés felvételekor vagy módosításakor láthatják.</li> </ul>

Írja le saját alkalmazásának biztonsági célkitűzéseit az Alkalmazást leíró vagy a Könyvtárat leíró űrlapján. Utána átnézheti a jogosultságok típusait, amelyeket felhasználhat az erőforrás biztonság tervezéséhez.

## A jogosultság típusainak megértése

Miután meghatározta saját erőforrás biztonságának céljait, és feljegyezte döntéseit a Könyvtárat leíró űrlapon, elkezdheti a jogosultság típusainak tervezését. Az erőforrás biztonság meghatározza, hogy a felhasználók hogyan érik el az objektumokat a rendszerben.

A **Jogosultság** azt jelenti, hogy valaki hogyan van feljogosítva egy objektum használatára. Például, lehet jogosultsága az információk megtekintésére vagy megváltoztatására a rendszeren. A rendszer több különböző jogosultság típust biztosít. Az IBM a jogosultság típusokat kategóriákba, úgynevezett **rendszer által megadott jogosultságokba** csoportosítja, amely legtöbb ember igényével találkozhat. Az alábbi táblázatok felsorolják a kategóriákat és ismertetik alkalmazhatóságukat a fájlok és programok biztonságához.

**Megjegyzés:** Olvassa el az alábbi táblázatokat, amikor a jogosultságokat tervezi.

38. táblázat: Rendszer által megadott jogosultságok

Jogosultság neve	Fájlokra megengedett műveletek	Fájlokra nem megengedett műveletek	Programokra megengedett műveletek	Programokra nem megengedett műveletek
*USE	Információ megtekintése a fájlban.	Információ törlése, módosítása a fájlban. Fájl törlése.	Program futtatása.	Program módosítása vagy törlése.
*CHANGE	Rekordok megtekintése, módosítása, törlése a fájlban.	Egész fájl törlése, tisztítása.	Programleírás módosítása.	Program módosítása vagy törlése.
*ALL	Fájl létrehozása és törlése. Rekordok felvétele, módosítása, törlése a fájlban. Fájlhasználat jogosultságának átadása.	Nincs	Program létrehozása, módosítása, törlése. Programhasználat jogosultságának átadása.	A program gazdájának módosítása örökölt jogosultságnál.
*EXCLUDE <sup>1</sup>	Nincs	Fájl elérése.	Nincs	Program elérése.
<p><b>1</b> Az *EXCLUDE felülbírálja a csoportprofilban megengedett nyilvános jogosultságot.</p>				

## Könyvtár- és objektum jogosultságok együttes munkája

Egyszerű erőforrás biztonság felépítéséhez próbálja meg a biztonságot az egész könyvtárra tervezni. Ehhez meg kell értenie, hogy a rendszer által megadott jogosultságok hogyan vonatkoznak a könyvtárakra, amelyeket az alábbi táblázat mutat be:

39. táblázat: Rendszer által megadott jogosultságok a könyvtárakhoz

Jogosultság neve	Megengedett műveletek	Nem megengedett műveletek
*USE	<ul style="list-style-type: none"> <li>Könyvtár objektumára: a jogosultság által megengedett művelet a megadott objektumra.</li> <li>Könyvtárra: leíró információ megtekintése.</li> </ul>	<ul style="list-style-type: none"> <li>Új objektum felvétele a könyvtárba.</li> <li>Könyvtárleírás módosítása.</li> <li>Könyvtár törlése.</li> </ul>
*CHANGE	<ul style="list-style-type: none"> <li>Könyvtár objektumára: a jogosultság által megengedett művelet a megadott objektumra.</li> <li>Új objektum felvétele a könyvtárba.</li> <li>Könyvtárleírás módosítása.</li> </ul>	<ul style="list-style-type: none"> <li>Könyvtár törlése.</li> </ul>
*ALL	<ul style="list-style-type: none"> <li>Minden módosítás engedélyezve.</li> <li>Könyvtár törlése.</li> <li>Mások feljogosítása a könyvtárhoz.</li> </ul>	<ul style="list-style-type: none"> <li>Nincs</li> </ul>

Meg kell érteni a könyvtár- és objektum jogosultságok együttes munkáját. Az alábbi táblázat példákat mutat be jogosultságokra, amelyek szükségesek mind az objektumhoz, mind a könyvtárhoz:

40. táblázat: Könyvtár- és objektum jogosultságok együttes munkája

Objektum típusa	Műveletek	Szükséges objektum jogosultság	Szükséges könyvtár jogosultság
Fájl	Adatváltoztatás	*CHANGE	*USE
Fájl	Fájl törlése.	*ALL	*USE
Fájl	Fájl létrehozása	*ALL	*CHANGE
Program	Program futtatása	*USE	*USE
Program	Programváltoztatás (újraserkesztés)	*ALL	*CHANGE
Program	Program törlése	*ALL	*USE

A katalógus jogosultság hasonló a könyvtár jogosultsághoz. Rendelkeznie kell jogosultsággal az objektum eléréséhez az útvonalba eső összes katalógusra.

Most készen áll az Alkalmazás könyvtárak biztonságának tervezésére.

## Alkalmazási könyvtárak biztonságának tervezése

Miután meghatározta saját erőforrás biztonságának céljait, elkezdheti az alkalmazási könyvtárak biztonságának tervezését. Válasszon ki egyet az alkalmazási könyvtárai közül, melyen végig követheti az itt leírt eljárást. Ha a rendszer külön könyvtárakban tárolja programjait és fájljait, válasszon egy fájlokat tartalmazó könyvtárat. Mikor befejezte a témakört, ismétlje meg a lépéseket a fennmaradt alkalmazási könyvtárakra is.

Nézze át az alkalmazásokról és a könyvtárakról összegyűjtött anyagokat:

- Alkalmazást leíró űrlap

- Könyvtár leíró űrlap
- Felhasználói csoportot leíró űrlap arra a csoportra vonatkozóan, amelyiknek szüksége van a könyvtárra
- Alkalmazásainak, könyvtárainak és felhasználói csoportjainak diagramja

Gondolja végig, mely csoportoknak kell információ a könyvtárból, miért kell nekik, mit kell tenniük vele.

### Könyvtár tartalmának meghatározása

Az alkalmazási könyvtárak a fontos alkalmazási fájlokat tartalmazzák. Más objektumokat is tartalmazhatnak, leginkább az alkalmazás megfelelő futásához szükséges programozási eszközöket, úgymint:

- Munka fájlok
- Adatterületek és üzenetsorok
- Programok
- Üzenetfájlok
- Parancsok
- Kimeneti sorok

Az objektumok többsége, a fájlok és kimeneti sorok kivételével, nem jelentenek biztonsági kockázatot. Általában csak kevés alkalmazási adatot tartalmaznak, gyakran olyan formában, hogy a programokon kívül nem ismerhető fel. Kilistáztathatja a könyvtár összes objektumának nevét és leírását a Display Library parancs használatával. Például, a CONTRACTS könyvtár kilistázásához szükséges parancs: `DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)`

A következő feladat annak eldöntése, hogy milyen nyilvános jogosultságot adjon az alkalmazási könyvtáraknak és a program könyvtáraknak.

### Alkalmazási könyvtárak nyilvános jogosultságának eldöntése

Az erőforrás biztonság szempontjából a **nyilvánosság** a rendszer összes jogosult bejelentkezőjét jelenti. A **nyilvános jogosultság** lehetővé teszi, hogy a felhasználó hozzáférjen az objektumhoz, ha nem rendelkezik más egyedi hozzáférési lehetőséggel. A könyvtárban lévő objektumok nyilvános jogosultságának eldöntésén túlmenően azt is meghatározhatja, hogy a könyvtárhoz később adandó új objektumok milyen nyilvános jogosultsággal rendelkezzenek. Ehhez a **Create Authority (CRTAUT)** paramétert használhatja. Általában a meglévő könyvtárobjektumok és az újonnan létrehozott objektumok nyilvános jogosultsága azonos.

A QCRTAUT (Create Authority) rendszerváltozó határozza meg az új objektumok nyilvános jogosultságát a rendszer teljes egészében. Az IBM \*CHANGE értékkel szállítja a QCRTAUT rendszerváltozót. Kerülje el a QCRTAUT megváltoztatását, mivel igen sok rendszerfunkció használja. Ha \*SYSVAL értéket ad meg egy alkalmazási könyvtár Create Authority (CRTAUT) opciójára, akkor ez a QCRTAUT rendszerváltozó (\*CHANGE) értékét használja.

Használja a nyilvános jogosultságot amennyire csak lehet az egyszerűség és a jó teljesítmény biztosítása végett. Feleljen az alábbi kérdésekre annak érdekében, hogy eldöntse melyik nyilvános jogosultságot rendeli a könyvtárhoz:

- A könyvtárban lévő információ többségét mindenkinek el kell érni a vállalatnál?
- A könyvtárban lévő információ többségének milyen elérési módja szükséges az embereknek?

A döntéskor koncentráljon az emberek és az információk többségére. Később meg fogja tanulni, mit tehet a kivételekkel. Az erőforrás biztonság tervezése gyakran körkörös folyamat. Rájöhet, hogy változtatásokat kell eszközölnie a nyilvános jogosultságban az adott objektumra vonatkozó igények figyelembevételét követően. Próbálja ki mind a könyvtárak, mind az objektumok nyilvános és magán jogosultságainak néhány kombinációját mielőtt kiválasztaná a biztonsági és a teljesítmény igényeknek is megfelelő változatot.

### Elegendő jogosultság biztosítása

A legtöbb alkalmazási funkció számára megfelelő az objektumok \*CHANGE és a könyvtárak \*USE jogosultsága. Azonban meg kell kérdeznie a programozót vagy az alkalmazás szállítóját annak tisztázására, hogy bizonyos alkalmazási funkciók nem igényelnek-e több jogosultságot:

- Törlődik-e fájl vagy más objektum a könyvtárban a feldolgozás alatt? Lesz-e fájl kitörölve? Lesznek-e emberek hozzáadva a fájlokhoz? Az objektum törlése, fájl kitakarítása, vagy member fájlhoz adása \*ALL jogosultságot igényel az objektumra.
- Létrehozódik-e fájl vagy más objektum a könyvtárban a feldolgozás alatt? Objektum létrehozásához \*CHANGE jogosultság kell a könyvtárra vonatkozóan.

Szándékában állhat példaként átnézni, hogy Sharon milyen jogosultságokat választott ki az objektumokhoz, mielőtt eldöntené a programkönyvtárak nyilvános jogosultságát.

#### **Példa: JKL Toy Company Könyvtár leíró űrlap:**

Sharon Jones áttekintette az ügyfélnyilvántartó (Customer Records) könyvtárat, továbbá a könyvtár információit használó alkalmazások és osztályok meglévő adatait. Megjegyzéseket készített a következtetésekről:

- Minden osztálynak, kivéve a raktárnak és a gyártásnak, szüksége van az ügyfélinformációk módosítási jogára.
- A raktár és a gyártás minden dolgozójának Korlátolt képességek (Yes) beállítású felhasználói profilja van, és így csak megadott menüket és programokat használhatnak. A menük engedélyezik az ügyfélinformációk megtekintését, változtatását azonban nem.
- A Customer Records könyvtár objektumainak nyilvános jogosultsága \*CHANGE értékre állítható. A menü korlátozások megakadályozzák az ügyfélinformációk jogosulatlan módosítását. Azonban, ezt ismét át kell tekinteni, ha a rendszerhez újabb osztályok csatlakoznak a későbbiekben.

Ez jó példa a kevésbé szigorú biztonsági megközelítésre. Ebben az esetben a kivételek a felhasználói profilon keresztül vannak érvényesítve, és nem a jogosultság korlátozásával. Sharon kitöltötte a Könyvtár leíró űrlapon a nyilvános jogosultságot a Customer Records (CUSTLIB) könyvtárra vonatkozóan.

41. táblázat: JKL Toy Company Könyvtár leíró űrlap — első rész: Customer Records példa

Könyvtár neve: CUSTLIB	Leírónév (szöveg): Customer Records
Könyvtár nyilvános jogosultsága:	*USE
Objektum nyilvános jogosultsága a könyvtárban:	*CHANGE
Új objektumok (CRTAUT) nyilvános jogosultsága:	*CHANGE

Sharon Jones felfedezte, hogy a Vevő tartozások alkalmazás hóvégi feldolgozásakor néhány ideiglenes fájl az ügyfélnyilvántartó könyvtárban kitakarításra kerül. Azt választotta, hogy egyedi jogosultságokkal kezeli ezeket a fájlokat, és nem vállalja azt a kockázatot, hogy a könyvtár más fontos eleme véletlenül törlésre kerüljön. Az összes többi feldolgozásra a \*CHANGE jogosultság megfelelő.

Mivel a hóvégi feldolgozást kevés ember futtatja, Sharon nem fél attól, hogy az ideiglenes fájlok biztonsági kockázatot jelentenek. Elhatározta, hogy inkább a fájloknak ad nyilvános \*ALL jogosultságot, mint a hóvégi feldolgozást végző személyeknek. Az alábbi táblázat mutatja a Könyvtár leíró űrlap második részét a Customer Records könyvtárra vonatkozóan:

42. táblázat: JKL Toy Company Könyvtár leíró űrlap — második rész: Customer Records példa

Könyvtári objektumok egyedi jogosultságainak listája				
Csoport- vagy felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági lista
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

Most eldöntheti a programkönyvtárak nyilvános jogosultságát.

## Programkönyvtárak nyilvános jogosultságának eldöntése

Az alkalmazási programok gyakran a fájloktól és az objektumoktól elkülönített könyvtárban találhatóak. Bár nem kötelező külön könyvtárak használata az alkalmazások számára, de nagyon sok programozó alkalmazza ezt a módszert az alkalmazások tervezésekor. Ha az alkalmazása külön programkönyvtárakkal rendelkezik, döntenie kell azok nyilvános jogosultságáról is. A \*USE jogosultság megfelelő mind a könyvtár, mind a könyvtárban lévő programok számára a programok futásához, de a könyvtárakban lehetnek olyan más objektumok is, amelyek további jogosultságot igényelnek. Tegyen fel néhány kérdést a programozónak:

- Használ az alkalmazás adatterületeket vagy üzenetsorokat a programok közötti kapcsolatra? Ezek a programkönyvtárban vannak? \*CHANGE objektumjogosultság szükséges az adatterületek és az üzenetsorok kezeléséhez.
- Vannak-e olyan objektumok a programkönyvtárban, mint például adatterületek, amelyek a feldolgozás alatt törölődnek? \*ALL jogosultság szükséges az objektum törléséhez.
- Vannak-e olyan objektumok a programkönyvtárban, mint például adatterületek, amelyek a feldolgozás alatt jönnek létre? \*CHANGE jogosultság szükséges új objektum létrehozásához a könyvtárban.

Töltse ki a Könyvtár leíró űrlap erőforrás biztonságra vonatkozó részeit a könyvtár tulajdonjog és a jogosultsági lista kivételével. Azután meghatározhatja a könyvtárak és objektumok tulajdonosait.

Szándékában állhat átnézni a következő két példát, hogy Sharon Jones hogyan határozta meg a jogosultságokat a programkönyvtárakhoz. Az első példában Sharon eldöntötte, hogy a korlátlan megközelítés megfelelő a vevő rendelések programkönyvtárához. A második példában több korlátozás is van, amelyet Sharon alkalmazott a vevő tartozások programkönyvtárához.

**Példa: JKL Toy Company Könyvtár leíró űrlap — nem korlátozó megközelítés:** Sharon Jones megvizsgálta a Vevő rendelés programkönyvtárát és az alábbi megjegyzéseket fűzte hozzá:

- Egy üzenetsor (COMSGQ01) szolgál a programok közötti kommunikációra.
- Az üzenetsor kitarakításra kerül, de törlésre sohasem. A \*CHANGE jogosultság megfelelő az üzenetsorhoz.

Sharon elhatározta, hogy \*USE jogosultságot ad a programkönyvtár minden objektumára és a COMSGQ01 üzenetsorra külön jogosultságot definiál. Az alábbi két táblázat mutatja be Könyvtár leíró űrlapját a COPGMLIB könyvtárra:

43. táblázat: JKL Toy Company Könyvtár leíró űrlap: Programkönyvtár példa

Könyvtár leíró űrlap		Első rész
Könyvtár neve: COPGMLIB	Leírónév (szöveg): Customer Order Program Library	
Könyvtár nyilvános jogosultsága: *USE		
Objektum nyilvános jogosultsága a könyvtárban: *USE		
Új objektumok (CRTAUT) nyilvános jogosultsága: *USE		
Könyvtár tulajdonosa:		

44. táblázat: JKL Toy Company Könyvtár leíró űrlap: Programkönyvtár példa

Könyvtár leíró űrlap				Második rész
Jogosultságok a könyvtár egyedi objektumaihoz				
Csoportprofil, felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági listák
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

## Programjogosultság használata elérés vezérléshez

Habár a JKL Toy Company legtöbb dolgozója jogosult az ügyfélinformációk módosítására, csak kevés ember állíthatja be az ügyfelek számlalimitjét. A számlalimitek a Customer Master (CUSTMAS) fájlban vannak, de módosításukra külön program, nevezetesen az ARPGM12 szolgál az ARPGMLIB könyvtárban. Sharon korlátozhatja a program használatát, így megelőzve azt, hogy jogosulatlan személy megváltoztathassa a számlalimiteket. Az alábbi táblázatok mutatják be az ARPGMLIB könyvtárra vonatkozó Könyvtár leíró űrlapot:

45. táblázat: JKL Toy Company Könyvtár leíró űrlap: Egyedi jogosultságok példa

Könyvtár leíró űrlap		Első rész
Könyvtár neve: ARPGMLIB	Leírónév (szöveg): Accounts Receivable Program Library	
Könyvtár nyilvános jogosultsága: *USE		
Objektum nyilvános jogosultsága a könyvtárban: *USE		
Új objektumok (CRTAUT) nyilvános jogosultsága: *USE		
Könyvtár tulajdonosa:		

46. táblázat: JKL Toy Company Könyvtár leíró űrlap: Egyedi jogosultságok példa

Könyvtár leíró űrlap			Második rész	
Jogosultságok a könyvtár egyedi objektumaihoz				
Csoportprofil, felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági listák
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

Szándékában állhat áttekinteni egy korlátozó példát is, amely örökölt jogosultságot használ, mielőtt meghatározná a könyvtárak és objektumok tulajdonjogát.

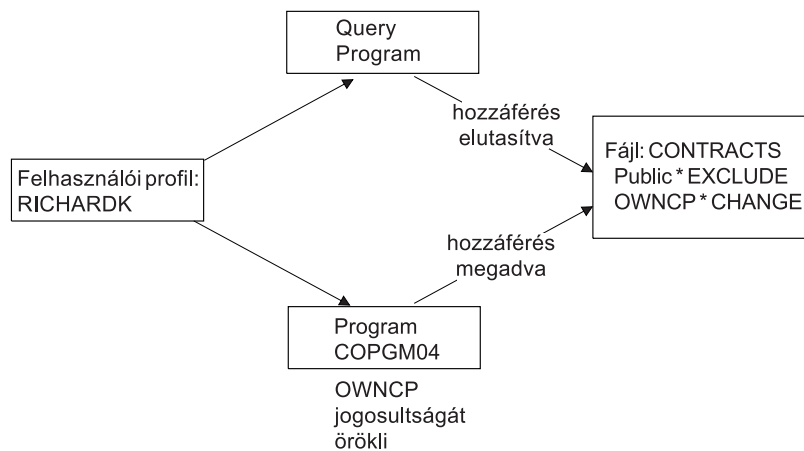
**Példa: JKL Toy Company Könyvtár leíró űrlap — korlátozó megközelítés:** Az eddig bemutatott példák a biztonság korlátlan megközelítésén alapultak, ahol az emberek többsége elérte a könyvtár tartalmát. A JKL Toy Company szerződési és árinformációi bizalmasnak és titkosnak tekinthetők és korlátozott megközelítést igényelnek. Szerencsére az összes ilyen információ külön könyvtárban van. A szerződéseket és árakat naprakészé tevő program szintén egy speciális könyvtárban van.

Sharon áttekintette a Szerződések és árak nevű alkalmazás biztonsági elemeit (Erőforrás biztonság céljainak meghatározása). Ugyancsak átnézte az Alkalmazást leíró és a Könyvtár leíró űrlapokat is. Sharon úgy érezte, nehéz összeegyeztetni a biztonsági elemeket az alkalmazással. Néhány megjegyzést fűzött hozzá és elhatározta, hogy megbeszéli a problémát az alkalmazás szállítójával:

- A Kereskedelmi és marketing osztály dolgozóinak, valamint a menedzsereknek kell létrehozni és módosítani szerződéseket. Nekik mind a programokat, mind a fájlokat használniuk kell.
- A Rendelésfeldolgozó osztály emberei indirekt módon módosítják a szerződéseket és látják az árakat rendelések felvételénél és kiszállításánál, de semmilyen más esetben nem láthatják azokat. Ők ugyan használni fognak Query programot saját - ügyfelekről és rendelésekről szóló - jelentéseik elkészítéséhez. Ha jogosultságot kapnak a Szerződések és árak nevű alkalmazás fájljaihoz, akkor Query programokat kellene létrehozni a megtekintésükhöz és nyomtatásukhoz.

Az alkalmazás szállítója az örökölt jogosultság lehetőségét ajánlotta a JKL Toy Company számára a probléma megoldásához. Az **örökölt jogosultság** lehetővé teszi a felhasználónak, hogy a program futása alatt örökölje a program tulajdonosának jogosultságait. A felhasználónak nem kell, hogy jogosultsága legyen az objektumhoz.

Az alábbi diagram bemutatja az örökölt jogosultság működését egy mintán keresztül. Karen Richards (RICHARDK) a Rendelésfeldolgozó osztály embere normális esetben nem jogosult a Contracts fájl használatára. Habár, mikor rendelést vesz fel, ellenőriznie és módosítania kell a szerződés mérlegét. A rendelést bevívó program (COPGM04), mely a szerződés mérlegével is dolgozik, örökli a OWNCP profil jogosultságait. Így, míg Karen a COPGM04 programot használja jogosult lesz a Contracts fájl használatára:



RV2L238-4

Az objektumok tulajdonjogáról további tájékoztatást kaphat a "Könyvtárak és objektumok tulajdonjogának meghatározása" című részben. Az alkalmazás szállítója vagy programozója megadhatja azt, hogy a program örökölje a tulajdonos jogosultságait, amikor létrehozza (fordítja) a programot, illetve később is megteheti ezt a programozó a Change Program (CHGPGM) paranccsal. Győződjön meg róla, hogy érti a program összes funkciójának a működését, mielőtt alkalmazná a fenti technikát.

Sharon elhatározta, hogy kihasználja az örökölt jogosultság funkciót a Szerződések és árak nevű alkalmazás fájljainak eléréséhez a Kereskedelmi és marketing osztályon kívül állók esetében. Eldöntötte azt is, hogy a \*CHANGE elérés megfelelő volt a Szerződések és árak nevű alkalmazás által használt összes objektumra. Az alábbi táblázat mutatja be a Contracts könyvtárra vonatkozó Könyvtár leíró űrlapot:

47. táblázat: JKL Toy Company Könyvtár leíró űrlap: Korlátozó jogosultságok példa

Könyvtár leíró űrlap		Első rész
Könyvtár neve: CONTRACTS	Leírónév (szöveg): Contracts and Pricing Library	
Könyvtár nyilvános jogosultsága: *EXCLUDE		
Objektum nyilvános jogosultsága a könyvtárban: *CHANGE		
Új objektumok (CRTAUT) nyilvános jogosultsága: *CHANGE		
Könyvtár tulajdonosa:		

48. táblázat: JKL Toy Company Könyvtár leíró űrlap: Korlátozó jogosultságok példa

Könyvtár leíró űrlap				Második rész
Jogosultságok a könyvtár egyedi objektumaihoz				
Csoportprofil, felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági listák
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

Nincs szükség arra, hogy korlátozza a könyvtárban lévő objektumok elérését, mivel magához a könyvtárhoz való hozzáférést korlátozta. Sharon ezenkívül a menedzsereknek, valamint a Kereskedelmi és marketing osztálynak adott jogosultságot a könyvtárhoz. Csoport jogosultságot használt egyedi jogosultságok megadása helyett.

**Megjegyzés:** Képzett programozó, aki eléri a könyvtárat, képes lehet a könyvtárban lévő objektumok elérési jogát megtartani még azután is, hogy a könyvtár jogosultsága vissza lett vonva. Ha egy könyvtár nagy biztonsági igényű objektumokat tartalmaz, korlátozza a könyvtárat és az objektumokat is a komplett védelem érdekében.

Szándékában állhat áttekinteni egy nem korlátozó példát is, amely nyilvános jogosultságot használ, mielőtt meghatározná a könyvtárak és objektumok tulajdonjogát.

## Könyvtárak és objektumok tulajdonosának meghatározása

Miután megtervezte az alkalmazási könyvtárak biztonságát, dönthet a könyvtárak és objektumok tulajdonjogáról. Minden objektum kap egy tulajdonost a létrehozásakor. Az objektum tulajdonosa automatikusan minden jogosultságot megkap az objektumra, ami magában foglalja azt a lehetőséget is, hogy feljogosíthat másokat az objektum használatára, módosítására és törlésére. A biztonsági felelős végrehajthatja ezeket a funkciókat a rendszer bármely objektumán.

A rendszer az objektum tulajdonosának profilját használva tudja követni, hogy kinek van jogosultsága az objektumhoz. A rendszer belsőleg hajtja végre ezt a funkciót. Ez a funkció nem feltétlenül hat közvetlenül a felhasználói profilra. Azonban, ha nem tervezte meg megfelelően az objektumok tulajdonjogait, néhány felhasználói profil túl nagyra nőhet.

Amikor a rendszer elment egy objektumot, vele együtt elmenti a tulajdonos profil nevét is. A rendszer felhasználja ezt az információt az objektum visszaállításakor. Ha a visszatöltött objektum tulajdonosának profilja nincs a rendszerben, a rendszer átadja a tulajdonjogot a QDFTOWN IBM profilnak.

### Javaslatok

Az alábbi javaslatok sokszor, de nem minden esetben alkalmazhatók. A javaslatok áttekintése után beszélje meg elgondolásait az objektumok tulajdonjogáról programozójával vagy az alkalmazás szállítójával. Ha vásárolt alkalmazása van, lehet, hogy nem tudja irányítani, melyik profil birtokolja a könyvtárakat és az objektumokat. Az alkalmazás felépülhet úgy is, hogy nem engedélyezi a tulajdonjog megváltoztatását.

- Ha lehet, kerülje az IBM profilok (úgy mint QSECOFR vagy QPGMR) használatát alkalmazás tulajdonosaként. Ezek a profilok sok objektumot birtokolnak és már nagyon nagyok.
- Normális esetben a csoportprofil nem birtokol alkalmazást. A csoport minden tagja a csoportprofilban megadott jogosultságokkal bír mindaddig, míg alacsonyabb jogosultságot nem rendel hozzá. Valójában, az alkalmazáshoz szükséges összes jogosultságot kellene biztosítania a csoport minden tagjának.
- Ha kiadja az alkalmazások vezérlésének felelősségét a vezetőknek a különböző osztályokon, akkor nekik kell az alkalmazási objektumok tulajdonosainak lenni. Mindazonáltal, az alkalmazás vezetőinek változhat a beosztása. Ha ez az eset áll fenn, az alkalmazás összes objektumának tulajdonjogát adja át az új vezetőnek.
- Sok ember használja egy speciális tulajdonosi profil létrehozásának technikáját minden egyes alkalmazáshoz, a jelszó \*NONE-ba állítása mellett. A rendszer az alkalmazási jogosultságok kezelésére használja a tulajdonosi profilt. A biztonsági felelős (vagy valaki más ilyen jogosultsággal) végzi az alkalmazás valódi kezelését, illetve a feladat delegálása esetén a vezetők, akik \*ALL jogosultsággal bírnak az adott alkalmazásokra.

Döntse el, melyik profilok birtokolják az alkalmazásokat. Írja be a tulajdonos profiljának adatait a Könyvtárat leíró úrlapon.

Szándékában állhat példaként átnézni, hogy a JKL Toy Company hogyan határozta meg az alkalmazás tulajdonjogát, mielőtt döntene a felhasználói könyvtárak tulajdonjogáról és eléréséről.

### Példa: JKL Toy Company alkalmazásainak tulajdonjoga

Sharon Jones elhatározta, hogy minden alkalmazáshoz létrehoz speciális tulajdonosi profilt. Ő és Ken Harrison - a helyettese - lesz felelős az alkalmazások biztonságának kezeléséért. Később, mikor a vállalati biztonsági igények komplexebbé válnak, Sharon delegálhat néhány biztonságkezelési feladatot az osztályvezetőknek.



Sharon kiegészítette saját Elnevezési szabályok űrlapját az alábbiakkal:

49. táblázat: JKL Toy Company Elnevezési szabályok űrlap: tulajdonosi profil példa

Objektum típusa	Elnevezési szabályok
Tulajdonosi profil	Egy-egy tulajdonosi profil lesz létrehozva minden alkalmazás részére. Ezek fogják birtokolni az egyes alkalmazások összes könyvtárát és objektumát. A tulajdonosi profil neve OWN plusz az alkalmazás rövidítése lesz. A Készletgazdálkodás (Inventory Control) tulajdonosi profilja OWNIC lesz.

Sharon elhatározta, hogy minden tulajdonosi profil OWN betűkkel kezdődik, aminek következtében a képernyőn és a nyomtatott listán is együtt jelennek meg.

Sharon hozzárendelte a tulajdonosokat az alkalmazási könyvtárakhoz, és leírta az új adatokat az Elnevezési szabályok űrlapokon is. Csak egy könyvtár - Customer Records (CUSTLIB) - volt, amelynek több alkalmazás a tulajdonosa. Mivel a Vevő tartozások nevű alkalmazás hoz létre új ügyfelet és állítja a számlalimitet, Sharon elhatározta, hogy ez lesz a tulajdonosa az ügyfél fájloknak. Tulajdonosok a hozzárendelése alapján:

Könyvtár neve	Tulajdonos neve
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

Most dönthet a felhasználói könyvtárak tulajdonjogáról és eléréséről.

## Felhasználói könyvtárak elérésének és tulajdonjogának meghatározása

Ha a rendszerben van IBM Query for iSeries vagy más döntéselőkészítő program, a felhasználóknak szükségük van egy könyvtárra, ahol a létrehozott query programokat tárolják. Normál esetben ez van megadva **aktuális könyvtárként** a felhasználói profilban. A "Bejelentkezést befolyásoló rendszerváltozók kiválasztása" című részben további tájékoztatást talál az egyes felhasználók aktuális könyvtárainak létrehozásáról. Sharon Jones úgy tervezi, hogy a Kereskedelmi és marketing osztály használja az aktuális könyvtárakat, míg a többi osztály a csoport könyvtárakat:

- Az SM osztály dolgozói erős felhasználói a Query programnak. Mindegyik felhasználónak saját könyvtárat kell biztosítani. Különböző, aggódnának a létrehozott lekérdező programok elnevezésén és fennáll a veszély, hogy véletlenül törlik egymás programjait.
- Kezdetben a többi osztály csoportkönyvtárakkal rendelkezik. Ha nagyon sok Query programot hoznak létre, megfontoljuk egyedi könyvtárak létrehozását.

Ha egy felhasználó egy csoporthoz tartozik, használhatja a felhasználói profilban lévő mezőt annak definiálására, hogy a felhasználó által létrehozott objektumokat a felhasználó vagy a csoport birtokolja-e. Ha a felhasználó birtokolja az objektumokat, akkor megadhatja, hogy milyen jogosultságokkal használhatják a csoporttagok. Ugyancsak megadhatja azt is, hogy a csoportjogosultság magánjogosultság-e vagy elsődleges csoportjogosultság. Az elsődleges csoportjogosultság jobb rendszerteljesítményt nyújthat. Sharon néhány további megjegyzést fűzött a felhasználói könyvtárakhoz:

- Jobb, ha a Kereskedelmi és marketing osztály emberei saját maguk birtokolják a létrehozott objektumaikat, mint ha csoport birtokolná. Nem kell nekik módosítani egymás lekérdező programjait.
- A csoportban mindenkinek tudni kell futtatni a másik lekérdező programjait, ami azt jelenti, hogy a csoport \*USE jogosultságot kap minden létrehozott objektumhoz.
- A csoportjogosultságnak elsődleges csoportjogosultságnak kell lenni.
- A nyilvánosság nem érheti el ezeket a könyvtárakat. A Kereskedelmi és marketing osztályon futtatott lekérdezéseknek lehet kimeneti fájlja. Ezek a fájlok tartalmazhatnak bizalmas adatokat.

- A többi osztálynál a csoport birtokolja saját csoportkönyvtárát és minden létrehozott objektumot a könyvtárban. Ez azt jelenti, hogy a csoport bármelyik tagja bármit törölhet a csoportkönyvtárban. Ha ez valamilyen problémát okoz, más módszert fogunk megpróbálni.

A táblázat a Kereskedelmi és marketing osztály számára készült Egyedi felhasználói profil űrlapot mutatja, ahol a felhasználók birtokolják az objektumokat:

50. táblázat: JKL Toy Company Egyedi felhasználói profil űrlap: felhasználó által birtokolt objektumok

Csoportprofil neve: DPTSM	
Létrehozott objektumok gazdája: *USRPRF	Csoportjogosultság az objektumokhoz: *USE
Csoportjogosultság típusa: *PGP	

A táblázat az osztály számára készült Egyedi felhasználói profil űrlapot mutatja, ahol csoportok birtokolják az objektumokat:

51. táblázat: JKL Toy Company Egyedi felhasználói profil űrlap: csoport által birtokolt objektumok

Csoportprofil neve: DPTxx	
Létrehozott obj. gazdája: *GRPPRF	Csoportjogosultság az objektumokhoz:

A **Csoportjogosultság az objektumokhoz** mezőt nem használja, ha a létrehozott objektumok tulajdonosa a csoport. A csoporttagok automatikusan \*ALL jogosultsággal rendelkeznek a létrehozott objektumokra.

Döntse el, ki legyen a felhasználói könyvtárak tulajdonosa és kik érjék el. Adja meg választását a **Létrehozott obj. gazdája** és a **Csoportjogosultság az objektumokhoz** mezőkre az Egyedi felhasználói profil űrlapon. Most pedig készen áll az objektumok csoportosítására.

## Objektumok csoportosítása

Miután meghatározta a könyvtárak és objektumok tulajdonosait, hozzákezdhet a rendszeren az objektumok csoportosításához. A jogosultságok irányításának egyszerűsítése érdekében használjon jogosultsági listát az azonos biztonsági igényű objektumok összefogására. Könnyebben adhat nyilvános-, csoportprofil-, vagy felhasználói profil jogosultságokat a jogosultsági listának, mint az egyedi objektumoknak. A rendszer pontosan úgy kezeli az objektumokat, ahogy védi őket a jogosultsági listával, de a különböző felhasználóknak különböző jogosultságokat adhat a lista révén.

A jogosultsági lista megkönnyíti a jogosultságok visszaállítását az objektumok visszatöltésekor. Ha az objektumokat jogosultsági listával védi, a visszatöltési eljárás automatikusan hozzáadja az objektumokat a listához.

Adhat csoportnak vagy felhasználónak jogosultságot jogosultsági lista irányítására (\*AUTLMGT). A Jogosultsági lista irányítása jog lehetőséget ad a felhasználónak, hogy más felhasználókat felvegyen vagy eltávolítson a listából, és módosíthassa azok jogosultságát.

### Javaslatok

- Használja a jogosultsági listát azokra az objektumokra, amelyek védeltséget igényelnek, de hasonló biztonsági igényeik vannak. A jogosultsági lista használata meggyőzheti arról, hogy inkább jogosultsági kategóriákban gondolkodjon, mintsem egyedi jogosultságokban. A jogosultsági lista könnyebbé teszi az objektumok visszatöltését és a jogosultságok felülvizsgálatát a rendszerben.
- A komplikált sémák elkerülése érdekében kombinálja a jogosultsági listákat, csoport- és egyedi jogosultságokat. Válassza a követelményeknek legjobban megfelelő kombinációt, mintsem mindig ugyanazt a módszert kövesse.

A jogosultsági lista elnevezésére vonatkozó elgondolásait ugyancsak írja le az Elnevezési szabályok űrlapon.

Amint elkészítette a Jogosultsági lista űrlapot, térjen vissza a Könyvtár leíró űrlaphoz, és írja be a megfelelő adatokat. A programozónak vagy az alkalmazás szállítójának már lehet, hogy van elkészített listája. Ellenőrizze velük.

Hasznosnak találhatja, ha megismerkedhet egy példán keresztül azzal, hogy Sharon Jones hogyan tervezte meg a JKL Toy Company cégnél a jogosultsági listákat, mielőtt a nyomtatók és a nyomtatandó anyag biztonságának tervezését elkezdené.

### Példa: JKL Toy Company Jogosultsági lista űrlap

Sharon áttekintette a Customer Records (CUSTLIB) könyvtár leírását, és úgy döntött, hogy létrehoz jogosultsági listát azokra a fájlokra, amelyek a hóvégi feldolgozáskor kitakarításra kerülnek. Habár csak három fájlról van szó, Sharon mégis elhatározta a jogosultsági lista létrehozását a jogosultságok irányításának egyszerűsítése végett. Ha később további fájlok kerülnek bele a hóvégi feldolgozásba, könnyedén hozzárendelheti őket a listához. Sharon elhatározta a fájlok kizárását a nyilvánosságból, megelőzve ezzel véletlen problémák jelentkezését hóvégi feldolgozáskor. Csak a feldolgozást végzőknek adott \*ALL jogosultságot. Rose Willis, rendszeroperátornak esténként meg kell tekinteni a fájlinformációkat a hóvégi feldolgozás ellenőrzése végett. Neki \*USE jogosultságra van szüksége.

Az alábbi táblázat az elnevezési szabályokat mutatja be, amelyeket Sharon használt a jogosultsági listákhoz:

52. táblázat: JKL Toy Company Elnevezési szabályok űrlap: jogosultsági lista példa

Elnevezési szabályok űrlap	
Készítette: Sharon Jones	Dátum: 9/5/99
Objektum típusa	Elnevezési szabály
Jogosultsági listák	Az egy adott könyvtárban lévő objektumokat védő lista neve áll a könyvtár nevének egy részéből, plusz az LST betűkből és egy számból. A CUSTLIB könyvtárban lévő objektumokat védő lista neve CUSTLST1. Több könyvtárban lévő objektumok listájának nevéhez az alkalmazás rövidítését használjuk, ha lehet: ARLST1. Ha a listához több alkalmazás objektumai tartoznak egyéb értelmes nevet választunk. A lista leírása a lista fő célját kell, hogy tartalmazza.

Az alábbi táblázat mutatja be a CUSTLIB könyvtárra vonatkozó Jogosultsági lista űrlapot. Sharon felhasználta a Könyvtár leíró űrlap adatait is a Jogosultsági lista űrlap elkészítéséhez:

53. táblázat: JKL Toy Company Jogosultsági lista űrlap: példa

Jogosultsági lista űrlap					
Jogosultsági lista neve: CUSTLST1					
Leírás: Hóvégi feldolgozás során törölt fájlok.					
Lista által védett objektumok felsorolása					
Objektum neve	Objektum típusa	Objektum könyvtára	Objektum neve	Objektum típusa	Objektum könyvtára
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
Listához hozzáféréssel rendelkező csoportok és felhasználók					
Csoport vagy felhasználó	Megengedett elérés típusa	Lista irányítás?	Csoport vagy felhasználó	Megengedett elérés típusa	Lista irányítás?
PUBLIC	*EXCLUDE	Nem	ROSSG	*ALL	Nem
SMITHJ	*ALL	Nem	JONESS	*ALL	Igen
WILLISR	*USE	Nem			

Sharon egyúttal módosította a CUSTLIB könyvtárra vonatkozó Könyvtár leíró űrlapot is a jogosultsági lista információival:

Könyvtár leíró űrlap				Második rész
Készítette: Sharon Jones		Dátum: 9/9/99		
Könyvtár neve: CUSTLIB				
Könyvtári objektumok egyedi jogosultságainak listája				
Csoportprofil, felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági lista
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Megjegyzendő, hogy a nyilvános jogosultságot minden fájlra \*AUTL értékre kell állítani ahhoz, hogy a rendszer a jogosultsági lista alapján határozza meg a nyilvánossági jogosultságot.

Tekintse át a csoport- és egyedi jogosultságokat a Könyvtár leíró űrlapokon. Határozza meg szükséges-e jogosultsági lista létrehozása. Ha igen, készítse el a Jogosultsági lista űrlapokat, és módosítsa a Könyvtár leíró űrlapokat a jogosultsági listák adataival. Azután megtervezheti a nyomtatók és a nyomtatott anyagok biztonságát.

## Nyomtatók és nyomtatott listák biztonságának tervezése

Miután csoportosította az objektumokat, meg kell terveznie a nyomtatandó listák védelmét. Terveket készített a rendszerben tárolt információ védelmére. Ugyancsak terveket kell készíteni a bizalmas információ védelmére, nyomtatásra várakozás és nyomtatás alatti periódusra vonatkozóan. Ellenőrizze a Fizikai biztonság tervezésére szolgáló űrlapon azokat a nyomtatókat, amelyeket bizalmas anyagok kinyomtatására használnak.

Mikor egy programot futtat, amely riportot listáz, a riport általában nem megy közvetlenül a nyomtatóra. A program létrehozza a riport másolatát, amelyet **spool fájlnak** vagy **nyomtatandó anyagnak** hívhatunk. A rendszer eltárolja a nyomtatandó anyagot egy **kimeneti sornak** nevezett objektumba, amíg a nyomtató nem elérhető. Amikor a kimeneti sorban nyomtatandó anyag van, megtekintheti a listát a munkaállomásán. Lehetősége van ott tartani, vagy másik nyomtatóra átirányítani.

A "spool" technika könnyebbé teszi a nyomtatás rendjét és a nyomtatók megosztását. Ugyancsak segít a bizalmas anyagok védelmében. Létrehozhat egy vagy több speciális kimeneti sort a bizalmas anyagok tárolására és korlátozhatja ezen sorok megtekintését és kezelését. Azt is vezérelheti, hogy a titkos anyagok mikor kerüljenek a kimeneti sorból a nyomtatóra.

Töltse ki a Nyomtatott listák és munkaállomás biztonság űrlapját ahogy halad végig a témakörön.

Mikor létrehoz egy speciális kimeneti sort, specifikálhat néhány paramétert a biztonsággal kapcsolatban:

- **Display Data (DSPDTA) paraméter:** A kimeneti sor DSPDTA paramétere határozza meg, hogy a felhasználó láthatja-e, küldheti-e vagy másolhatja-e egy másik felhasználó "spool" fájlját.
- **Authority to Check (AUTCHK) paraméter:** A kimeneti sor AUTCHK paramétere határozza meg, hogy a felhasználó módosíthatja-e vagy törölheti-e egy másik felhasználó "spool" fájlját.
- **Operator Control (OPRCTL) paraméter:** A kimeneti sor OPRCTL paramétere határozza meg, hogy a \*JOBCTL speciális jogosultságú (vagy \*SYSOPR felhasználói osztályú) felhasználó vezérelheti-e a kimeneti sort.

A kimeneti sor paramétere, a kimeneti sorra vonatkozó felhasználói jogosultságok és a speciális jogosultságok együttes munkája határozza meg azokat a funkciókat, amelyeket a felhasználó végrehajthat a kimeneti sorban lévő "spool" fájlokkal. Az alábbi táblázat megmutatja, hogy milyen kombinációk mellett a felhasználó milyen funkciókat hajthat végre:

Nyomtatási funkciók	Output Queue paraméters			Kimeneti sor jogosultság	Egyedi jogosultság
	DSPDTA	AUTCHK	OPRCTL		

"Spool" fájl felvétele a sorba <sup>1</sup>	Tetszőleges	Tetszőleges	Tetszőleges	*READ	Nincs
	Tetszőleges	Tetszőleges	*Yes	Tetszőleges	*JOBCTL
"Spool" fájlok listájának megtekintése (WRKOUTQ parancs) <sup>2</sup>	Tetszőleges	Tetszőleges	Tetszőleges	*READ	Nincs
	Tetszőleges	Tetszőleges	*Yes	Tetszőleges	*JOBCTL
"Spool" fájlok megjelenítése, másolása, küldése (DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPFL) <sup>2</sup>	*YES	Tetszőleges	Tetszőleges	*READ	Nincs
	*NO	*DTAAUT	Tetszőleges	*CHANGE	Nincs
	*NO	*OWNER	Tetszőleges	Gazda <sup>3</sup>	Nincs
	*YES	Tetszőleges	*Yes	Tetszőleges	*JOBCTL
	*NO	Tetszőleges	*Yes	Tetszőleges	*JOBCTL
	*OWNER <sup>5</sup>	Tetszőleges	Tetszőleges	Tetszőleges	Tetszőleges
"Spool" fájlok módosítása, törlése, tartása, felszabadítása (CHGSPLFA, DLTSPLF, HLDSPFL, RLSSPLF) <sup>2</sup>	Tetszőleges	*DTAAUT	Tetszőleges	*CHANGE	Nincs
	Tetszőleges	*OWNER	Tetszőleges	Gazda <sup>3</sup>	Nincs
Kimeneti sor módosítása, törlése, tartása, felszabadítása (CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT) <sup>2</sup>	Tetszőleges	*DTAAUT	Tetszőleges	*CHANGE	Nincs
	Tetszőleges	*OWNER	Tetszőleges	Gazda <sup>3</sup>	Nincs
	Tetszőleges	Tetszőleges	*YES	Tetszőleges	*JOBCTL
Írás indítása a sorra (STRPRTWTR, STRRMTWTR) <sup>2</sup>	Tetszőleges	*DTAAUT	Bármí	*CHANGE <sup>4</sup>	Nincs
	Tetszőleges	Bármí	*YES	Bármí <sup>4</sup>	*JOBCTL
<p><b>1</b> Ez a jogosultság szükséges a nyomtatandó anyag kimeneti sorba irányításához.</p> <p><b>2</b> Használva ezeket a parancsokat vagy ekvivalens opciókat képernyőről.</p> <p><b>3</b> A kimeneti sor tulajdonosának (gazdájának) Önnek kell lenni.</p> <p><b>4</b> Szintén *USE jogosultság kell a nyomtatóegység leíráshoz.</p> <p><b>5</b> A "spool" fájl tulajdonosának kell lenni, vagy *SPLCTL speciális jogosultsággal kell rendelkezni ahhoz, hogy használja ezt a parancsot.</p>					

Nézze át a Fizikai biztonsági terv nyomtatókról szóló részét. Töltse ki a Nyomtatott listák és munkaállomás biztonság úrlapját ahogy halad végig a témakörön.

Hasznosnak találhatja, ha megismerkedhet egy példán keresztül azzal, hogy Sharon Jones hogyan határozta meg a JKL Toy Company cégnél a kimeneti sorok paramétereit, mielőtt megtervezné a munkaállomások biztonságát.

### **Példa: JKL Toy Company Kimeneti sor és munkaállomás biztonság úrlapja — kimeneti sor**

A JKL Toy Company Kereskedelmi és marketing osztálya két esetben nyomtat bizalmas információkat:

- Előzetes árlisták, melyek az árváltozás tervezési időszakában kerülnek nyomtatásra. Az osztályon és a vállalat vezetőin kívül senki sem láthatja a kinyomtatott információt.
- A szerződések is bizalmasak tárgyalásuk időszakában. A szerződés első fogalmazásában csak a róla tárgyaló személy által látható még az osztályon belül is.

Sharon elhatározta két speciális kimeneti sor létrehozását:

#### **PRICEQ**

Az elsődleges árlisták részére lesz használva. Az osztály bármely dolgozója végrehajthat bármilyen funkciót a kimeneti sorral. Az osztályon kívül senki sem használhatja, beleértve a rendszeroperátorokat is. A PRICEQ kimeneti sor a CONTRACTS könyvtárban található.

## NEWCP

Tárgyalás alatt álló szerződések részére lesz használva. A kimeneti sor ugyan megosztott az osztály dolgozói között, de a "spool" fájl a kimeneti sorban csak az vezérelheti, aki létrehozta. A NEWCP kimeneti sor a CONTRACTS könyvtárban található.

Az alábbi táblázat bemutatja a Kimeneti sor és munkaállomás biztonság űrlapját, amelyet Sharon készített a fenti két kimeneti sorhoz:

54. táblázat: JKL Toy Company Kimeneti sor és munkaállomás biztonság űrlapja: nyomtató kimeneti sor

Korlátozott kimeneti sor paraméterlistája:				
Kimeneti sor neve	Kimeneti sor könyvtára	Fájl megtekintése (DSPDTA)	Ellenőrzés jogosultság (AUTCHK)	Operátor vezérlés (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

Az "Alkalmazási könyvtárak nyilvános jogosultságának eldöntése" című témakör példákon keresztül mutatja be a JKL Toy Company CONTRACTS könyvtárára vonatkozó jogosultságokat. Csak az osztály dolgozói és a vezetők érik el a könyvtárat. A könyvtár objektumainak (beleértve ezen kimeneti sorokat is) nyilvános jogosultsága \*CHANGE.

Mivel a NEWCP kimeneti sor AUTCHK paramétere \*OWNER, csak a "spool" fájl tulajdonosa dolgozhat vele (lásd a Nyomtatási funkciók végrehajtásához szükséges jogosultságot). Ez megakadályozza azt, hogy az osztály dolgozói kinyomtassák egymás szerződéseit, illetve megtekintsék azokat a kimeneti sorban.

Miután biztonságossá tette a nyomtató kimeneti sort, megtervezheti a munkaállomások biztonságát.

## Munkaállomások biztonságának tervezése

Miután megtervezte a nyomtatók és a nyomtatandó anyagok biztonságát, elkezdheti a munkaállomás biztonság tervezését. A Fizikai biztonság tervezésekor felsorolta az elhelyezésük miatt biztonsági kockázatot hordozó munkaállomásokat. Az ott leírtak segítségével meghatározhatja, hogy mely munkaállomásokat kell korlátoznia.

Ösztökélheti az állomások felhasználóit, hogy fokozottabban tartsák be a biztonsági előírásokat. Jelentkezzenek ki, valahányszor elhagyják a munkaállomást. Esetleg feljegyezheti döntését az ilyen munkaállomásokról követendő kijelentkezési eljárásokra vonatkozóan a biztonsági szabályzatban. A kockázat minimálisra csökkentése érdekében korlátozza a munkaállomásokról végrehajtható funkciókat.

A funkciók korlátozásának legegyszerűbb módja a munkaállomáson, ha az állomásokat korlátozott funkcióval ellátott felhasználói profilokhoz rendeljük. Sharon Jones ezt a technikát választotta a JKL Toy Company Raktár osztályánál. Sharon csak a készletfelvételi program futtatását engedélyezte Ray Wagner és Janice Ames számára, akik a bevételi raktárban dolgoznak. Egyben ők azok csak, akik a bevételi részben lévő munkaállomásokon be tudnak jelentkezni.

Szándékában állhat annak megelőzése, hogy biztonsági felelősi vagy szerviz jogosultsággal minden munkaállomásról be lehessen jelentkezni. Ha ennek érdekében a QLMTSECOFR rendszerváltozót használja, akkor az ilyen jogosultságú személyek csak egy megadott munkaállomáson tudnak bejelentkezni.

Töltse ki a Kimeneti sor és munkaállomás biztonság űrlapjának munkaállomásra vonatkozó részét.

Szándékában állhat áttekinteni egy példán, hogy Sharon hogyan tervezte meg a munkaállomások biztonságát, miközben kitölti a Kimeneti sor és munkaállomás biztonság űrlapjának munkaállomásokra vonatkozó részét. Egyúttal nézze át az erőforrás biztonságra vonatkozó ajánlásokat, hogy terve egyszerű és teljes legyen. Miután átnézte a példát és az ajánlásokat, elkezdheti alkalmazás telepítésének tervezését.

## Példa: JKL Toy Company Kimeneti sor és munkaállomás biztonság úrlapja — munkaállomás

Sharon Jones átnézte a Fizikai biztonság tervét, és meghatározta, hogy melyik munkaállomás jelent biztonsági kockázatot. A JKL Toy Company esetében például külső személy igen könnyen elérheti a raktár fogadóhelyiségében és a távoli eladóhelyen lévő munkaállomásokat. Sharon jelezte a Fizikai biztonság tervében, hogy ezek a munkaállomások potenciális kockázatot jelentenek biztonsági szempontból.

A funkciók korlátozásának legegyszerűbb módja a munkaállomáson, ha az állomásokat korlátozott funkcióval ellátott felhasználói profilokhoz rendeljük. Sharon Jones ezt a technikát választotta a JKL Toy Company Raktár osztályánál. Sharon csak a készletfelviteli program futtatását engedélyezte Ray Wagner és Janice Ames számára, akik a bevételi raktárban dolgoznak. Egyben ők azok csak, akik a bevételi részben lévő munkaállomásokon be tudnak jelentkezni.

Sharon felülvizsgálta a QLMTSECOFR rendszerváltóra vonatkozó választását. Elhatározta, hogy a fenti két helyszínen a sebezhető munkaállomások további védelme érdekében a QLMTSECOFR változót 1(Igen) értékre állítja.

Az alábbi táblázat bemutatja a Kimeneti sor és munkaállomás biztonság úrlapjának munkaállomás részét, amelyet Sharon készített:

55. táblázat: JKL Toy Company Kimeneti sor és munkaállomás biztonság úrlapja: munkaállomás példa

<b>Biztonsági felelős munkaállomásai:</b>	
Ha megadott munkaállomásokra korlátozta a biztonsági felelőst (QLMTSECOFR rendszerváltó = igen), az alábbiakban sorolja fel azokat a munkaállomásokat melyekre a biztonsági felelősnek és minden *ALLOBJ jogosultságú felhasználónak jogosultsága van: Minden munkaállomás, kivéve az alább felsoroltak.	
<b>Sorolja fel a jogosultságokat a korlátozott munkaállomásokra:</b>	
Munkaállomás neve	Jogosult csoportok vagy felhasználók (*CHANGE jogosultság)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

Szándékában állhat átnézni az erőforrás biztonsági ajánlások összefoglalóját, mielőtt megtervezné az alkalmazások telepítését.

## Erőforrás biztonsági ajánlások összefoglalója

Miután befejezte a munkaállomás biztonság tervezését, átnézheti az alábbi erőforrás biztonsági ajánlásokat. Az iSeries rendszer nagyon sok opciót ajánl fel a rendszer információinak védelmére. Ez nagyfokú rugalmasságot jelent a vállalat számára legelőnyösebb erőforrás biztonság megtervezéséhez. Azonban az opciók ilyen gazdagsága zavart is okozhat.

Ez a témakör a JKL Toy Company esetét bemutatva megpróbálja demonstrálni azt a vezérlőelvet, amely alapján a témakör közelít az erőforrás biztonság tervezéséhez:

- Az általánostól a specifikusság felé haladva:
  - Tervezze meg a könyvtárak biztonságát. Ne foglalkozzon egyedi objektumokkal, ha nem muszáj.
  - Először tervezze meg a nyilvános jogosultságot, majd a csoport- és végül az egyedi jogosultságot.
- A teljesítmény növelése, valamint a mentés és visszatöltés egyszerűsítése érdekében, csak azokra az objektumokra adjon meg speciális biztonságot, amelyekre a nyilvános jogosultság nem elégíti ki a követelményeket.
- Adja a könyvtár új objektumainak (CRTAUT) ugyanazt a nyilvános jogosultságot, amit már a könyvtár meglévő objektumainak többségére adott.

- Próbálja meg a csoportoknak és az egyéneknek legalább annyi jogosultságot adni, mint amennyi a nyilvánosságnak van. Ez csökkenti a teljesítményt, későbbi hibákhoz vezet és megnehezíti az ellenőrzést. Könnyebbé válik a biztonság tervezése és ellenőrzése, ha tudja, hogy egy objektumhoz mindenkinek van legalább a nyilvánossággal egyező jogosultsága.
- Használjon jogosultsági listát az azonos biztonsági igényű objektumok csoportba gyűjtésére. A jogosultsági listák egyszerűbben kezelhetők, mint az egyedi jogosultságok és segítik a biztonsági információk visszaállítását.
- Hozzon létre speciális felhasználói profilokat alkalmazás-tulajdonosnak. Állítsa a tulajdonos jelszavát \*NONE értékre.
- Kerülje el, hogy IBM profilok, úgymint QSECOFR vagy QPGMR alkalmazás-tulajdonos legyen.
- Használjon speciális kimeneti sorokat a bizalmas riportok részére. Tegye a kimeneti sort a bizalmas információt tároló könyvtárba.
- Korlátozza azoknak a számát, akiknek biztonsági felelősi jogosultságuk van.
- Legyen óvatos, mikor \*ALL jogosultságot ad objektumoknak vagy könyvtáraknak. Az emberek \*ALL jogosultsággal véletlenül is törölhetnek dolgokat.

Gyűjtse össze a következő információkat, ha biztos akar abban lenni, hogy sikeresen megtervezte az erőforrás biztonság beállítását:

- Töltse ki a Könyvtár leíró űrlapok első és második részét az összes alkalmazási könyvtár számára.
- Az Egyedi felhasználói profil űrlapokon töltse ki a **Létrehozott objektumok tulajdonosa** és a **Csoportjogosultság létrehozott objektumokhoz** mezőket.
- Rögzítse az Elnevezési szabályok űrlapon a jogosultsági listák elnevezésének módját.
- Készítse el a Jogosultsági lista űrlapokat.
- Egészítse ki a Könyvtár leíró űrlapokat a jogosultsági lista adataival.
- Készítse el a Kimeneti sor és munkaállomás biztonság űrlapját.

Most készen áll az alkalmazás telepítés tervezésére.

## Alkalmazások telepítésének tervezése

Az erőforrás biztonság tervezésének befejezéséhez el kell készíteni alkalmazásainak telepítési tervét. Az alábbi témakör segítségével megtervezheti az alkalmazások tulajdonjogát és a jogosultságokat, miután telepíti őket. Az itt leírt módszerek nem biztos, hogy minden alkalmazásra adaptálhatók. Konzultáljon programozójával vagy az alkalmazás szállítójával egy jó telepítési terv kialakítása végett.

Ha az alkalmazást egy szállítótól kívánja beszerezni, használja fel ezt a fejezetet az alkalmazási könyvtárak feltöltése előtti és utáni, biztonsággal összefüggő tevékenységének tervezéséhez.

Ha programozó által saját gépen kifejlesztett alkalmazást telepít, használja fel ezt a fejezetet az alkalmazás tesztverziójának termékké változtatásakor felmerülő biztonsági feladatok tervezésére.

Először egy alkalmazásra hajtja végre a lépéseket. Azután térjen vissza és készítse el az Alkalmazás telepítési űrlapokat a többi alkalmazásra is.

### Milyen űrlapokra van szükség?

Készítsen másolatot a következő űrlapokról és töltse ki az itt leírtak olvasása során:

56. táblázat: Alkalmazás telepítés tervezéséhez szükséges űrlapok

Űrlap neve	Szükséges másolatok száma
Alkalmazás telepítési űrlap	Alkalmazásonként egy



Az alkalmazás telepítés tervezéséhez használja fel az alábbi űrlapokat is, amelyeken már korábban összegyűjtötte az adatokat:

Űrlap neve	Készítette:
Könyvtár leíró űrlap	Könyvtári információk leírása
Jogosultsági lista űrlapja	Objektumok csoportosítása

A Alkalmazások betöltése című témakörben tanulmányozhatja, hogy milyen lépéseket kell megtenni az alkalmazások telepítéséhez.

Az alkalmazás telepítés tervezéséhez olvassa el még az alábbi témaköröket:

- Felhasználói profilok és telepítési értékek meghatározása az alkalmazások számára.
- Telepítési értékek módosítása.

## Felhasználói profilok és telepítési értékek meghatározása az alkalmazások számára

Amikor az alkalmazások telepítését tervezi, először a felhasználói profilokról, valamint az egyes alkalmazások telepítési értékeiről kell dönteni. Mielőtt egy másik rendszeren készített alkalmazást telepítene, létre kell hoznia egy vagy több felhasználói profilt. Az alkalmazás könyvtárait és objektumait birtokló - úgynevezett tulajdonosi - profilnak meg kell lenni a rendszerben a könyvtárak feltöltése előtt. Írja fel az Alkalmazás telepítési űrlapon, milyen profilokat kell létrehoznia a könyvtáraknak és milyen paramétereket kell beállítania.

A szükséges telepítési értékek meghatározásához tegye fel a következő kérdéseket a programozójának vagy az alkalmazás szállítójának, és jegyezze fel válaszaikat az Alkalmazás telepítési űrlapon:

- Melyik profil az alkalmazási könyvtár tulajdonosa?
- Melyik profil a könyvtári objektumok tulajdonosa?
- Milyen a könyvtár nyilvános jogosultsága (AUT)?
- Milyen az új objektumok nyilvános jogosultsága (CRTAUT)?
- Milyen az objektumok nyilvános jogosultsága a könyvtárban?
- Milyen programok - ha vannak - öröklik a tulajdonos jogosultságát?

Találja ki, vajon a programozó vagy az alkalmazás szállítója hozott-e létre jogosultsági listákat az alkalmazáshoz. Készítse el a Jogosultsági lista űrlapot minden meglévő jogosultsági listára, vagy kérdezzen rá a lista információira a programozótól.

Meghatározhatja, hogy kell-e módosítani valamelyik telepítési értéket.

## Telepítési értékek módosítása az alkalmazások számára

Hasonlítsa össze az Alkalmazás telepítési űrlap információit a Könyvtár leíró űrlapon lévő könyvtár erőforrás biztonsági tervével. Ha közöttük eltérés mutatkozik, el kell döntenie, hogy mit fog megváltoztatni a telepítést követően.

### Alkalmazás tulajdonjogának módosítása

Ha a programozó vagy az alkalmazás szállítója már hozott létre speciális tulajdonosi profilt az alkalmazás könyvtárai és objektumai számára, akkor inkább azt használja, még akkor is, ha az nem egyezik a tervezett elnevezési szabályokkal. Az objektumok tulajdonjogának megváltoztatása sok időt venne igénybe és ezért kerülendő.

Ha az IBM által szállított egyik csoportprofil (például QSECOFR vagy QPGMR) birtokolja az alkalmazást, akkor át kell ruházni a tulajdonjogot egy másik profilnak az alkalmazás telepítése után.

Néha a programozók úgy tervezik az alkalmazásokat, hogy az objektum tulajdonjoga nem változtatható meg. Próbáljon a korlátok között úgy lavírozni, hogy a biztonság kezelésére vonatkozó követelményeit még kielégítse. Azonban, ha az alkalmazás tulajdonosa IBM profil (mint például QSECOFR), akkor a programozónak vagy a szállítónak tervet kell készíteni a tulajdonjog módosítására. Ideális esetben az alkalmazás telepítése előtt kell megváltoztatni a tulajdonjogot.

## Nyilvános jogosultság módosítása

Amikor menti az objektumokat, velük együtt menti nyilvános jogosultságukat is. Amikor visszatölt egy alkalmazási könyvtárat a rendszerére, a könyvtár és annak minden objektuma ugyanazzal a jogosultsággal fog rendelkezni, mint amivel eltárolták. Ez még akkor is igaz, ha a könyvtárat másik rendszeren mentette.

A könyvtár CRTAUT értéke (nyilvános jogosultság az új objektumokra) nincs hatással a betöltendő objektumokra. Ők a tárolt nyilvános jogosultsággal kerülnek betöltésre, függetlenül a könyvtár CRTAUT értékétől.

Ha szükséges, meg kell változtatni a könyvtárak és objektumok nyilvános jogosultságát, hogy megegyezzen a Könyvtár leíró űrlapon lévő értékkel.

Szándékában állhat egy példán áttekinteni, hogy Sharon Jones hogyan tervezte meg az alkalmazások telepítését a JKL Toy Company számára, miközben saját ilyen irányú tervét készíti.

Az alábbiakat tegye meg, ha bizonyos akar abban lenni, hogy az alkalmazások telepítését körültekintően megtervezte:

- Fejezze be az elkezdett Alkalmazás telepítési űrlap kitöltését. Azután térjen vissza az elejére, és készítse el az űrlapot a többi alkalmazásra is.
- Nézze át az összes űrlapot, és bizonyosodjon meg arról, hogy mindegyiket kitöltötte. Készítsen róluk másolatot, és tartsa őket biztonságos helyen, amíg nem telepíti a rendszert és a licencprogramokat.

Miután befejezte a tervezési feladatokat, készen áll a biztonság beállítására.

**Példa: JKL Toy Company Alkalmazás telepítési űrlap:** A JKL Toy Company egy alkalmazás szállítótól vette a Vevő rendelések és a Vevő tartozások nevű alkalmazásokat. A Szerződések és árák nevű alkalmazás kifejlesztésére és a Vevő rendelések alkalmazáshoz történő illesztésére külső programozót vettek igénybe.

Sharon Jones a Könyvtár leíró űrlapjait használta fel az Alkalmazás telepítési űrlap elkészítéséhez. Az alábbi táblázat Sharon Könyvtár leíró űrlapjának egy példányát mutatja be a CUSTLIB könyvtárra: (lásd a "Könyvtári információk leírása" című témakört)

57. táblázat: JKL Toy Company Könyvtár leíró űrlap: példa

Könyvtár leíró űrlap	Első rész
Készítette: Sharon Jones	Dátum: 9/9/99
Könyvtár neve: CUSTLIB	Leírónév (szöveg): Customer Records Library
A könyvtár funkciójának rövid leírása: Tartalmazza az összes ügyfélfájl, beleértve a rendeléseket és a vevők számláit is.	
Határozza meg a könyvtár biztonsági elemeit, vajon van-e titkos információ: A mai napon megengedtük, hogy mindenki megnézhesse a vevő rendeléseket. Az információ pontosságának védelme érdekében korlátoznunk kell, hogy kik változtathatják meg.	
Könyvtár nyilvános jogosultsága: *USE Objektum nyilvános jogosultsága a könyvtárban: *CHANGE Új objektumok (CRTAUT) nyilvános jogosultsága: *CHANGE Könyvtár tulajdonosa: OWNER	

Az alábbi táblázat bemutatja az Alkalmazás telepítési űrlapot, amelyet Sharon készített a Vevő rendelések alkalmazáshoz: Ne felejtse el, hogy Sharon döntése értelmében az alkalmazás szállítója által létrehozott tulajdonosi profil lesz használva. A COWNER profil lesz mind a fájl-, mind a programkönyvtárak tulajdonosa.

Az alkalmazás telepítése után Sharon feladata lesz:

- Ha szükséges, meg kell változtatni a könyvtárak nyilvános jogosultságát, hogy egyezzenek a Könyvtár leíró űrlapokon lévő erőforrás biztonsági terv értékeivel.
- A COWNER profil felhasználói osztályának beállítása \*USER értékbe és a speciális jogosultságok eltávolítása.
- A COWNER profil jelszavának beállítása \*NONE értékre.

58. táblázat: JKL Toy Company Alkalmazás telepítési űrlap: példa

Alkalmazás neve: Vevő rendelések		Leírás: Rendelések felvétele, követése, kiszállítása.
Az alkalmazás telepítéséhez szükséges profilok listája és magyarázata: A könyvtár fájllai a COWNER profil tulajdonában vannak. A programkönyvtár tulajdonosa a QPGMR profil.		
<b>Könyvtár neve: CUSTLIB</b>		
	<b>Telepítés előtt</b>	<b>Telepítés után</b>
Könyvtár tulajdonosa	COWNER	COWNER
Objektum tulajdonosa	COWNER	COWNER
Könyvtár nyilvános jogosultsága	*EXCLUDE	*USE
Objektum nyilvános jogosultsága	*ALL	*CHANGE
Új objektumok nyilvános jogosultsága	*CHANGE	*CHANGE
<b>Könyvtár neve: COPGMLIB</b>		
	<b>Telepítés előtt</b>	<b>Telepítés után</b>
Könyvtár tulajdonosa	QPGMR	COWNER
Objektum tulajdonosa	QPGMR	COWNER
Könyvtár nyilvános jogosultsága	*EXCLUDE	*USE
Objektum nyilvános jogosultsága	*ALL	*CHANGE
Új objektumok nyilvános jogosultsága	*CHANGE	*CHANGE

Most, hogy befejezte a tervezési feladatokat, készen áll a felhasználói biztonság beállítására.

## A felhasználói biztonság beállítása

Az itt leírtak a felhasználói biztonság beállításához szükséges lépéseken vezetnek végig a parancssori kezelőfelület felhasználásával. Ha új rendszert állít be, minden lépést az adott sorrendben kell végrehajtani. A rendszer felhasználja az egyes lépések információit a következő lépésnél. Az alapszintű rendszerbiztonság beállításához két feladatsort kell elvégezni. Először meg kell adni a felhasználói biztonságot, majd másodikként meg kell védeni az erőforrásokat a rendszeren. Az alábbi két táblázat kiemeli azokat a lépéseket, ahol konfigurálnia kell a felhasználót és az erőforrás biztonságot.

**Megjegyzés:** Először végre **KELL** hajtania az összes lépést a felhasználói biztonság beállításához, mielőtt elkezdene az erőforrás biztonság beállítását.

59. táblázat: A felhasználói biztonság beállításának lépései

Lépés	Tevékenység ebben a lépésben	Használandó űrlap
A teljes környezet beállítása	Kezdeti rendszerváltozók és hálózati tulajdonságok beállítása. QSECOFR profil létrehozása.	Rendszerváltozók kiválasztására szolgáló űrlap
Biztonsági rendszerváltozók beállítása	További rendszerváltozók beállítása.	Rendszerváltozók kiválasztására szolgáló űrlap

59. táblázat: A felhasználói biztonság beállításának lépései (Folytatás)

Lépés	Tevékenység ebben a lépésben	Használandó űrlap
Alapszintű biztonság előkészítése az alkalmazások betöltéséhez	Tulajdonosi profilok létrehozása. Alkalmazások betöltése. Az alkalmazási könyvtáraknak és objektumoknak a rendszeren kell lenni a hátralévő lépések befejezése előtt.	Alkalmazás telepítési űrlap
Felhasználói csoportok beállítása	Jobleírások, csoportkönyvtárak, csoportprofilok létrehozása.	Felhasználói csoportot leíró űrlap
Egyedi felhasználók beállítása	egyedi könyvtárak és felhasználói profilok létrehozása.	Egyedi felhasználói profil űrlapja

60. táblázat: Az erőforrás biztonság beállításának lépései

Lépés	Tevékenység ebben a lépésben	Használandó űrlap
Tulajdonjog és nyilvános jogosultság beállítása	Könyvtárak és objektumok tulajdonjogának és nyilvános jogosultságának kialakítása.	Alkalmazás telepítési űrlap
Jogosultsági lista létrehozása	Jogosultsági listák létrehozása.	Jogosultsági lista űrlap
Egyedi jogosultságok beállítása	Egyedi könyvtárak és objektumok elérésének beállítása.	Könyvtárat leíró űrlap
Nyomatott listák védelme	A nyomtatott listákat a kimeneti sor létrehozásával és a nyomtató hozzárendelésével védi.	Kimeneti sor és munkaállomás biztonság űrlapja
Munkaállomások biztonsága	Munkaállomások védelme.	Kimeneti sor és munkaállomás biztonság űrlapja

A fenti táblázatban felsorolt témakörökön túlmenően olvassa el az alábbiakat is a rendszerbiztonság kezeléséhez:

- Biztonság tesztelése.
- Biztonsági információk módosítása.
- Biztonsági információk mentése.
- Biztonság figyelése.

### Mielőtt elkezdene

Ha új rendszert telepít, hajtsa végre a következő lépéseket a biztonság beállítása előtt:

- Győződjön meg róla, hogy a telepített rendszeregység és perifériák megfelelően működnek. Ha nem tervezi az iSeries elnevezések használatát az egységekre, akkor a munkaállomások és nyomtatók csatlakoztatásával várjon addig, míg be nem állítja az egységek nevét meghatározó (QDEVNAMING) rendszerváltozót. Az Új rendszerváltozók alkalmazása megmondja, hogy mikor kell csatlakoztatni az egységeket.
- Töltsön be egy licencprogramot, amelyet használni fog később.

## A teljes környezet beállítása

Ahhoz, hogy elkezdje a felhasználói biztonság kialakítását, állítsa be a teljes környezetet a felhasználók számára. Ebben a témakörben a SETUP menüt fogja használni a rendszerváltozók beállításához és a saját felhasználói profil létrehozásához. A DST felhasználók azonosítóit és jelszavait is módosítani fogja.

A következőkben minta parancssori képernyőket láthat, amelyek illusztrálják a lépéseket. Azonban, ezek nem mutatják a teljes képernyőt. Csupán a feladat elvégzéséhez szükséges információkat.

### Milyen űrlapokra van szükség?

Vigye be az "Átfogó biztonsági stratégia tervezése" című részben elkészített Rendszerváltozók kiválasztására szolgáló űrlap adatait.

A teljes környezet beállításához szükségszerűen elvégzendő feladatok:

1. Bejelentkezés a rendszerre.
2. Megfelelő támogatási szint kiválasztása.
3. Mások bejelentkezésének megakadályozása.
4. Biztonsági rendszerváltozók értékeinek bevitele.
5. Rendszerváltozók új értékeinek alkalmazása.
6. Biztonsági felelős profiljának létrehozása.

Miután végrehajtotta a fenti lépéseket, meg kell változtatnia a szervizeszközökhöz tartozó jelszavakat, hogy meggátolja helytelen használatukat. A részletekről a Szervizeszközök című részben olvashat.

## Bejelentkezés a rendszerre

A rendszerkörnyezet beállításához be kell jelentkeznie a rendszerre.

1. Jelentkezzen be a konzolon biztonsági felelősként (QSECOFR). Ha első alkalommal jelentkezik be, használja a QSECOFR jelszót. Mivel a rendszer lejártként szállítja a jelszót, ezért kérni fogja a megváltoztatását. Meg kell változtatnia a jelszót a sikeres bejelentkezéshez.
2. Adjon SETUP értéket a bejelentkezési képernyő *Menu* mezőjére.

**Megjegyzés:** A SETUP menü pontos neve: Rendszer, felhasználók, egységek egyéniesítésének menüje. Az anyagban SETUP menü név alatt találja.

```
Sign On
      System . . . . .
      Subsystem . . . . .
      Display . . . . .

User . . . . . QSECOFR
Password . . . . .
Program/procedure . . . . .
Menu . . . . . SETUP
Current library . . . . .
```

Miután bejelentkezik a rendszerre, ki kell választani a megfelelő támogatási szintet.

## Megfelelő támogatási szint kiválasztása

Miután bejelentkezik a rendszerre, kiválaszthatja a megfelelő támogatási szintet a felhasználók számára. A **támogatási szint** meghatározza, hogy a képernyők melyik verzióját látja. Sok rendszerképernyő két különböző verzióval rendelkezik:

- alap támogatási szint, amely kevesebb információt tartalmaz, és nem használ szakkifejezéseket.
- közepes támogatási szint, amely több információt biztosít, és műszaki kifejezéseket használ.

Néhány mező vagy funkció csak egy adott verziójú képernyőn jelenik meg. A parancsok mondják meg, melyik verziót kell használni. A támogatási szint változtatásához az **F21** (Select assistance level) funkcióbillentyűt kell használni. Az **F21** billentyű nem érhető el minden képernyőn.

Miután kiválasztotta a támogatási szintet, meg kell akadályozni, hogy mások bejelentkezzenek a rendszerre, miközben beállítja a biztonságot.

## Mások bejelentkezésének megakadályozása

Miután kiválasztotta a megfelelő támogatási szintet, meg kell akadályozni, hogy mások bejelentkezzenek a rendszerre. Ha attól tart, hogy valaki belekotárkodik a rendszerbe a biztonsági beállítások előtt, megelőzheti, ha letiltja a más munkaállomásról történő bejelentkezést. Ez nem kötelező lépés. Csak akkor tegye ezt meg, ha szükséges az ideiglenes biztonság:

1. A SETUP menüben hívja a parancssori képernyőt az **F9** lenyomásával.
2. Gépélje be a GO DEVICESTS parancsot.
3. A képernyő a Device Status Tasks menüt mutatja. Ha látja a Work with Configuration Status menüt, az **F21** (Select assistance level) billentyűt lenyomva állítsa be az alap támogatási szintet.
4. Válassza ki az **1-es** opciót (Work with display devices).
5. A Work with Display Devices képernyőn a saját munkaállomása kivételével mindegyiket tiltsa le. Elérheti, ha **2-es** értéket ír be az egyes munkaállomások neve elé, majd nyomja meg az **Enter** billentyűt.
6. Térjen vissza a SETUP menühöz az **F3** (Exit) billentyű kétszeri megnyomásával.
7. Nyomja meg az **F12** (Cancel) billentyűt a parancssorból való kilépéshez.

```
Work with Display Devices

Type options below, then press Enter.
1=Make available      2=Make unavailable  5=Display
7=Display message    8=Work with controller and line
13=Change description

Opt Device      Type      Status
--  ---
2_  DSP02        3196     Available to use
2_  DSP03        3196     Available to use
2_  DSP04        3196     Available to use
```

Ha egy egységet letiltott, a bejelentkezési képernyő még akkor sem jelenik meg rajta, ha bekapcsolják. A munkaállomások addig vannak letiltva, míg le nem állítja és el nem indítja újra a rendszert. Lehet, hogy ezt a lépést meg kell ismételnie.

Miután megelőzte, hogy valaki más bejelentkezhessen a rendszerre, állítsa be a biztonsági rendszerváltozók értékeit.

## Biztonsági rendszerváltozók értékeinek bevitele

Miután megelőzte, hogy valaki más bejelentkezzen, vigye be a rendszerváltozók értékeit.

Az alábbi eljárással vigye be a Rendszerváltozók kiválasztására szolgáló űrlap első részében található beállításokat:

1. Válassza ki a SETUP menü **1-es** opcióját (Change system options).
2. Vigye be a rendszerváltozók kiválasztására szolgáló űrlapon lévő információkat a Change System Options képernyőn. Ha nem akar a felajánlott értéken változtatni a Tab billentyűvel átlépheti az adott mezőt.
3. Adja meg a pontos dátumot és időt a képernyőn, ha nem lett beállítva a rendszer indításakor.
4. Ha minden adatot bevitt, lapozzon a következő képernyőre. A *More...* felirat a képernyő jobb alsó sarkában azt jelenti, hogy legkevesebb még egy oldal van.

```

Change System Options
System:
Type choices below, then press Enter.
System name . . . . . JKLTOY      Name
Date and time options:
System date . . . . . 09/21/99    MM/DD/YY
System time . . . . . 10:52:57    HH:MM:SS
Date separator . . . . . 1        1=/
                                   2=-
                                   3=.
                                   4=,
                                   5=blank
Date format . . . . . MDY         YMD, MDY, DMY, JUL
Time separator . . . . . 1        1=:
                                   2=.
                                   3=,
                                   4=blank
More...
F1=Help  F3=Exit  F5=Refresh  F12=Cancel

```

5. Gépelje be választásait a második oldalon, majd lapozzon.

```

Change System Options
Type choices below, then press Enter.
Security options:
Security level . . . . . 40
:
Allow security officers to
sign on to any display
station . . . . . N

```

6. Gépelje be választásait a képernyő harmadik oldalán, majd nyomja meg az **Enter** billentyűt.

```

Change System Options
Type choices below, then press Enter.
Device options:
Device naming format for new
devices . . . . . 1
Default system printer . . . PRT01
Additional options:
Put users in S/36 environment
at sign-on . . . . . N
Save job accounting
information about completed
printer output . . . . . Y

```

7. Ismét a SETUP menüt látja. A képernyő alján az alábbi üzenet jelenik meg: **System options successfully changed. IPL required.**

**Megjegyzés:** A rendszer csak akkor igényel új betöltést (IPL), ha megváltoztatta a biztonsági szintet.

Ebben a részben az egyes témakörök végén egy táblázatot talál a lehetséges hibákról és a helyreállításukról. Használja ezeket a táblázatokat, ha az eredményei eltérnek a leírtaktól. A táblázatok lehet, hogy nem nyújtanak mindenre megoldást. A táblázatok vezérfonalat kívánnak adni a probléma megoldásában és nagyobb kényelmet a rendszer használatában.

Lehetséges hiba	Helyreállítás
A MAIN menü van kijelezve.	<b>F3</b> (Exit) vagy <b>F12</b> (Cancel) billentyűt nyomott. Gépelje be a <b>GO SETUP</b> parancsot és próbálja újra.
Másik képernyőt lát, mint például Change Cleanup Options képernyőt. Ismét a Change System Option képernyő jelenik meg, miután megnyomta az <b>Enter</b> billentyűt.	Rossz opciót választott a SETUP menüben. Az <b>F3</b> (Exit) megnyomásával térjen vissza a menühöz, és próbálkozzon újra. Nézze meg a képernyő alján lévő hibaüzenetet. Feltehetően nem megengedett értéket gépelt be. Ne felejtse el használni az <b>F1</b> (Help) billentyűt, ha további információra van szüksége. Használja az <b>F5</b> (Refresh) billentyűt, ha azt akarja, hogy a rendszer visszatöltse a gépelés előtti értékeket. Próbálja újra. Annyiszor használhatja a képernyőt, ahányszor kell a rendszerváltozók megváltoztatásához. Válassza ki a SETUP menü <b>1-es</b> opcióját és vigye be az elmaradt értéket. <b>Figyelem! Ha a rendszer már működik, ne változtassa meg a biztonsági szintet a programozóval történő konzultáció nélkül. Ne változtassa meg a rendszer nevét sem, ha iSeries Accesset használ vagy másik számítógéppel kommunikál.</b>
<b>Enter</b> billentyűt nyomott, mielőtt begépelte volna minden választását a képernyőn.	Válassza ki ismét a SETUP menü <b>1-es</b> opcióját, és lapozzon a második oldalra. Írja be választásait, majd nyomja meg az <b>Enter</b> billentyűt.
<b>Enter</b> billentyűt nyomott lapozás helyett.	

Miután bevitte az új értékeket, alkalmazni kell őket.

## Rendszerváltozók új értékeinek alkalmazása

Miután beírta a rendszerváltozók értékeit, néhányat közülük alkalmazni kell. A rendszerváltozók módosításának többsége azonnal érvényesül. Azonban a biztonsági szint módosítása esetén a változások csak akkor lépnek életbe, ha leállította a rendszert és újraindította. Miután ellenőrizte, hogy minden értéket helyesen begépelte a Change System Options képernyőn, készen áll az új változók alkalmazására.

**Megjegyzés:** Csatlakoztassa a munkaállomásokat a rendszerhez, ha még nem tette volna meg. Mikor a rendszert indítja, a munkaállomások konfigurálása automatikusan megtörténik a Change System Options képernyőn megadott elnevezési szabály szerint.

Használja a következő eljárást a rendszer leállítására és újraindítására. Mikor a rendszer indul, a Change System Options képernyőn megadott értékek érvénybe lépnek.

1. Győződjön meg róla, hogy a konzolon jelentkezett be és a többi munkaállomáson senki sincs bejelentkezve.
2. Győződjön meg róla, hogy a kulcszár a processzor egységen Normal pozícióban van.
3. Válassza ki a SETUP menüben a Power On and Off Tasks opciót.
4. Válassza ki az azonnali (\*IMMED) kikapcsolás, majd ismételt bekapcsolás opciót. Nyomja meg az **Enter** billentyűt.
5. A rendszer a kikapcsolási döntés megerősítését kéri a megjelenő képernyőn. Jóváhagyásul nyomja meg az **F16** (Confirm) billentyűt.

Ennek eredményeképpen a rendszer leáll és azután automatikusan újraindul. A képernyő néhány percig semmit sem mutat. Utána a bejelentkezési képernyő fog megjelenni.

Miután alkalmazta (érvényesítette) a rendszerváltozók új értékeit, hozza létre a biztonsági felelős profilját saját maga számára a rendszeren.



## Biztonsági felelős profiljának létrehozása

**Biztonsági felelős** az a felhasználó a rendszer szempontjából, aki \*SECOFR felhasználói osztályú vagy \*ALLOBJ és \*SECADM egyedi jogosultságokkal bír.

Miután alkalmazta a Change System Option képernyőn bevitt értékeket, hozzon létre saját maga és helyettese számára felhasználói profilt. A jövőben inkább a saját profilját használja, mintsem a QSECOFR profilt a biztonsági feladatok elvégzésére.

1. Jelentkezzen be a rendszerre QSECOFR azonosítóval és kérje a SETUP menüt.

Figyelje meg, hogy a választott rendszernév a bejelentkezési képernyő jobb felső sarkában látható.

```
Sign On
      System . . . . .
      Subsystem . . . . .
      Display . . . . .

User . . . . . QSECOFR
Password . . . . .
Program/procedure . . . . .
Menu . . . . . SETUP
Current library . . . . .
```

2. Válassza ki a SETUP menü *Work with user enrollment* opcióját. A Work with User Enrollment képernyő kilistázza a rendszerben lévő aktuális profilokat.

**Megjegyzés:** Ha látja a Work with User Profile képernyőt, az **F21** (Select assistance level) billentyűvel módosítsa az alap támogatási szintet.

3. Új profil létrehozásához gépeljen **1** (Add) értéket az *Opt* (option) oszlopba és egy profilnevet a *User* oszlopba. Nyomja meg az **Enter** billentyűt.

```
Work with User Enrollment

Type options below, then press Enter.
1=Add 2=Change 3=Copy 4=Remove 5=Display

Opt   User           Description
1     JONESS
QDOC  Document User Profile
QSECOFR Security Officer User Profile
```

4. Az Add User képernyőn adja meg magát a jelszót.
5. Töltse ki a minta képernyőn látható mezőket a saját megfelelő információival.
6. Lapozzon (page down) a képernyő következő lapjára.

```

                                Add User

Type choices below, then press Enter.

User . . . . . JONESS
User description . . . . Jones, Sharon
Password . . . . . secret
Type of user . . . . . *SECOFR
User group . . . . . *NONE

Restrict command line use _____
Default library . . . . .
Default printer . . . . *WRKSTN
Sign on program . . . . *NONE
Library . . . . .

First menu . . . . .
Library . . . . .

```

7. Töltse ki a második oldalt, majd nyomja meg az **Enter** billentyűt.
8. Ellenőrizze a megerősítő üzenetet a Work with User Enrollment képernyő alján.
9. Nyomja meg az **F3** (Exit) billentyűt a SETUP menühöz való visszatérés végett.

```

                                Add User

Type choices below, then press Enter.

Attention key program . . *SYSVAL
Library . . . . .

```

#### Lehetséges hiba

**Enter** billentyűt nyomott, mielőtt begépelte volna az összes információt.

#### Helyreállítás

Használja a *Change* opciót a Work with User Enrollment képernyőn az éppen most létrehozott profil módosításához. Ha a profil nem jelenne meg a listában, nyomja meg az **F5** (Refresh) billentyűt, és lapozzon a megtalálásához.

Miután létrehozta saját maga számára a biztonsági felelősi profilt, változtassa meg a Szervizeszközök felhasználóinak azonosítóit és jelszavait. Olvassa el az Információs központ Szervizeszközök című témakörét.

## Biztonsági rendszerváltozók beállítása

Ebben a részben a Work with System Values (WRKSYSVAL) parancsot használja fel a rendszerváltozók módosítására és megjelenítésére.

### Milyen űrlapok szükségesek?

Vigye be az "Átfogó biztonsági stratégia tervezése" című részben elkészített Rendszerváltozók kiválasztására szolgáló űrlap adatait.

A következő feladatok végrehajtásából áll a rendszerváltozók beállítása:

1. Biztonsági rendszerváltozók módosítása.
2. Egyedi rendszerváltozók módosítása.

### Bejelentkezés a parancssori kezelőfelülethez

Az alábbiak szerint jelentkezzen be a rendszerre:

**Profil** Saját (\*SECADM és \*ALLOBJ jogosultság szükséges)

**Menü** MAIN

Miután bejelentkezik, elkezdheti a biztonsági rendszerváltozók módosítását.

## Biztonsági rendszerváltozók módosítása

A rendszerre való bejelentkezés után kövesse az alábbi eljárást a Rendszerváltozók kiválasztására szolgáló űrlap második részében lévő rendszerváltozók értékeinek beviteléhez.

1. Gépelje be a WRKSYSVAL \*SEC parancsot a parancssorba, és nyomja meg az **Enter** billentyűt. A parancs neve után beírt \*SEC azt jelenti, hogy csak a biztonsággal kapcsolatos rendszerváltozókat akarja látni.
2. A Work with System Values képernyőn gépeljen be **2** (Change) értéket az *Option* oszlopban a módosítani kívánt rendszerváltozó elé. Ha a módosítani kívánt rendszerváltozó nem látható a képernyőn, lapozzon lefelé amíg megtalálja.

```
Work with System Values
Position to . . . . . Starting character
Subset by Type . . . . . *SEC          F4 for list

Type options, press Enter.
2=Change  5=Display

Option  System Value  Type  Description
2      QINACTMSGQ  *SEC  Inactive job message queue
      QLMTDEVSSN  *SEC  Limit device sessions
      QLMTSECOFR  *SEC  Limit security officer device
      QMAXSGNACN  *SEC  Action to take for failed
      :
```

3. Gépelje be választását a rendszerváltozóra, és nyomja meg az **Enter** billentyűt. A Work with System Values képernyőt látja újra.

```
Change System Value
System value . . . . . : QLMTDEVSSN
Description . . . . . : Limit device sessions

Type choice, press Enter.

Limit device session . . . . 0          0=Do not
                                1=Limit
```

4. Ellenőrizze a megerősítő üzenetet a képernyő alján.

### Lehetséges hiba

A minta Work with System Values képernyőn látható rendszerváltozóktól eltérőket lát a képernyőjén.

A rendszer nem hajtotta végre a parancsot. Még látja a menüt.

### Helyreállítás

Elfelejtette begépelni a \*SEC paramétert. Hasonlítsa össze a *Subset by type* mezőt képernyője tetején a minta képernyővel. Vigye a kurzort a *Subset by type* mezőre. Gépelje be a \*SEC értéket, és nyomja meg az **Enter** billentyűt.

Ellenőrizze a hibaüzenetet a képernyő alján. Feltehetően helytelen parancsnevet gépelt be. Próbálja újra. Ha az üzenet szerint nincs jogosultsága, jelentkezzen ki majd újra be egy biztonsági felelősi jogosultságú profillal.

## Lehetséges hiba

Ismét a Change System Value képernyő jelenik meg, miután megnyomta az **Enter** billentyűt.

Egy menüt lát a Work System Values képernyő helyett.

Olyan rendszerváltozót választott, amit nem akar módosítani.

## Helyreállítás

Ellenőrizze a hibaüzenetet a képernyő alján. Feltehetően helytelenül gépelte be választását, vagy a megengedett tartományon kívül eső értéket adott meg. Használja az **F1** (Help) billentyűt további információért.

Valószínűleg kétszer nyomta meg az **Enter** billentyűt. Gépelje be a **WRKSYSVAL \*SEC** parancsot.

Nyomja meg az **F12** (Cancel) billentyűt a Work with System Values képernyőhöz való visszatérés érdekében.

## Mit jelent a \* (csillag)?

Valószínűleg már észrevette, hogy egyes értékek előtt csillag (\*) található. A rendszer a csillaggal különbözteti meg a speciális értékeket a szabályos szavaktól. Például, ha **\*NONE** értéket ad meg a felhasználói profilban jelszóként, ez azt jelenti, hogy a rendszer senkit sem enged bejelentkezni ezzel a profillal. Ha viszont csak **NONE** értéket ad meg, ez azt jelenti, hogy a felhasználónak a **NONE** karaktereket kell begépelnie jelszóként.

Mialatt a biztonságot állítja be a rendszeren, figyelmesen használja a csillagot a parancsokban és az űrlapokon is.

Miután megváltoztatta a biztonsági rendszerváltozókat, módosítsa az egyedieket.

## Egyedi rendszerváltozók módosítása

Miután módosította a biztonsági rendszerváltozókat, módosíthatja az egyedieket is.

Például, a Disconnect Job Time-Out Interval (QDSCJOBITV) rendszerváltozó nem tartozik a biztonsági értékek közé. Nem jelenik meg a Work with System values képernyő **\*SEC** alkészletében sem. A QDSCJOBITV és más egyedi rendszerváltozó módosítását az alábbiak szerint végezheti el:

1. Gépelje be a **WRKSYSVAL QDSCJOBITV** parancsot, és nyomja meg az **Enter** billentyűt.
2. A Work with System Values képernyőn gépeljen be **2** (Change) értéket az *Option* oszlopban a QDSCJOBITV elé.
3. Gépelje be választását a QDSCJOBITV részére.
4. Ellenőrizze a jóváhagyó üzenetet.

```
Change System Value
System value . . . . . : QDSCJOBITV
Description . . . . . : Disconnected job time-out interval

Type choice, press Enter.

Disconnected job time-out interval ..... 300
```

## Biztonsági értékek listázása

A Rendszerváltozók kiválasztására szolgáló űrlap összes információjának bevitele után kinyomtathatja a biztonsági rendszerváltozók beállításait. Gépelje be a **WRKSYSVAL \*SEC OUTPUT(\*PRINT)** parancsot. Fűzze le a Rendszerváltozók kiválasztására szolgáló űrlap értékeit mutató lista egy másolatát. A biztonsági értékek minden módosításakor nyomtasson ki új listát.

Miután bevitte a rendszerváltozók összes módosítását a Rendszerváltozók kiválasztására szolgáló űrlapról, előkészülhet az alkalmazások betöltéséhez.

## Biztonság előkészítése az alkalmazások betöltéséhez

Miután beállította a rendszerváltozókat, előkészülhet az alkalmazások betöltéséhez. Ez a rész tárgyalja az alkalmazási könyvtárak betöltéséhez szükséges biztonsági lépéseket. A profilok és más biztonsági objektumok létrehozása után a "Tulajdonjog és nyilvános jogosultság beállítása", valamint az "Erőforrás biztonság beállítása" című részek ismertetik, hogyan alakíthatja ki a tulajdonjogot és a jogosultságot az alkalmazásokhoz.

Ha lehetséges, az alkalmazások könyvtárait a felhasználói csoportok és egyedi profilok létrehozása előtt tölts be. Hivatkoznia kell az alkalmazás objektumaira, mikor jobleírásokat és profilokat hoz létre.

Ha nem tudja az alkalmazás objektumait a csoport- és egyedi profilok képzése előtt betölteni, figyelmeztető üzenetet kaphat a következők szerint:

- The system does not find initial libraries when you create job descriptions.
- The system does not find the initial program or menu when you create profiles.

Nem lehet sikeresen tesztelni a jobleírásokat és a profilokat addig, amíg be nem tölti az alkalmazási könyvtárakat.

Vegye elő az "Alkalmazások telepítésének tervezése" című részben előkészített Alkalmazás telepítési űrlapot.

A következő feladatok végrehajtásából áll az egyes alkalmazások betöltése:

1. Tulajdonosi profil létrehozása.
2. Alkalmazás betöltése.

### Bejelentkezés a rendszerre

- Tulajdonosi profilok létrehozásához:

**Profil** Saját (\*SECADM jogosultság szükséges)

**Menü** MAIN

- Alkalmazási könyvtárak betöltéséhez:

Ellenőrizze az alkalmazás szállítójával, hogy vajon a könyvtárak betöltéséhez biztonsági felelősként vagy alkalmazás tulajdonosként kell-e bejelentkeznie.

Miután bejelentkezik, létrehozhat tulajdonosi profilt az alkalmazásokhoz.

### Tulajdonosi profil létrehozása

Miután bejelentkezik a rendszerre, ellenőrizze az Alkalmazás telepítési űrlap információit, hogy létre kell-e hozni valamilyen profilt az alkalmazás betöltése előtt. A profil létrehozásához:

1. Gépelje be a CRTUSRPRF (Create User Profile) parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. A Create User Profile képernyőn tölts ki a mezőket a programozó vagy az alkalmazás szállítójának előírásai szerint.
3. Használja az **F10** (More fields) billentyűt, valamint lapozzon lefelé a további mezők megjelenítéséhez.

#### Create User Profile (CRTUSRPRF)

Type choices, press Enter.

```
User profile . . . . . >
User password . . . . . *USRPRF
Set password to expired . . . . *NO
Status . . . . . *ENABLED
User class . . . . . *USER
Assistance level . . . . . *SYSVAL
Current library . . . . . *CRTDFT
Initial program to call . . . . *NONE
  Library . . . . .
Initial menu . . . . . MAIN
  Library . . . . . *LIBL
Limit capabilities . . . . . *NO
Text 'description' . . . . . xxxxxx tulajdonosa
```

4. Ellenőrizze az üzenetet a képernyő alján.

**Megjegyzés:** A Csoportprofil létrehozása című szakasz részletesen tárgyalja a profilok létrehozását.

Miután létrehozta az alkalmazás tulajdonosát, elkezdheti az alkalmazás betöltését.

### Alkalmazás betöltése

Az alkalmazási könyvtárak betöltésekor kövesse az alkalmazás szolgáltatójának utasításait. A "Tulajdonjog és a nyilvános jogosultság beállítása" című részben tanulmányozhatja a tulajdonjog és a nyilvános jogosultság beállítását az alkalmazások számára.

Miután betöltötte az összes alkalmazást, összeállíthatja a felhasználói csoportokat.

### Felhasználói csoportok beállítása

Miután végrehajtotta az alkalmazások betöltésére vonatkozó biztonsági lépéseket, beállíthatja a felhasználói csoportokat. Csoportprofilokat, csoportkönyvtárakat és jobleírásokat fog létrehozni. Hajtsa végre az itt leírtakat az egyik felhasználói csoportjával, majd térjen vissza, és ismételje meg a lépéseket az összes többi csoportra. A minta képernyő a Felhasználói csoportot leíró űrlapok információit mutatja be a JKL Toy Company Kereskedelmi és marketing osztályára (SM), valamint Raktár osztályára (WH).

Vegye elő a "felhasználói csoportok tervezése" című részben előkészített Felhasználói csoportot leíró űrlapokat.

Az alábbi feladatok végrehajtásából áll a felhasználói csoportok beállítása:

1. Könyvtár létrehozása a felhasználói csoportnak.
2. Jobleírás létrehozása.
3. Csoportprofil létrehozása.

#### Bejelentkezés a rendszerre

**Profil** Saját (\*SECADM jogosultság szükséges)

**Menü** MAIN

Miután bejelentkezik, létrehozhat egy könyvtárat a felhasználói csoportnak.

### Könyvtár létrehozása a felhasználói csoportnak

Miután bejelentkezik a rendszerre, hozzon létre egy könyvtárat a felhasználói csoportnak. Ha osztott könyvtárat tervez a csoport által létrehozott objektumok számára, például Query program használatakor, hozza létre a könyvtárat a csoportprofil előtt:

1. Gépelje be a CRTLIB (Create Library) parancsot, és nyomja meg az **F4** (Prompt) billentyűt.

2. Töltse ki a képernyőt. A könyvtár neve legyen a csoportprofil neve.
3. Nyomja meg az **F10** (Additional parameters) billentyűt.
4. Töltse ki a könyvtár, és a könyvtárban újonnan létrehozott objektumok nyilvános jogosultságát.
5. Nyomja meg az **Enter** billentyűt. Ellenőrizze a megerősítő üzenetet.

```

                                Create Library
Type choices, press Enter.
Library . . . . . DPTWH
Library type . . . . . *PROD
Text 'Description' . . . . . Raktár könyvtár

                                Additional Parameters
Authority . . . . . *USE
Auxiliary storage pool ID . . . . . 1
Create authority . . . . . *CHANGE
Create object auditing . . . . . *SYSVAL

```

#### Lehetséges hiba

**Enter** billentyűt nyomott, mielőtt begépelte volna a könyvtár leírását a képernyőn.

Rossz könyvtárnevet adott.

#### Helyreállítás

Gépelje be a **CHGLIB** parancsot, és nyomja meg az **F4** (Prompt) billentyűt. Gépelje be a könyvtár nevét a képernyőn, és nyomja meg az **Enter** billentyűt. Gépelje be a leírást a Change Library képernyőn.

Használja a Rename Object (RNMOBJ) parancsot.

Miután létrehozta a könyvtárat a csoport számára, létrehozhatja a jobleírást.

### Jobleírás létrehozása

Miután létrehozta a könyvtárat a csoport számára, hozzon létre jobleírást is mindegyik csoport számára.

Ha a kezdeti könyvtárlistába szükséges könyvtárak nincsenek betöltve a rendszeren, figyelmeztető üzenetet kap a jobleírás létrehozásakor.

1. Gépelje be a **CRTJOB** (Create Job Description) parancsot, és nyomja meg az **F4** (prompt) billentyűt.
2. Töltse ki ezeket a mezőket:

**Job description:**

mint a csoportprofil neve

**Library name:**

QGPL

**Text:** csoportleírás

3. Nyomja meg az **F10** (Additional parameters) billentyűt.
4. Lapozzon (page down) az *Initial library list* mezőre.

```

Create Job Description
Type choices, press Enter.
Job description . . . . . DPTSM
Library . . . . . QGPL
Job queue . . . . . QBATCH
Library . . . . . *LIBL
Job priority (on JOBQ) . . . . . 5
Output priority (on OUTQ) . . . . . 5
Print device . . . . . *USRPRF
Output queue . . . . . *USRPRF
Library . . . . .
Text 'description' . . . . . Kereskedelem és Marketing

```

5. Gépeljen + (plusz) jelet a \*SYSVAL helyett az *Initial library list* mezőre, jelezve, hogy további értékeket akar megadni. Nyomja meg az **Enter** billentyűt.

```

Accounting code . . . . . *USRPRF
:
CL syntax check . . . . . *NOCHK
Initial library list . . . . . +
+ for more values

```

6. Az *Initial library list* mezőre gépelje be azokat a könyvtárakat, amelyeket bejelölt (✓) a Felhasználói csoportot leíró űrlapon:

- Soronként egy könyvtárnevet adjon meg.
- Beleértve a QGPL és QTEMP könyvtárakat is. Minden munka használja a QTEMP könyvtárat az ideiglenes objektumok tárolására. **Minden kezdeti könyvtárlista kell, hogy tartalmazza a QTEMP könyvtárat.** A legtöbb alkalmazás számára meg kell adni a QGPL könyvtárat is a kezdeti listában.
- Nem kell a listához adnia az aktuális (default) könyvtárat. A rendszer automatikusan hozzáadja a bejelentkezéskor.

7. Nyomja meg az **Enter** billentyűt. Ellenőrizze az üzeneteket. Lapozzon (page down) az összes üzenet megjelenítéséhez.

```

Specify More Values for
Type choices, press Enter.
Initial library list . . . . . CUSTLIB
                             ITEMLIB
                             COPGMLIB
                             ICPGMLIB
                             QGPL
                             QTEMP

```

**Lehetséges hiba**

**Enter** billentyűt nyomott **F10** helyett.

**Helyreállítás**

A helyes könyvtár megadásához gépelje be a **CHGJOB** (Change Job Description) parancsot, és nyomja meg az **F4** billentyűt.



## Lehetséges hiba

Jobleírás létrehozásakor hibaüzenetet kap.

## Helyreállítás

A legáltalánosabb hibaüzenet akkor jelentkezik, ha olyan könyvtárat próbál felvenni a listába, ami nincs a rendszeren. Ez figyelmeztető üzenet. A jobleírás kezdeti könyvtárlistája tartalmazza a hiányzó könyvtárat. Azonban addig nem tud a jobleíráshoz tartozó profillal bejelentkezni, míg be nem tölti a hiányzó könyvtárat.

Ha a könyvtár be van töltve, feltehetően helytelenül gépelte be a nevét. Ellenőrizze a könyvtár nevét és próbálja újra.

Miután létrehozta a jobleírást, létrehozhatja a csoportprofil.

## Csoportprofil létrehozása

Miután létrehozta a jobleírást, hozza létre a csoportprofil. Ehhez használja fel a Felhasználói csoportot leíró űrlap második részét.

1. Használja a Work with User Profiles parancsot. Gépelje be a WRKUSRPRF \*ALL parancsot. Kezdetben a képernyő az IBM profilekat sorolja fel.

**Megjegyzés:** Ha látja a Work with User Enrollment menüt, az **F21** (Select assistance level) billentyűt lenyomva állítsa be a közepes támogatási szintet.

2. Az új profil létrehozásához gépeljen be **1** értéket az *Opt* (option) oszlopba és egy profilnevet a *User Profile* oszlopba. Nyomja meg az **Enter** billentyűt.

```
Work with User Profiles

Type options, press Enter.
 1=Create  2=Change  3=Copy  4=Delete  5=Display
12=Work with objects by owner

  User
Opt Profile  Text
1  DPTSM
   QDOC      Document User Profile
   QSECOFR   Security Officer User Profile
```

3. Írja be az információkat a megfelelő mezőkre a Felhasználói csoportot leíró űrlapról.
4. Használja a **Tab** billentyűt azon mezők átlépésére, ahol elfogadja az alapértéket.
5. Nyomja meg az **F10** (Additional parameters) billentyűt.
6. Lapozzon.

Create User Profile (CRTUSRPRF)

Type choices, press Enter.

```
User profile . . . . . > DPTSM
User password . . . . . *none
Set password to expired . . . . . *NO
Status . . . . . *ENABLED
User class . . . . . *USER
Assistance level . . . . . *SYSVAL
Current library . . . . . *CRTDFT
Initial program to call . . . . . cpsetup
  Library . . . . . cppgmlib
Initial menu . . . . . cpmain
  Library . . . . . cppgmlib
Limit capabilities . . . . . *yes
Text 'description' . . . . . Sales and Marke
```

7. Vigye be a Felhasználói csoportot leíró űrlap maradék értékeit a képernyő további oldalain, és nyomja meg az **Enter** billentyűt.

Create User Profile

Additional Parameters

```
Special authority . . . . . *USRCLS
:
Job description . . . . . DPTSM
Library . . . . . QGPL
```

Create User Profile

```
Group authority . . . . . *NONE
:
Print device . . . . . PRT03
```

8. Ellenőrizze az üzeneteket.

**Ne felejtse el!**

A csoportprofil speciális típusú felhasználói profil. Sok üzenet és képernyő hivatkozik csoportprofilra felhasználóként vagy felhasználói profilként. Csak a rendszer tudja, hogy egy csoportprofil hozott létre, ha tagot ad hozzá vagy csoportazonosító számot (gid) rendel hozzá.

**Lehetséges hiba**

**Enter** billentyűt nyomott, mielőtt begépelte volna az összes értéket a csoportprofilba.

Rossz névvel hozta létre a profilt.

**Helyreállítás**

Nyomja meg az **F5** (Refresh) billentyűt a létrehozott profil hozzáadása végett a Work with User Profiles képernyőn. Használja a **2** (Change) opciót a profil helyesbítésére. A profil nevét nem tudja megváltoztatni. Használja a másolás (**3**) opciót az új profil létrehozására a helyes névvel. Utána a törlés (**4**) opcióval törölje az elhibázott profilt.

## Lehetséges hiba

A Felhasználói csoportot leíró űrlap néhány mezője nem jelenik meg a képernyőn.

Néhány alapértelmezett értéket véletlenül törölt a Create User Profile képernyőn.

## Helyreállítás

Győződjön meg róla, hogy közepes támogatási szintet használ. A Create User Profile képernyő alap támogatási szintű verzióját Add a User képernyőnek hívjuk. A támogatási szint megváltoztatásához először térjen vissza a Work with User Enrollmentment képernyőhöz az **F12** (Cancel) billentyű megnyomásával. Majd az **F21** billentyűvel változtassa meg a támogatási szintet. Olvassa el a "Megfelelő támogatási szint kiválasztása" című részt.

Ha a mezőt üresen hagyja, a rendszer az alapértéket fogja használni a felhasználói profil létrehozásakor. Ha meg akarja nézni az alapértékeket, nyomja meg az **F5** (Refresh) billentyűt a teljes képernyő visszaállításához. Gépelje be ismét az információkat.

## Eredmények listázása

Kilistáztathatja az összes profil nevét és leírását a Display Authorized Users (DSPAUTUSR) parancs használatával. Gépelje be a DSPAUTUSR OUTPUT(\*PRINT) parancsot. Ellenőrizze, hogy minden csoportprofil jelszava \*NONE értékű.

Hajtsa végre az alábbiakat, mielőtt beállítja az egyedi felhasználókat:

- Hozzon létre minden csoportnak jobbleírást.
- Opcionálisan hozzon létre könyvtárat minden csoportnak.
- Hozzon létre minden csoportnak csoportprofil.

## Egyedi felhasználók beállítása

Amikor beállította a felhasználói csoportokat, végrehajtotta a csoportprofilok létrehozásához szükséges lépéseket. Most, a csoportok tagjai számára készít egyedi profilokat.

Hajtsa végre az itt leírtakat az egyik felhasználói csoport tagjaival, majd térjen vissza, és ismétlje meg a lépéseket az összes többi csoportra is. A minta képernyőkön lévő felhasználók a Egyedi profil űrlapokról valók, amelyeket Sharon Jones a JKL Toy Company Kereskedelmi és marketing osztályára (SM), valamint Raktár osztályára (WH) vonatkozóan töltött ki. Az űrlapok másolatait megtalálhatja az "Egyedi felhasználói profilok tervezése" című részben.

Vegye elő az "Egyedi felhasználói profilok tervezése" című részben kitöltött Egyedi felhasználói profilok űrlapjait.

Az alábbi feladatok végrehajtásából áll az egyedi profilok létrehozása csoportok tagjai számára:

1. Személyi könyvtár létrehozása. (nem kötelező)
2. Csoportprofil másolása.
3. Jelszó beállítása lejárt állapotba.
4. További felhasználók létrehozása. (nem kötelező)

**Megjegyzés:** Ismétlje meg a Személyi könyvtár létrehozása és a További felhasználók létrehozása közötti lépéssort, amíg minden csoporttag nem rendelkezik felhasználói profillal.

5. Felhasználó adatainak módosítása, ha szükséges.
6. Eredmények megjelenítése.

## Bejelentkezés a rendszerre

**Profil** Saját (\*SECADM jogosultság szükséges)

**Menü** SETUP

## Személyi könyvtár létrehozása

Ahhoz, hogy elkezdje az egyedi felhasználók beállítását, létre kell hoznia személyi könyvtárakat minden tag számára az objektumok (mint például Query programok) elhelyezése céljából. A személyi könyvtárakat az egyedi felhasználói profilok létrehozása előtt kell kialakítani.

1. Gépelje be a **CRTL** parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Adja a könyvtárnak ugyanazt a nevet, mint a felhasználói profilnak.
3. Nyomja meg az **F10** (Additional parameters) billentyűt.
4. Töltse ki a könyvtár, és a könyvtárban újonnan létrehozott objektumok nyilvános jogosultságát.
5. Nyomja meg az **Enter** billentyűt. Ellenőrizze a megerősítő üzenetet.

```
                Create Library
Type choices, press Enter.
Library . . . . . DPTSM
Library type . . . . . *PROD
Text 'description' . . . . . Warehouse Library

                Additional Parameters
Authority . . . . . *EXCLUDE
Auxiliary storage pool ID . . . . . 1
Create authority . . . . . *CHANGE
Create object auditing . . . . . *SYSVAL
```

Miután elkészítette a személyi könyvtárat, hozza létre az egyedi profilt a csoportprofil másolásával.

## Csoportprofil másolása

A csoportprofilnak kettős szerepe van:

1. A rendszer felhasználja annak meghatározására, hogy egy csoporttag jogosult-e egy adott objektum használatára.
2. Mintaként használhatja az egyes csoporttagok profiljainak létrehozásához.

Amikor beállította a felhasználói csoportokat, létrehozta a csoportprofilokat. Most a csoportprofil másolásával létrehoz egy egyedi profilt, majd az egyedi profil másolásával egy másik egyedi profilt a csoporton belül.

1. Válassza ki a **SETUP** menü **Work with User Enrollment** menüpontját.

**Megjegyzés:** Ha látja a **Work with User Profiles** menüt, az **F21** (Select assistance level) billentyűt lenyomva állítsa be az alap támogatási szintet.

2. Gépeljen be a **3** (Copy) értéket az *Opt* oszlopban a csoport elé. A Copy User képernyő jelenik meg. (Ha a csoport, amit másolni szeretne nincs a képernyőn, lapozzon (page down), míg megjelenik.) A rendszer üresen hagyja a felhasználó neve mezőt, a fennmaradó mezőket a csoportprofilból tölti fel.

```
                Work with User Enrollment
Type options below, then press Enter.
  1=Add  2=Change  3=Copy  4=Remove  5=Display

Opt      User          Description
3        DPTSM        Sales and Marketing Department
         DPTWH         Warehouse Department
```

3. Gépelje be a létrehozni kívánt profil nevét és leírását.
4. Hagyja a jelszó mezőt üresen. A rendszer automatikusan az új profil nevét adja meg jelszóként.
5. Írja be a csoportprofil nevét a *User group* mezőre.

6. Ellenőrizze a felhasználót az Egyedi felhasználói profilok űrlapján, vajon a csoporttól eltérő értéket kell-e adni számára. Ha igen, gépelje be az eltérő értékeket.
7. Lapozzon.

```

                                Copy User
Copy from user . . . . . : DPTWH
Type choices below, then press Enter.
User . . . . .           WILLISR
User description . . . . . Willis, Rose
Password . . . . .
Type of user . . . . .  *SYSOPR
User group . . . . .   DPTWH

Restrict command line use N

Default library . . . . . DPTWH
Default printer . . . . . PRT04
Sign on program . . . . . *NONE
Library . . . . .

First menu . . . . .    ICMAIN
Library . . . . .      ICPGMLIB

```

8. Ha kell, módosítson a képernyő következő oldalán, majd nyomja meg az **Enter** billentyűt.
9. Ellenőrizze a megerősítő üzenetet a Work with User Enrollmentment képernyő alján.

```

                                Copy User
Copy from user . . . . . : DPTWH
Type choices below, then press Enter.
Attention key program . . *SYSVAL
Library . . . . .

```

### Lehetséges hiba

A Create User Profile képernyőt látja a Copy User képernyő helyett.

A választott profilnév nem fér bele a felhasználó mezőbe.

### Helyreállítás

Nyomja meg az **F12** (Cancel) billentyűt a Work with User Profiles képernyőhöz való visszatérés érdekében. Majd az **F21** billentyűvel állítsa be az alap támogatási szintet. Kezdje el a másolási eljárást ismét.

Annak ellenére, hogy a név 10 karakter lehet a Copy User és az Add User képernyők nem támogatnak 8 karakternél hosszabb nevet. Vagy válasszon rövidebb nevet, vagy használja a közepes támogatási szintet a felhasználói profilok létrehozásakor.

### Felhasználói profil tesztelése

Mikor az első egyedi profilt létrehozza a csoportban, tesztelje le úgy, hogy bejelentkezik vele. Ellenőrizze, hogy a helyes kezdeti menüt látja és a kezdeti program sikeresen lefut.

Ha nem tud a profillal sikeresen bejelentkezni, feltehetően a rendszer nem talál valamit, amit a profilban megadott. Ez lehet bejelentkezési program, jobleírás, kezdeti könyvtárlista egyik könyvtára, stb. A Work with Printer Output képernyő segítségével keresse meg a bejelentkezési kísérletkor keletkezett job naplót. A napló pontosan leírja a keletkezett hibát.

Olvassa el a "Biztonság tesztelése" című részt, ahol tájékozódhat a biztonsági változtatásokkal összefüggő hibák diagnosztizálásáról és teszteléséről.

Miután tesztelte a felhasználói profilt, beállíthatja a jelszót lejárt állapotba.

## Jelszó beállítása lejárt állapotba

Állítsa be úgy az egyedi profilokat, hogy a felhasználók az első bejelentkezéskor kénytelenek legyenek jelszavaikat módosítani. A *Set password to expire* mező nem jelenik meg alap támogatási szint esetén a Copy User képernyőn. Ezt külön kell módosítani, miután másolással létrehozta a felhasználói profilt. A *Set password to expire* mező módosításához gépelje be a **CHGUSRPRF profil neve PWDEXP(\*YES)** parancsot.

**Megjegyzés:** Ha a profilt tesztelni szeretné bejelentkezéssel, akkor a jelszó lejárt állapotba állítása *előtt* tesztelje.

### Lehetséges hiba

Tesztelte a profilt és a rendszer a jelszó cseréjét kérte.

### Helyreállítás

Gépelje be a **CHGUSRPRF profil neve** parancsot, és nyomja meg az **F4** (Prompt) billentyűt. Állítsa vissza a jelszót a profil nevére. (Gépelje be a profil nevét a jelszó mezőbe.) Gépeljen **\*YES** értéket a *Set password to expire* mezőbe. A feladathoz közepes támogatási szintre van szüksége.

Miután létrehozta az első egyedi felhasználói profilt, további felhasználókat hozhat létre.

## További felhasználók létrehozása

Miután a csoportprofil másolásával létrehozta az első egyedi profilt, további felhasználókat hozhat létre. Másolja az első felhasználói profilt a következő csoporttag profiljának létrehozására. Jól nézze meg mindegyik egyedi profilt, amit másolással hozott létre. Ellenőrizze az Egyedi felhasználói profilok űrlapja alapján, hogy valóban módosította-e az új felhasználói profilok egyedi beállításait.

1. A Work with User Enrollmentment képernyőn gépeljen **3** (Copy) értéket a másolni kívánt profil elé.
2. A Copy User képernyőn gépelje be a profil nevét és a leírását.
3. Írja be az új felhasználó egyéb egyedi értékeit.

Work with User Enrollmentment

Type options below, then press Enter.  
1=Add 2=Change 3=Copy 4=Remove 5=Display

Opt	User	Description
	DPTSM	Sales and Marketing Department
	DPTWH	Warehouse Department
<b>3</b>	WILLISR	Willis, Rose

### Lehetséges hiba

A másolni kívánt profil nem jelenik meg a Work with User Enrollmentment képernyőn.

### Helyreállítás

Nyomja meg az **F5** (Refresh) billentyűt. Lapozzon fel (page up) és le (page down). A profilok neve abc sorrendben jelenik meg.

Ha szeretné módosítani a felhasználó adatait, olvassa el a Felhasználó adatainak módosítása című részt.

## Felhasználó adatainak módosítása

Lehet, hogy néhány felhasználónak be kell állítani olyan értékeket, amely nem jelenik meg a Copy User képernyőn. Például, néhány felhasználó több csoporthoz is tartozhat. A másolással létrehozott profilt külön módosítani kell ilyenkor.

1. A Work with User Enrollment képernyőn az **F21** (Select assistance level) billentyűt lenyomva állítsa be a közepes támogatási szintet.
2. A Work with User Profiles képernyőn gépeljen **2** (Change) értéket az *Opt* (option) oszlopban a változtatni kívánt profil neve elé. Nyomja meg az **Enter** billentyűt.

```

Work with User Profiles

Type options, press Enter.
1=Create 2=Change 3=Copy 4=Delete 5=Display
12=Work with objects by owner

User
Opt Profile Text
2 AMESJ Ames, Janice
  DPTSM Sales and Marketing Department
  QDOC Document User Profile
  QSECOFR Security Officer User Profile
  WAGNERR Wagner, Ray
  WILLISR Willis, Rose

```

3. A Change User Profile képernyőn nyomja meg az **F10** (Additional parameters) billentyűt.
4. Lapozzon (page down) lefelé, amíg megtalálja a változtatni kívánt mezőt. Például, ha a felhasználót másik csoporthoz is szeretné hozzárendelni, lapozzon a *Supplemental Groups* mezőhöz.
5. Gépelje be a kívánt értékeket, és nyomja meg az **Enter** billentyűt. Megerősítő üzenetet fog kapni, és ismét a Work with User Profiles képernyő jelenik meg.

```

Change User Profile (CHGUSRPRF)

Type choices, press Enter.

Maximum allowed storage . . . . *NOMAX
Highest schedule priority . . . . 3
Job description . . . . . DPTWH
Library . . . . . QGPL
Group profile . . . . . DPTWH
Owner . . . . . *GRPPRF
Group authority . . . . . *USE
Group authority type . . . . . *PGP
Supplemental groups . . . . . DPTIC
+ for more values

```

Amint módosította a felhasználó adatait, megjelenítheti az eredményeket, hogy ellenőrizze a profilekat.

## Felhasználói profilok megjelenítése

A létrehozott profilok megjelenítésére több módszer létezik.

### Egyetlen profil megjelenítése

Használja az **5** (Display) opciót a Work with User Enrollment vagy a Work with User Profiles képernyők egyikén.

### Egyetlen profil listázása

Használja a Display User Profile parancsot: DSPUSRPRF *profil-neve* DETAIL(\*BASIC) OUTPUT(\*PRINT).

### Csoporttagok megjelenítése

Gépelje be a DSPUSRPRF *csoportprofil neve* \*GRPMBR parancsot. Használhatja az OUTPUT(\*PRINT) opciót a lista nyomtatásához.

## Összes profil listázása

Kilistáztathatja az összes profil nevét és leírását csoportonkénti bontásban a Display Authorized Users (DSPAUTUSR) parancs használatával: `DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT)`.

Mielőtt beállítja a tulajdonjogot és a nyilvános jogosultságot, feltétlenül hajtsa végre a következő feladatokat:

- Fejezze be az összes egyedi profil létrehozását.
- Állítsa a jelszót lejárt állapotba mindegyik profilban.
- Nyomtassa ki az összes profilt csoportbontásban, és tartsa egy helyen a Felhasználói csoportot leíró űrlapokkal. Új felhasználó bejegyzésekor nyomtassa ki ismét a listát.

---

## Erőforrás biztonság beállítása

Ebben a részben objektumok tulajdonjogát és nyilvános jogosultságát, valamint alkalmazások egyedi jogosultságát állítja be. Ugyancsak beállítja a munkaállomások és nyomtatók biztonságát. Hajtsa végre a leírt lépéseket az egyik könyvtárára, majd térjen vissza, és ismétlje meg a lépéseket az alkalmazás összes többi könyvtárára. Amikor egy alkalmazás erőforrás biztonságának beállítását befejezte, ismétlje meg a lépéseket a többi alkalmazásra is.

Alkalmazza az itt leírt eljárásokat, valahányszor új alkalmazást telepít a rendszeren, vagy ha biztonságot akar beállítani egy meglévő alkalmazáson.

A témakör mintául szolgáló képernyői bemutatják a JKL Toy Company Jogosultsági lista űrlapjait, Könyvtárat leíró űrlapjait, valamint Kimeneti sor és munkaállomás biztonsági űrlapját. Az űrlapok mintapéldányait megtalálja a "Tulajdonjog és a nyilvános jogosultság beállítása" című részben.

### Milyen űrlapokra van szükség?

- "Alkalmazások telepítésének tervezése" című részben előkészített Alkalmazás telepítési űrlap.
- "Objektumok csoportosítása" című részben előkészített Jogosultsági lista űrlap.
- "Könyvtárak és objektumok tulajdonjogának meghatározása" című részben előkészített Könyvtárat leíró űrlapok.
- "Nyomtatott listák védelme" és "Munkaállomások védelme" című részekben előkészített Kimeneti sor és munkaállomás biztonság űrlapja.
- "Átfogó biztonsági stratégia tervezése" című részben előkészített Rendszerfelelőségek űrlapja.

Az erőforrás biztonság beállítására több lehetőség kínálkozik. A témakörön belüli lépések sorrendje megegyezik az Alkalmazás telepítési űrlapok, a Jogosultsági lista űrlapja, valamint a könyvtárat leíró űrlap adatainak sorrendjével:

1. Tulajdonjog és nyilvános jogosultság beállítása.
2. Jogosultsági listák létrehozása.
3. Objektumok védelme jogosultsági listával.
4. Felhasználók felvétele jogosultsági listákba.
5. Egyedi jogosultságok beállítása.
6. Nyomtatott listák védelme.
7. Munkaállomások védelme.
8. Rendszeroperátori üzenetsor elérhetőségének korlátozása.

## Tulajdonjog és nyilvános jogosultság beállítása

Ebben a témakörben az alkalmazási könyvtárak, a csoport-, valamint személyi könyvtárak tulajdonjogát és nyilvános jogosultságát fogja beállítani. Hajtsa végre az itt leírtakat az egyik alkalmazásával, majd térjen vissza, és ismétlje meg a lépéseket az összes többi alkalmazására is. A minta képernyők Sharon Jones Alkalmazás telepítési űrlapját mutatják, amelyet a Vevő rendelések alkalmazáshoz készített az "Alkalmazások telepítésének tervezése" című részben.

Alkalmazza az itt leírt eljárásokat, valahányszor új alkalmazást telepít a rendszeren, vagy ha biztonságot akar beállítani egy meglévő alkalmazáson.



Vegye elő az "Alkalmazások telepítésének tervezése" című részben előkészített Alkalmazás telepítési űrlapot.

A tulajdonjog és a nyilvános jogosultság beállítása a következő feladatok végrehajtásából áll:

1. Tulajdonosi profil létrehozása.
2. Könyvtár tulajdonjogának módosítása.
3. Alkalmazási objektumok tulajdonjogának beállítása.
4. Könyvtár nyilvános hozzáféréseinek beállítása.
5. Nyilvános jogosultság beállítása a könyvtár összes objektumára.
6. Nyilvános jogosultság beállítása az új objektumokra.
7. Csoport- és személyi könyvtárak kezelése.

### Bejelentkezés a rendszerre

**Profil** Saját (\*ALLOBJ jogosultság szükséges)

**Menü** MAIN

### Tulajdonosi profil létrehozása

Ha még nincs tulajdonosi profil, tegye a következőt:

- Használja a CRTUSRPRF (Create User Profile) parancsot a létrehozáshoz. Állítsa a jelszót \*NONE értékre.

Ha már van tulajdonosi profil, tegye a következőt:

- Használja a CHGUSRPRF (Change User Profile) parancsot a jelszó \*NONE értékre állításához.

Miután létrehozta a tulajdonos profilját, módosítsa a könyvtár tulajdonjogát.

### Könyvtár tulajdonjogának módosítása

Ez a lépés a könyvtár tulajdonjogát módosítja és nem a könyvtárban lévő objektumokét.

**Figyelem!** Egyeztessen az alkalmazás szállítójával mielőtt az alkalmazás bármely objektumának módosítaná a tulajdonjogát. Néhány alkalmazás funkciója megkövetelhet egy adott objektumtulajdonost.

1. Gépelje be a CHGOBJOWN (Change Object Owner) parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Töltse ki a könyvtárnév, objektumtípus (\*LIB) és új tulajdonos mezőket.
3. Ellenőrizze a megerősítő üzenetet.

```
Change Object Owner (CHGOBJOWN)

Type choices, press Enter.

Object . . . . . > COPGMLIB
Library . . . . . > *LIBL      Name,
Object type . . . . . > *LIB
New owner . . . . . COWNER
Current owner authority . . . . *REVOKE
```

#### Lehetséges hiba

Hibaüzeneteket kap.

#### Helyreállítás

A legáltalánosabb hibatípus, hogy vagy a könyvtár nem található, vagy a tulajdonosi profil. Ellenőrizze gépelését és próbálja újra.

Miután módosította a könyvtár tulajdonjogát, következhet az alkalmazási objektumok tulajdonjogának beállítása.

## Alkalmazási objektumok tulajdonjogának beállítása

Az alkalmazási objektumok tulajdonjogának módosítása megterhelő feladat, mert mindegyiket egyedileg kell elvégezni. Ha lehetséges, kérje a programozót vagy az alkalmazás szállítóját a kívánatos tulajdonjog beállítására.

### Könyvtár objektumainak kilistázása

Mielőtt tulajdonjogot módosít, listázza ki a könyvtár összes objektumát a Display Library paranccsal. Ezt ellenőrző listaként is használhatja. Gépelje be a DSPLIB *könyvtár neve* \*PRINT parancsot.

### Legjobb módszer kiválasztása

Válassza az alábbi két módszer egyikét a könyvtári objektumok tulajdonjogának módosításához:

61. táblázat: *Objektum tulajdonjogának módosítási módszerei*

Módszer	Amit tesz	Mikor érdemes
Work with Objects by Owner parancs	Megjelenít a képernyőn egy listát a profil által birtokolt összes objektumról. Az objektum tulajdonjogának módosítását a parancs egyik opciója biztosítja.	Ez egy jól használható módszert jelent. Azonban, ha QPGMR vagy QSECOFR birtokolja az objektumokat, az IBM nem ajánlja használatát. Ezek a profilok sok objektumot birtokolnak, így a lista nagyon nagy lenne.
Change Object Ownership parancs	A parancsot mindegyik objektumra külön ki kell adni. Azonban használhatja a <i>Retrieve (F9)</i> opciót az előző parancs ismétlésére, csökkentve ezzel a gépelési igényt.	Ez gyorsabb módszernek tűnik, amikor QPGMR vagy QSECOFR birtokolja az objektumokat.

**Work with objects by Owner (WRKOBJOWN) parancs használata:** Ez a módszer elsősorban olyan könyvtári objektumok tulajdonjogának módosítására való, amelyeket *nem* IBM profil (QPGMR vagy QSECOFR) birtokol.

1. Gépelje be a WRKOBJOWN *tulajdonosprofil neve* parancsot. A képernyőn megjelenik az adott profil birtokában lévő összes objektum felsorolása.
2. Gépeljen be **9** (Change owner) értéket mindazon objektumok elé, amelyekkel dolgozni akar.
3. Gépelje be a képernyő alján a *Parameters or command* vonalra a NEWOWN(*tulajdonosprofil neve*) parancsot, és nyomja meg az **Enter** billentyűt.
4. A rendszer módosítja az összes kijelölt objektum tulajdonjogát a begépelte új profil számára. A képernyő alján megerősítő üzenetet kap. Az objektumok eltűnnek a képernyőről, mivel a profil már nem birtokolja őket.
5. Ismétlje meg a fenti lépéseket (2 - 4), amíg az összes kívánt módosítást végre nem hajtja.

```

Work with Objects by Owner

User profile . . . . . : OLDFOWNER

Type options, press Enter.
  2=Edit authority      4=Delete  5=Display author
  8=Display description 9=Change owner

Opt  Object      Library      Type      Attribute
  9   CUSTMAS    CUSTLIB     *FILE
  9   CUSTMSGQ   CUSTLIB     *MSGQ
     ITEMMSGQ   ITEMLIB     *MSGQ

:

Parameters or command
====> NEWOWN (COWNER)
F3=Exit  F4=Prompt  F5=Refresh  F9=Retrieve
F18=Bottom

```

**Lehetséges hiba**

A Change Object Owner képernyőt látja.

**Helyreállítás**

Akkor láthatja ezt a képernyőt, ha beállította a **9** (Change owner) opciót, de nem gépelt be paramétert a Work with Objects by Owner képernyő alján. Ugyancsak ezt a képernyőt látja, ha helytelen paramétert gépelt be. Nyomja meg az **F12** (Cancel) billentyűt a Work with Objects by Owner képernyőhöz való visszatérés érdekében. Próbálja újra. Győződjön meg róla, hogy a mintában megadott módon gépelte be a paramétert.

A QPGMR vagy QSECOFR által birtokolt objektumok tulajdonosainak módosításához használja a Change Object Owner parancsot.

**Change Object Owner parancs használata:** Ez a módszer elsősorban olyan könyvtári objektumok tulajdonjogának módosítására való, amelyeket *IBM profil* (QPGMR vagy QSECOFR) birtokol.

1. Gépelje be a CHGOBJOWN parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Töltse ki a képernyő mezőit a listáján szereplő első objektum adataival, és nyomja meg az **Enter** billentyűt.

```

Change Object Owner (CHGOBJOWN)

Type choices, press Enter.

Object . . . . . > CUSTMAS
Library . . . . . > CUSTLIB
Object type . . . . . > *FILE
New owner . . . . . COWNER
Current owner authority . . . . *REVOKE

```

3. Megerősítő üzenetet kap arról, hogy az objektum tulajdonjoga megváltozott. Húzza ki a tételt a listájáról.
4. Nyomja meg az **F9** (Retrieve) billentyűt a begépelte parancs ismételt betöltésére.
5. Nyomja meg az **F4** (Prompt) billentyűt. A Change Object Owner képernyőn írja be a következő objektum információit, és nyomja meg az **Enter** billentyűt.
6. Ismétlje meg a 4. és 5. lépést a könyvtár minden objektumára.

**Munka ellenőrzése**

Ellenőrizze a Work with Objects by Owner parancs segítségével, hogy megváltozott-e a könyvtár minden objektumának tulajdonjoga. Gépelje be a *WRKOBJOWN új tulajdonosprofil neve* parancsot. Hasonlítsa össze a könyvtár objektumainak kezében lévő listájával.

Miután módosította a könyvtári objektumok tulajdonjogát, beállíthatja a könyvtár nyilvános elérését.

## Könyvtár nyilvános jogosultságának beállítása

Miután beállította az alkalmazási objektumok tulajdonjogát, módosíthatja a könyvtár nyilvános jogosultságát az Edit Object Authority (EDTOBJAUT) parancssal.

1. Gépelje be az EDTOBJAUT *könyvtár neve* \*LIB parancsot.
2. Vigye a kurzort a \*PUBLIC mezőre.
3. Gépelje be a könyvtár nyilvános jogosultságát (amivel szeretné, hogy a nyilvánosság rendelkezzen), és nyomja meg az **Enter** billentyűt.

```

                                Edit Object Authority
Object . . . . . : CUSTLIB      Owner . . . . . : COWNER
Library . . . . . : QSYS       Primary group . . . : *NONE
Object type . . . . . : *LIB

Type changes to current authorities, press Enter.

Object secured by authorization list . . . . . *NONE

User      Group      Object
COWNER
*PUBLIC   Authority
          *ALL
          *CHANGE

```

4. A képernyő az új jogosultságot mutatja.

Most beállíthatja a könyvtár összes objektumának nyilvános jogosultságát.

## Nyilvános jogosultság beállítása a könyvtár összes objektumára

A Revoke Object Authority (RVKOBJAUT) parancs segítségével eltávolíthatja a könyvtári objektumok aktuális nyilvános jogosultságát. A Grant Object Authority (GRTOBJAUT) parancs révén pedig beállíthat új nyilvános jogosultságot a könyvtár összes objektumára:

1. Gépelje be a RVKOBJAUT parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Töltse ki a képernyőt a minta szerint, behelyettesítve saját alkalmazási könyvtárának nevét, és nyomja meg az **Enter** billentyűt.

```

                                Revoke Object Authority (RVKOBJAUT)

Type choices, press Enter.

Object . . . . . *all
Library . . . . . custlib
Object type . . . . . *all
Users . . . . . *public
          + for more values
Authority . . . . . *all

```

**Megjegyzés:** Ha a könyvtár rengeteg objektumot tartalmaz, néhány perc is eltelhet, míg a rendszer végrehajtja a kérést.

3. Gépelje be a GRTOBJAUT parancsot, és nyomja meg az **F4** (Prompt) billentyűt.

4. Töltse ki a képernyőt a minta szerint, behelyettesítve saját alkalmazási könyvtárának nevét és a kívánt jogosultságot, majd nyomja meg az **Enter** billentyűt.

```

Grant Object Authority (GRTOBJAUT)

Type choices, press Enter.

Object . . . . . *all
Library . . . . . custlib
Object type . . . . . *all
Users . . . . . *public
                + for more values
Authority . . . . . *use

```

**Megjegyzés:** Ha a könyvtár rengeteg objektumot tartalmaz, néhány perc is eltelhet míg a rendszer végrehajtja a kérést.

Miután beállította a könyvtár valamennyi objektumának nyilvános jogosultságát, a job napló segítségével ellenőrizheti munkáját.

**Munka ellenőrzése job napló segítségével:** Ha a GRTOBJAUT parancsot használja több objektum jogosultságának megváltoztatásához, ellenőrizze a naplót (job log), hogy a művelet sikeresen fejeződött-e be.

1. Gépelje be a DSPJOBLOG (Display Job Log) parancsot.
2. Nyomja meg az **F10** (Display detailed messages) billentyűt.
3. A könyvtár minden objektumára vonatkozóan kell üzenetnek lenni a jogosultság változásáról. Húzza ki az objektumokat a listájáról amikor az üzeneteket ellenőrzi.

```

Display All Messages

System: RCHASxxx
Job . . . : QPADEV0010   User . . . : JCHEIDEL   Number . . . : 025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Authority given to user *PUBLIC for object CUSTMAS in CUSTLIB object type
  *FILE.
  Authority given to user *PUBLIC for object CUSTMSGQ in CUSTLIB object type
  *MSGQ.
  Authority given to 2 objects. Not given to 0 objects. Partially given to 0
  objects.
  Object authority granted.
7>> dspjoblog

```

#### Lehetséges hiba

A job napló jelzi, hogy több objektum jogosultsága nem változott meg a könyvtárban.

#### Helyreállítás

Vegye igénybe a Help (**F1**) billentyűt, ha további információkat szeretne kapni az üzenetről. Használja az EDTOBJAUT parancsot a problémás objektumok jogosultságának egyedi módosításához.

Most beállíthatja az új objektumok nyilvános jogosultságát.

### Új objektumok nyilvános jogosultságainak beállítása

A könyvtárleírás (CRTAUT) paramétere határozza meg, hogy mi lesz a könyvtár újonnan létrehozott objektumának nyilvános jogosultsága. Az objektumokat létrehozó parancsok használják és alapértelmezésnek veszik a CRTAUT által definiált jogosultságot. A CRTAUT paramétert a meglévő könyvtári objektumok többségére érvényes nyilvános jogosultsági értékkel azonosra kell beállítani.

1. Gépelje be a CHGLIB *könyvtár-neve* parancsot, és nyomja meg az **F4** (Prompt) billentyűt.

2. Nyomja meg az **F10** (Additional parameters) billentyűt.
3. Gépelje be választását a *Create authority* mezőre.

```

Change Library (CHGLIB)

Type choices, press Enter.

Library . . . . . > CUSTLIB
Library type . . . . . *PROD
Text 'description' . . . . . 'Customer Records'

Additional Parameters

Create authority . . . . . *CHANGE
Create object auditing . . . . . *SYSVAL

```

Ha a CRTAUT mezőre \*SYSVAL értéket ad, a rendszer a QCRTAUT rendszerváltozónak az új objektum létrehozásakor aktuális értéke alapján határozza meg a jogosultságot. Ha a CRTAUT paraméternek egy adott értéket ad, megelőzheti a QCRTAUT rendszerváltozó módosításából eredő jogosultság változást.

Most a csoport- és személyi könyvtárak kezelése következhet.

## Csoport- és személyi könyvtárak kezelése

A saját profilja birtokolja a csoport- és személyi könyvtárakat, amelyeket a felhasználói csoportok és az egyedi felhasználók beállításakor hozott létre.

Használja fel az itt tanult módszereket ahhoz, hogy csoportprofilhoz rendelje a csoportkönyvtár tulajdonjogát, és egyedi felhasználói profilhoz a személyi könyvtárakét. Alkalmazza az EDTOJAUT parancsot.

Állítsa be a Create Authority paramétert minden csoport- és személyi könyvtárra, a könyvtárban keletkező új objektumok nyilvános jogosultságának meghatározása érdekében. Használja a CHGLIB parancsot.

Mielőtt elkezdené jogosultsági listák létrehozását, végezze el az alábbi feladatokat:

- Az Alkalmazás telepítési űrlapok és a Könyvtárak leíró űrlapok segítségével ellenőrizze, hogy létrehozott és beállított minden tulajdonjogot és nyilvános jogosultságot az összes alkalmazási könyvtárra.
- Állítsa be az összes létrehozott csoport- és személyi könyvtár tulajdonjogát, valamint nyilvános jogosultságát.

**Megjegyzés:** Listát kaphat a rendszer összes könyvtáráról a DSPOBJD \*ALL \*LIB \*PRINT parancs segítségével.

## Jogosultsági lista létrehozása

Miután beállította a tulajdonjogot és a nyilvános jogosultságot, készen áll a jogosultsági listák beállítására. A Jogosultsági lista űrlapján leírt adatok felhasználásával hozzon létre jogosultsági listákat a könyvtár védelmére. Alkalmazza a Create Authorization List (CRTAUTL) parancsot:

1. Gépelje be a CRTAUTL parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Írja át az adatokat a Jogosultsági lista űrlapjáról.
3. Nyomja meg az **F10** (Additional parameters) billentyűt.
4. Használja a jogosultsági paramétert a lista által védett objektumok nyilvános jogosultságának meghatározására.
5. Ellenőrizze a megerősítő üzenetet.

```

Create Authorization List (CRTAUTL)

Type choices, press Enter.

Authorization list . . . . . custlst1
Text 'description' . . . . . Files cleared at

Additional Parameters

Authority . . . . . *ALL

```

**Lehetséges hiba**

**Helyreállítás**

Helytelenül gépelte be a lista nevét.

Nem változtathatja meg a lista nevét, ha a rendszer egyszer már létrehozta. Törölje a listát (DLTAUTL) paranccsal és próbálja újra.

Elfelejtette megadni a lista nyilvános jogosultságát.

Használja az Edit Authorization List (EDTAUTL) paranccsot.

Következő lépésként védheti objektumait jogosultsági listával.

## Objektumok védelme jogosultsági listával

Amint létrehozza a jogosultsági listát, az Edit Object Authority (EDTOBJAUT) paranccsal védetté teheti a Jogosultsági lista űrlapján szereplő elemeket:

1. Gépelje be az EDTOBJAUT paranccsot, és nyomja meg az **F4** (prompt) billentyűt.
2. Töltse ki a képernyő mezőit, és nyomja meg az **Enter** billentyűt.
3. Adja meg a lista nevét az Edit Object Authority képernyőn.
4. Ha az objektumok nyilvános jogosultságát a lista határozza meg, módosítsa a mezőt \*AUTL értékre.
5. Ismételje meg ezt a lépést a Jogosultsági lista űrlapjának minden objektumára.

```

Edit Object Authority

Object . . . . . : ARFILE01      Owner . . . . . : OWNER
Library . . . . . : CUSTLIB      Primary group . . . : *NONE
Object type . . . . . : *FILE

Type changes to current authorities, press Enter.

Object secured by authorization list . . . . . CUSTLST1

User      Group      Object
OWNER
*PUBLIC   *ALL
          *AUTL

```

A továbbiakban hozzáadhat felhasználókat a jogosultsági listához.

## Felhasználók hozzáadása jogosultsági listához

Amint jogosultsági listával védi az objektumokat, az Edit Authorization List (EDTAUTL) paranccsal hozzáadhatja a listához a Jogosultsági lista űrlapján szereplő felhasználókat:

1. Gépelje be az EDTAUTL *jogosultsági lista neve* paranccsot.
2. Nyomja meg az **F6** (Add new users) billentyűt az Edit Authorization list képernyőn.
3. Gépelje be a felhasználók vagy csoportok neveit és a lista objektumaihoz való jogosultságukat, majd nyomja meg az **Enter** billentyűt.

4. Az új felhasználóknak meg kell jelenniük a listán.

```

                                Add New Users
Object . . . . . : WSLST1      Owner . .
Library . . . . . : QSYS

Type new users, press Enter.

      Object  List
User   Authority Mgt
QSECOFR *CHANGE
    
```

**Lehetséges hiba**

Rossz jogosultságot adott egy csoportnak vagy felhasználónak a listára vonatkozóan.  
Téves felhasználó- vagy csoportnevet adott a listához.

**Helyreállítás**

Az Edit Authorization List képernyőn megváltoztathatja a jogosultságot.  
Eltávolíthatja a felhasználót vagy a csoportot a Remove Authorization List Entry (RMVAUTLE) parancsot használva, vagy szóközöket gépelhet a User's Authority mezőre az Edit Authorization List képernyőn.

**Munka ellenőrzése**

Használja a Display Authorization List (DSPAUTL) parancsot a jogosultsági listához adott felhasználók megjelenítéséhez. A lista által védett összes objektum megjeleníthető az **F15** billentyűvel.

Mielőtt beállítja az egyedi jogosultságokat, végezze el az alábbi feladatokat:

- A CRTAUTL parancs segítségével hozza létre az alkalmazás számára szükséges listákat.
- Az EDTOAJAUT parancs segítségével védje az objektumokat jogosultsági listákkal.
- Adja hozzá a felhasználókat a jogosultsági listához az EDTAUTL parancs felhasználásával.

**Egyedi jogosultságok beállítása**

A "Tulajdonjog és a nyilvános jogosultság beállítása" című részben megismerhette a könyvtári objektumok nyilvános jogosultságának beállítását a Könyvtárat leíró űrlap első részében található adatok alapján, a GRTOBJAUT parancs használatával. Most pedig az Edit Object Authority (EDTOBJAUT) parancs segítségével beállíthat egyedi jogosultságokat a könyvtárnak, valamint a könyvtárban található objektumoknak, alapul véve a Könyvtárat leíró űrlap második részének információit.

Az egyedi jogosultságok beállításához olvassa el az alábbiakat:

- Egyedi jogosultság beállítása könyvtár számára.
- Egyedi jogosultság beállítása objektum számára.
- Jogosultság beállítása egyszerre több objektum számára.

**Egyedi jogosultság beállítása könyvtár számára**

A könyvtár valóban egy speciális típusú objektum. Ugyanúgy állítja be a jogosultságot a könyvtárhoz, mint bármely más objektumhoz, használva az EDTOAJAUT parancsot. Minden könyvtár az IBM által szállított QSYS könyvtárban található. A képernyők a JKL Toy Company Szerződések (CONTRACTS) könyvtárának információit (a Könyvtárat leíró űrlap második részében található) mutatják a következő példákban:

Könyvtári objektumok egyedi jogosultságainak listája				
Csoportprofil, felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági lista



DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. Gépelje be az EDTOBJAUT parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Töltse ki a képernyő mezőit, és nyomja meg az **Enter** billentyűt.

```

Edit Object Authority (EDTOBJAUT)

Type choices, press Enter.

Object . . . . . CONTRACTS
Library . . . . . QSYS
Object type . . . . . *LIB

```

3. Az Edit Object Authority képernyőn nyomja meg az **F6** (Add new users) billentyűt, hogy a képernyőn nem listázott felhasználóknak jogosultságot tudjon adni.
4. Nyomja meg az **Enter** billentyűt.

```

Add New Users

Object . . . . . : CONTRACTS      Owner . . . . . : OWNCP
Library . . . . . : QSYS          Primary group . . . : *NONE
Object type . . . . . : *LIB

Type new users, press Enter.

User          Object
DPTSM         *USE  Authority
DPTMG         *USE

```

5. Az Edit Object Authority képernyőnek meg kellene egyeznie a Könyvtár leíró űrlap első és második részének információival.

```

Edit Object Authority

Object . . . . . : CONTRACTS      Owner . . . . . : OWNCP
Library . . . . . : QSYS          Primary group . . . : *NONE
Object type . . . . . : *LIB

Type changes to current authorities, press Enter.

Object secured by authorization list . . . . . *NONE

User      Group      Object
OWNCP     *ALL
DPTSM     *USE
DPTMG     *USE
*PUBLIC   *EXCLUDE

```

A könyvtári új objektumok nyilvános jogosultsága (CRTAUT) nem jelenik meg. Használja a Display Library (DSPLIB) parancsot a CRTAUT megtekintésére.

Az eljárással egyébként megadhat egyedi jogosultságot is egy objektum számára a rendszeren.

Most beállíthat egyedi jogosultságot egy objektum számára.

## Egyedi jogosultság beállítása objektum számára.

Objektumhoz való egyedi jogosultság beállításának módja megegyezik a könyvtárra vonatkozó egyedi jogosultság beállításával. A képernyők a JKL Toy Company COPGMLIB könyvtárának információit (a Könyvtár leíró űrlap második részében található) használják fel:

62. táblázat: JKL Toy Company Könyvtár leíró űrlapja

Csoportprofil, felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági lista
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Gépelje be az EDTOBJAUT parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Töltse ki a képernyő mezőit, és nyomja meg az **Enter** billentyűt.
3. Töltse ki a jogosultsági információkat az Edit Object Authority képernyőn, és nyomja meg az **Enter** billentyűt.

```
                                Edit Object Authority
Object . . . . . : COMSGQ01      Owner . . . . . : OWNCO
Library . . . . . : COPGMLIB    Primary group . . . : *NONE
Object type . . . : *MSGQ
Type changes to current authorities, press Enter.
Object secured by authorization list . . . . . *NONE

User      Group      Object
OWNCO                    *ALL
*PUBLIC                    *CHANGE
```

Most beállíthat jogosultságot egyszerre több objektum számára.

## Jogosultság beállítása egyszerre több objektum számára

Az eddigi példákban az EDTOBJAUT parancsot használtuk, amellyel csak egy objektumhoz állítottunk be egyedi jogosultságot. A Grant Object Authority (GRTOBJAUT) parancssal egyszerre több objektum számára állíthat be jogosultságot. Gépelje be a GRTOBJAUT parancsot, és nyomja meg az **F4** (Prompt) billentyűt. A következőkben minta megoldásokat talál többszörös, egyidejű módosításokra:

- Ebben a példában a CUSTLIB összes üzenetsorának nyilvános jogosultsága \*CHANGE értékre változik.

```
                                Grant Object Authority (GRTOBJAUT)
Type choices, press Enter.
Object . . . . . *all
Library . . . . . custlib
Object type . . . *msgq
Users . . . . . *public
                + for more values
Authority . . . . *change
```

- Ebben a példában a CUSTLIB WRK kezdőkezőkarakterekkel rendelkező fájljaira kap \*ALL jogosultságot az AMES nevű felhasználó.

```

Grant Object Authority

Type choices, press Enter.

Object . . . . . WRK*
Library . . . . . custlib
Object type . . . . . *file
Users . . . . . AMES
+ for more values
Authority . . . . . *all

```

Ez a példa speciális technikát használ paraméter megadásra, amit **általános** elnevezésnek hívunk. Sok parancs megengedi, hogy az első karaktereket követően csillagot (\*) használjon a paraméter megadásakor. Ilyenkor a rendszer végrehajtja a műveletet az összes olyan objektumra, amelynek a neve az adott karakterekkel kezdődik. A parancs online súgója mondja meg, mely paraméterekre lehet az általános nevet használni.

- Két lépésben kell biztonságossá tenni az AR betűkkel kezdődő fájlokat, amelyek az ARLST1 nevű jogosultsági listát használják, és nyilvános jogosultságukat a lista határozza meg. A képernyők bemutatják a szükséges lépéseket.

```

Grant Object Authority

Type choices, press Enter.

Object . . . . . AR*
Library . . . . . CUSTLIB
Object type . . . . . *FILE
:
Authorization list . . . . . ARLST1

```

```

Grant Object Authority

Type choices, press Enter.

Object . . . . . AR*
Library . . . . . CUSTLIB
Object type . . . . . *FILE
Users . . . . . *PUBLIC
+ for more values
Authority . . . . . *AUTL
+ for more values

```

A "Munka ellenőrzése job napló segítségével" című részben leírtak szerint a DSPJOBLOG paranccsal ellenőrizheti, hogy a rendszer elvégezte-e a kívánt jogosultsági változtatásokat.

Mielőtt áttérne a "Nyomtatott listák védelme" című részre, állítsa be a Könyvtárat leíró űrlap második részében megadott egyedi jogosultságokat az EDTOJAUT vagy a GRTOJAUT parancsokkal.

## Nyomtatott listák védelme

Miután beállította az egyedi jogosultságokat, védheti a bizalmas listákat a következő témakörökben leírtak alapján:

- Kimeneti sor létrehozása és kezelésének vezérlése.
- Speciális nyomtatott lista hozzárendelése a sorhoz.

### Kimeneti sor létrehozása

1. Gépelje be a CRTOUTQ (Create Output Queue) parancsot, és nyomja meg az **F4** (Prompt) billentyűt.
2. Adja meg a kimeneti sor nevét és a könyvtárat.
3. Nyomja meg az **F10** (Additional parameters) billentyűt.

4. Lapozzon(page down) a kimeneti sor biztonsági információihoz.

```

Create Output Queue (CRTOUTQ)

Type choices, press Enter.

Output queue . . . . . > NEWCP
Library . . . . . CONTRACTS
Maximum spooled file size:
Number of pages . . . . . *NONE          Number, *NONE
Starting time . . . . .                  Time
Ending time . . . . .                    Time
+ for more values
Order of files on queue . . . . . *FIFO
Remote system . . . . . *NONE

:
Text 'description' . . . . . New Contracts Queue

```

5. Írja be a Kimeneti sor és munkaállomás biztonság űrlapján lévő információkat, meghatározva ezzel, hogy ki használhatja és felügyelheti a kimeneti sort.

6. Nyomja meg az **Enter** billentyűt, és ellenőrizze a megerősítő üzeneteket.

```

Create Output Queue (CRTOUTQ)

Type choices, press Enter.

Additional Parameters

Display any file . . . . . *NO
Job separators . . . . . 0
Operator controlled . . . . . *NO
Data queue . . . . . *NONE
Library . . . . .
Authority to check . . . . . *OWNER
Authority . . . . . *LIBCRTAUT

```

**Lehetséges hiba**

**Enter** billentyűt nyomott **F10** helyett.

Rossz könyvtárban hozta létre a kimeneti sort.

**Helyreállítás**

Használja a Change Output Queue (CHGOUTQ) parancsot a további adatok beviteléhez.

Vigye át a sort a megfelelő könyvtárba a Move Object (MOV OBJ) paranccsal.

Most hozzárendelheti a nyomtatandó listát egy kimeneti sorhoz.

**Nyomtató kimeneti lista hozzárendelése kimeneti sorhoz**

Miután létrehozott egy kimeneti sort, hozzárendelheti a listát a sorhoz. A nyomtatófájl általában vezérli a nyomtatandó lista kimenő helyét. Ellenőrizze az alkalmazás szállítójával a nyomtatófájlok neveit és könyvtárait a bizalmas riportok számára.

Ha nem jut ehhez az információhoz, nyomtasson riportot és tartsa azt a kimeneti sorban. Használja az Attribute opciót a Work with Spooled Files képernyőn a nyomtatófájl nevének azonosítása végett. A nyomtatófájl neve a *Device file* mezőn jelenik meg a Work with Spooled File Attributes képernyőn.

A nyomtatófájl rendeltetési helyének (kimeneti sor) módosításához használja a Change Printer File (CHGPRTF) parancsot.

```
CHGPRTF FILE(könyvtár neve/nyomtatófájl neve)
      OUTQ(könyvtár neve/kimeneti sor neve)
```

A riport új helyre megy ezután, valahányszor valaki ismét kéri a riportot. Egy kimeneti sorban lévő "spool" fájl rendeltetési helyének módosításához használja a Work with Spooled Files képernyő módosítás opcióját.

Például, Sharon Jones a JKL Toy Company esetében az árlisták részére a PRCLST1 nyomtatófájlt rendelte a PRICEQ kimeneti sorhoz. Ezt gépeli:

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

Ahhoz, hogy az összes árlista riport a PRICEQ kimeneti sorba menjen, Sharon általános nyomtatófájl nevet használ:

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

Ahhoz, hogy az összes új szerződés a NEWCP kimeneti sorba menjen, Sharon megváltoztatta a szerződés létrehozásához mintaként szolgáló dokumentum kimeneti sorát.

## Munka ellenőrzése

A bizalmas dokumentumok védelmi stratégiájának legjobb ellenőrzési módszere a dokumentumok nyomtatása. Nézze meg, hogy valóban a kijelölt kimeneti sorba megy-e. Jelentkezzen be rendszeroperátorként és ellenőrizze, hogy látja-e és tudja-e kezelni a fájlokat a sorban.

Mielőtt biztonságossá tenné a munkaállomásokat, feltétlenül végezze el a következőket:

- Hozza létre a Kimeneti sor és munkaállomás biztonság űrlapján felsorolt kimeneti sorokat a CRTOUTQ parancs segítségével.
- Rendelje hozzá a kimenő listákat az új kimeneti sorokhoz a CHGPRTF parancs használatával.

## Munkaállomások biztonsága

Miután biztonságossá tette a kimenő listákat, gondoskodjon a munkaállomások biztonságáról. Ugyanúgy kezelheti a munkaállomásokat jogosultság szempontjából, mint a rendszer más objektumait. Használja az EDTOBJAUT parancsot, ha jogosultságot ad a felhasználóknak a munkaállomások használatára.

A felhasználóknak \*CHANGE jogosultsággal kell rendelkezniük a munkaállomásról történő bejelentkezéshez. Ha a QLMTSECOFR rendszerváltozó No (0) értékű, a biztonsági felelős és az \*ALLOBJ jogosultságú felhasználók bármely munkaállomáson be tudnak jelentkezni.

Ha a QLMTSECOFR rendszerváltozó Yes (1) értékű, kövesse az alábbi lépéseket a munkaállomásokhoz való jogosultság beállításához:

Munkaállomásról bejelentkező felhasználók	Nyilvános jogosultság	QSECOFR jogosultság	Egyedi felhasználói jogosultság
Minden felhasználó	*CHANGE	*CHANGE	Nem igénylődik
Csak kiválasztott felhasználók	*EXCLUDE	Nem jogosult	*CHANGE
Kiválasztott- és az összes objektumhoz jogosult felhasználók	*EXCLUDE	*CHANGE	*CHANGE
Minden felhasználó, kivéve az összes objektumhoz jogosult	*CHANGE	Nem jogosult	Nem igénylődik

Mielőtt korlátozná a rendszeroperátori üzenetsor elérhetőségét, használja az EDTOBJAUT parancsot a munkaállomások biztonságának beállításához, a Kimeneti sor és munkaállomás biztonság űrlapján felírt adatok alapján.

## Rendszeroperátori üzenetsor elérhetőségének korlátozása.

Növelheti a biztonságot a kimenő lista védelmével, a munkaállomások biztonságossá tételével és a rendszeroperátori üzenetsor elérhetőségének korlátozásával.

Az ASSIST menü üzenetkezelő opciója engedi a felhasználóknak a rendszeroperátor (QSYSOPR) üzenetsorát megjelenítő funkcióbillentyű használatát. A rendszeroperátori üzenetekre adott helytelen válasz problémát okozhat a rendszer működésében. \*CHANGE jogosultság kell a válaszadáshoz és az üzenetek törléséhez. Csak a rendszeroperátornak kellene ezzel a jogosultsággal rendelkezni. Tekintse át a Rendszerfelelőségek űrlapját, hogy eldöntse, kinek legyen \*CHANGE jogosultsága a rendszeroperátori üzenetsorhoz.

Használja az EDTOAJAUT parancsot:

1. Gépelje be az EDTOAJAUT QSYSOPR \*MSGQ parancsot, és nyomja meg az **Enter** billentyűt.
2. Nyomja meg az **F11** billentyűt a részletes objektumjogosultság megjelenítéséhez.
3. Adjon \*OBJOPR nyilvános jogosultságot, ahogy azt a mintán látja, és nyomja meg az **Enter** billentyűt.

```
                Edit Object Authority
Object . . . . . : QSYSOPR      Owner . . . . . : QSYS
Library . . . . . : QSYS       Primary group . . . : *NONE
Object type . . . . : *MSGQ

Type changes to current authorities, press Enter.

Object secured by authorization list . . . . . *NONE

User      Group      Object Authority Opr Mgt Exist Alter Ref
*PUBLIC

USER DEF X
```

4. A rendszer módosítja az *Object Authority* oszlopot USER DEF (User defined) értékre.
5. Nyomja meg ismét az **F11** billentyűt a részletes adatjogosultság megjelenítéséhez.
6. Adjon \*ADD nyilvános jogosultságot, ahogy azt a mintán látja, és nyomja meg az **Enter** billentyűt.

```
                Edit Object Authority
Object . . . . . : QSYSOPR      Owner . . . . . : QSYS
Library . . . . . : QSYS       Primary group . . . : *NONE
Object type . . . . : *MSGQ

Type changes to current authorities, press Enter.

Object secured by authorization list . . . . . *NONE

User      Group      Object Authority Read Add Update Delete Execute
*PUBLIC

USER DEF X
```

7. Használja az **F6** (Add Users) billentyűt a QSYSOPR üzenetekért felelős felhasználók bejegyzéséhez. Adjon \*CHANGE jogosultságot nekik.

**Figyelem!** Ne adjon \*EXCLUDE nyilvános jogosultságot. Minden munkának (és felhasználónak) képesnek kell lenni üzenetet küldeni a QSYSOPR üzenetsorba.

Az alábbiakat tegye meg, ha bizonyos akar abban lenni, hogy befejezte az erőforrás biztonság beállítását:

- A Jogosultsági lista űrlapok és a Könyvtár leíró űrlapok segítségével ellenőrizze, hogy kialakította az összes alkalmazási könyvtár biztonságát.
- Ellenőrizze a Kimeneti sor és munkaállomás biztonság űrlapjának adatait annak megállapítására, hogy biztonságossá tette munkaállomásait és létrehozta a speciális kimeneti sorokat.
- Korlátozza a rendszeroperátori (QSYSOPR) üzenetsor elérését.

- Mentse el az alkalmazási könyvtárait a leszállított előírás szerint. A rendszer megőrzi a tulajdonjogot és a nyilvános jogosultságot az alkalmazással együtt.
- Mentse el a létrehozott biztonsági információkat a Save Security Data (SAVSECDTA) parancs segítségével. A "Biztonsági információk mentése" című témakör részletesen tárgyalja a biztonsági információk mentését.

Most elkezdheti a biztonsági beállítások tesztelését.

---

## Biztonság tesztelése

Ez a témakör a rendszeren létrehozott biztonság tesztelésének technikáit ismerteti. A tesztelés ebben a környezetben annak ellenőrzését jelenti, hogy a beállítások a várakozásnak megfelelően dolgoznak és hatnak. A "Biztonság figyelése" című rész tárgyalja, hogyan lehet kiértékelni a rendszerbiztonság hatékonyságát.

Próbálja ki a biztonságot valahányszor komolyabb változtatásokat eszközöl a rendszeren. Például, ha új alkalmazást vesz fel, módosítja egy meglévő alkalmazás erőforrás biztonságát, új felhasználói csoportot vesz fel vagy megváltoztatja a biztonsági szintet.

Olvassa át az alábbi témaköröket a teszteléshez és a problémák diagnosztizálásához, mikor biztonsági változtatásokat végez:

- Felhasználói profilok tesztelése.
- Erőforrás biztonság tesztelése.

## Felhasználói profilok tesztelése

A biztonság tesztelésének kezdeteként ki akarja próbálni az egyik felhasználói profilt, amikor egy új csoportot állít be a rendszeren. Próbálja ki az egyik egyedi profilt, amelyet a csoportprofilból hozott létre.

- Sikeresen be tud jelentkezni a profillal? Ha nem tud bejelentkezni, ellenőrizze a naplót (job log), ami a sikertelen bejelentkezés hatására lesz kitöltve. Az Assist menü Work with Printer Output opciójával találhatja meg a naplót további információkért.

A leggyakoribb problémák:

- A szükséges objektumok egyike hiányzik, mint például kezdeti menü, aktuális könyvtár, vagy kezdeti program.
- A job leírásban specifikált könyvtárlista okoz hibákat. Vagy a könyvtár hiányzik, vagy elfelejtette a QGPL, QTEMP könyvtárakat felvenni a listába.
- A felhasználónak nincs jogosultsága a munkaállomás használatára.
- Mikor bejelentkezik, a megfelelő kezdeti menü vagy program jelenik meg a képernyőn?
- Mi történik, ha a bejelentkezési képernyőn ad meg kezdeti menüt vagy aktuális könyvtárat? Ha a felhasználói profil Korlátolt képességek mezője (YES) beállítású, hibaüzenetet kellene kapni.
- A megfelelő képernyő jelenik meg az Attention gomb lenyomásakor?
- A lista a megfelelő nyomtatón jelenik meg? Ha nem, használja a Work with Printer Output opciót az ASSIST menüben a lista megtalálásához. Ellenőrizze a felhasználói profilt és a job leírást, hogy megtalálja, miért ment a kimenő lista másik nyomtatóra.
- Elér parancssort?
- Végre tudja hajtani az alkalmazási funkciókat biztonsági hibák nélkül? További részletekért olvassa el az "Erőforrás biztonság tesztelése" című részt.
- Végre tudja hajtani a szükséges rendszerfeladatokat, mint például nyomtatók kezelése, könyvtárak mentése?

Ha a rendszer a jelszó cseréjét kérte mikor bejelentkezett a profillal, állítsa vissza a profillal azonos jelszót a tesztelés befejezését követően:

1. Jelentkezzen be a saját profiljával (biztonsági felelősi jogosultsággal).
2. Gépelje be a `CHGUSRPRF profil neve PASSWORD(profil neve) PWDEXP(*YES)` parancsot.

Most, hogy kipróbálta a felhasználói profilokat, ellenőrizheti az erőforrás biztonságát.

## Erőforrás biztonság tesztelése

Miután kipróbálta a felhasználói profilokat, tesztelje le az erőforrás biztonságát is. Amikor erőforrás biztonságot tesztel, keresse a következőket:

- Azokat a felhasználókat, akiknek nincs elég jogosultságuk munkájuk elvégzéséhez.
- Azokat a felhasználókat, akiknek több jogosultságuk van, mint amennyit szándékában állt adni.

### Elégtelen jogosultság tesztelése

Tesztelje mind az interaktív, mind a kötegelt funkciókat, hogy rendelkezik-e a profil elégséges jogosultsággal.

### Interaktív mód tesztelése

Az alkalmazás erőforrás biztonságának teszteléséhez esetleg több különböző felhasználói profillal kell bejelentkezni. A feladata az, hogy minta-felhasználók segítségével meggyőződjön arról, hogy az adott jogosultságok elegendők-e.

- Teszt funkciók, amelyek különböző jogosultsági szintet igényelnek: megtekintés, változtatás, törlés.
- Teszt programok, nem pont menük. Egy menüpont kiválasztása nem biztos, hogy elég a jogosultság teszteléséhez. Néha a rendszer nem éri el a fájlt addig, amíg egy műveletet valóban meg nem próbál végrehajtani (például rekord törlése). A jogosultság ellenőrzése akkor történik meg, amikor a rendszerrel megnyitja a fájlt. Az alkalmazás kivitele meghatározza, hogy a rendszer mikor nyitja meg a fájlt.
- Jegyezze fel a biztonsági hibákat és oldja meg őket. Ha egy jogosultsági hiba jön, nézze meg a képernyőn megjelenő üzenetet, mely megmondja milyen jogosultsága elégtelen, vagy melyik objektumot próbálta használni.

### Kötegelt mód tesztelése

- Futtasson kötegelt mintamunkákat az alkalmazásból, a munkákat elküldő profilt használva.
- Teszteljen különböző jogosultsági szinteket igénylő kötegelt munkákat, úgymint információ nyomtatása, információ változtatása, fájl kitakarítása hó végén.
- Ellenőrizze a QSYSOPR üzenetsort és a QHST naplót a biztonsági hibákról. Használja a DSPLOG parancsot a QHST napló megtekintésére. A biztonsági üzenetek tartománya: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00 és CPD4A00.

Ugyancsak használhatja a biztonsági felülvizsgálati funkciót a biztonsági hibák és a biztonsággal kapcsolatos események feljegyzésére.

### Túl sok jogosultság tesztelése

Ha beállít erőforrás biztonságot a bizalmas információk védelmére, tesztelje mintaprofilokkal, hogy biztosan működik-e. Jelentkezzen be olyan profillal, melynek nem lenne szabad a titkos információt hordozó fájlt elérni.

- Van olyan menü, amely engedi a fájl elérését?
- Mi történik, ha olyan opciót választ ki, mely használja a fájlt?
- Elér parancsot?
- Tud-e futtatni olyan parancsot, amely kilistázza a fájlt: `CPYF FROMFILE(fájl-neve) TOFILE(QSYSVRT)?`
- Meg tudja-e a fájlt Query eszközzel tekinteni?

A tesztelési eredmények jelezhetik azt, hogy módosítani kell a biztonsági információkat.

---

## Biztonsági információk módosítása

Most, hogy teljesen megtervezte a rendszer biztonságát, feltétlenül ügyeljen arra, hogy fennmaradjon a terv hatékonysága a rendszer bővülésével és az üzleti igények változásával együtt.



A témakör kihangsúlyozta az egyszerűséget, mint lényeges célt a biztonság tervezésében. Felhasználói csoportokat tervezett, amelyek az egyedi felhasználók mintájául szolgáltak. Megpróbálta használni inkább a nyilvános jogosultságot, jogosultsági listákat, könyvtárjogosultságot, mintsem egyedi jogosultságokat adni. Használja ezt az előnyös megközelítést a biztonság felügyelete során is:

- Mikor új felhasználói csoportot vagy új alkalmazást ad a rendszerhez, használja a tervezés során megismert technikákat.
- Mikor valamit módosítani kell a biztonság vonatkozásában, próbáljon inkább az általános szempontból közelíteni, mintsem kivételt létrehozni az egyedi probléma megoldására.

A Biztonsági parancsok című rész elmagyarázza, hogy milyen parancsokat használhat a biztonsági információ megjelenítésére, változtatására és törlésére.

Olvassa el az alábbiakat a különböző változtatásokkal kapcsolatos javaslatok és információk megismeréséért:

- Új felhasználó hozzáadása a rendszerhez.
- Új felhasználói csoport létrehozása.
- Felhasználói csoport módosítása.
- Új alkalmazás hozzáadása.
- Új munkaállomás hozzáadása.
- Felhasználói felelősség módosítása.
- Felhasználó eltávolítása a rendszerből.

## Biztonsági parancsok

Az alábbi táblázat mutatja azokat a parancsokat, amelyek segítségével dolgozhat a biztonsági objektumokkal. A parancsokkal a következő feladatokat hajthatja végre:

- Biztonsági információk megtekintése és listázása.
- Biztonsági információk módosítása.
- Biztonsági információk törlése.

63. táblázat: Biztonsági parancsok

Bizt. objektum	Megjelenítés	Változtatás	Törlés
Rendszerváltozó	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Nem törölhető
Jobleírás	WRKJOBID DSPJOBID	WRKJOBID CHGJOBID	DLTJOBID
Csoportprofil	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF <sup>1, 2</sup>
Felhasználói profil	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF <sup>1</sup>
Objektum jogosultságok	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
Objektum tulajdonjog	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN megengedi az előző tulajdonos jogainak visszavételét.
Elsődleges csoport	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP beállítja az elsődleges csoportot *NONE értékre

63. táblázat: Biztonsági parancsok (Folytatás)

Bizt. objektum	Megjelenítés	Változtatás	Törlés
Objektum felülvizsgálat	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (*NONE beállítva) CHGAUD
Jogosultsági lista	DSPAUTL DSPAUTLOBJ	EDTAUTL (felh. jogosultság a listához) EDTOBJAUT (objektum védelem listával) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (teljes lista) <sup>3</sup> RMVAUTLE (felh. jog. elvétele a listától) EDTOBJAUT (objektum védelem listával) RVKOBJAUT

1. Az IBM a Work with User Enrollment képernyő eltávolítás opcióját ajánlja a profil törléséhez. Az opcióval törölheti a profil által birtokolt bármely objektumot, vagy új tulajdonoshoz rendelheti. A DLTUSRPRF parancs bizonyos paramétereivel törölheti a felhasználó összes objektumát, vagy új tulajdonoshoz rendelheti. Nem törölheti a profilt, míg nem törölte, vagy nem rendelte más tulajdonába a profil birtokolta objektumokat. Ugyancsak nem törölheti a profilt, ha az elsődleges csoport egy objektumra.
2. Addig nem törölhet csoportprofil, míg van tagja. A DSPUSRPRF parancs \*GRPMBR opciója listázza ki a csoport tagjait. Változtassa meg a *group profile* mezőt minden egyedi profilban, mielőtt törli a csoportprofil.
3. Jogosultsági listát nem törölhet addig, amíg véd objektumot. A DSPAUTLOBJ parancsral kaphat riportot azokról az objektumokról, amelyeket a lista véd. A listával védett bármely objektum jogosultságát módosíthatja az EDTOBJAUT parancsral.

## Biztonsági információ megtekintése és listázása

A biztonsági információt kilistáztathatja a Display (DSP) parancs (\*PRINT) opciójával. Például, a MYLIST nevű jogosultsági lista megjelenítéséhez gépelje be a DSPAUTL MYLIST \*PRINT parancsot.

Egyes képernyő parancsok biztosítanak opciókat különböző típusú listák nyomtatásához. Például, amikor egyedi felhasználói profilekat képzett, a DSPUSRPRF parancs \*GRPMBR opciójával listázta ki a csoportprofil összes tagját. Használja az **F4** (Prompt) billentyűt és az online súgót a biztonsági objektumok lehetséges listázási módjainak megtalálásához.

A Display parancsok segítségével megjelenítheti a biztonsági információkat a képernyőn. Ugyancsak használhatja a Work with... (WRK) parancsokat is erre a célra, amelyek több funkciót adnak. A Work with... parancsok lista-képernyőt biztosítanak. Az információ megváltoztatásához, törléséhez, megtekintéséhez használhatja az ilyen képernyőt.

Amikor biztonsági parancsokkal jelenít meg vagy nyomtat ki információkat, általános nevet is használhat. Ha begépel a WRKUSRPRF DPT\* parancsot a Work with User Enrollment vagy a Work with User Profile képernyőn, csak a DPT betűkkel kezdődő profilek fognak megjelenni. Az adott parancs online súgója nyújt segítséget ahhoz, hogy megtudja melyik paraméterére adhat általános nevet.

## Biztonsági információk módosítása

Módosíthatja a biztonsági információkat interaktív módon a Work with... (WRK) vagy az Edit... (EDT) parancsokkal. Megtekintheti az információt, megváltoztathatja azt, illetve újra megtekintheti a változtatás után.

Úgy is megváltoztathatja a biztonsági információt, hogy sem előtte, sem utána nem tekinti meg, ha a Change... (CHG) vagy a Grant... (GRT) parancsokat használja. Ez az eljárás különösen hasznos, ha egyszerre több objektumot módosít. Például, a GRTOBJAUT parancsot használta, amikor beállította a könyvtár összes objektumának nyilvános jogosultságát ("Nyilvános jogosultság beállítása a könyvtár összes objektumára" oldalszám: 94).

## Biztonsági információ törlése

Bizonyos biztonsági információt törölhet vagy eltávolíthat interaktív módon a Work with... (WRK) vagy az Edit... (EDT) parancsokkal. Használhatja a Delete... (DLT), Remove... (RMV), és Revoke... (RVK) parancsokat is biztonsági

információ törléséhez. Gyakran, bizonyos feltételeknek meg kell felelni ahhoz, hogy a rendszer engedje a törlési műveletet. A Biztonsági parancsok című részben lévő megjegyzések leírnak néhány ilyen feltételt.

## Új felhasználó hozzáadása a rendszerhez

Ha új felhasználót kell a rendszerhez adnia, kövesse a következő eljárást:

1. Rendelje a személyt egy felhasználói csoporthoz. Használja a Felhasználói csoportot leíró űrlapot referenciaként.
2. Döntse el, kell-e rendszerfunkciókat végrehajtani az új felhasználónak vagy sem. Ha igen, rögzítse az erre vonatkozó információkat a Rendszerfelelősségek űrlapján.
3. Vegye fel a személy adatait az Egyedi felhasználói profil űrlapján.
4. Nézze át a Rendszerfelelősségek űrlapját és a Felhasználói csoportot leíró űrlapot annak megállapítására, hogy szükséges-e a csoporttól eltérő jogosultságot adni az új felhasználónak.
5. Hozzon létre egyedi profilt a csoportprofil másolásával vagy csoporttag profilt. Győződjön meg róla, hogy a jelszót lejárt állapotba állította. (Lásd a "Csoportprofil másolása" című részt.)
6. Adjon a biztonsági feljegyzéséből másolatot az új felhasználónak.

Az új felhasználói csoport létrehozását az "Új felhasználói csoport létrehozása" című részben tanulmányozhatja.

## Új felhasználói csoport létrehozása

Több okból is szükségessé válhat új csoport létrehozása:

- További osztályoknak kell a rendszert használni.
- Rájöhet, hogy pontosabban megadott csoportokat kell létrehozni az erőforrás biztonsági elvárások kielégítése érdekében.
- A vállalat átszervezte néhány részlegét.

Új felhasználói csoport létrehozásához tegye a következőket:

1. A "Felhasználói csoportok tervezése" című részben található utasítások alapján töltsé ki a Csoportot leíró űrlapot.
2. Adja hozzá a csoportot a Csoportok, alkalmazások, könyvtárak diagramjához.
3. Értékelje ki, vajon kell-e végrehajtania rendszerfunkciót valamelyik csoporttagnak. Frissítse a Rendszerfelelősségek űrlapját. (Olvassa el a "Rendszerfunkciókért felelősök meghatározása" című részben leírtakat.)
4. Az Egyedi felhasználói profil űrlapjának kitöltéséhez használja fel a Felhasználói csoportot leíró űrlap és a Rendszerfelelősségek űrlap információit.
5. Hozzon létre egy csoportkönyvtárat.
6. Hozzon létre egy jobleírást a csoportnak.
7. Hozzon létre egy csoportprofil.

**Megjegyzés:** Az ötödik, hatodik és hetedik lépések végrehajtásáról szóló utasítások a "Felhasználói csoportok beállítása" című részben találhatók.

8. Hozzon létre egyedi profilokat a csoporttagoknak. (Lásd az "Egyedi felhasználók beállítása" című részt.)
9. Értékelje ki a Könyvtárat leíró űrlapokat, amelyeket a csoport számára szükséges alkalmazásokhoz töltött ki. Tegye meg a csoport által használandó alkalmazások objektumainak eléréséhez szükséges lépéseket, felhasználva az Erőforrás biztonság beállítása című részben ismertetett technikákat.
10. Adjon a csoport minden tagjának egy másolatot a biztonsági feljegyzéséből.

A felhasználói csoport módosítását a "Felhasználói csoport módosítása" című részben tanulmányozhatja.

## Felhasználói csoport módosítása

Eltérő módokon kell kezelnie a csoport jellemzőinek különböző módosításait. Kövessen végig néhány példát és megoldást:

## Csoportjogosultság módosítása

Észreveheti, hogy egy csoportnak jogosultságot kell adni egy objektumhoz, amit nem vett figyelembe a kezdeti tervben. Tegye a következőket:

1. Az Edit Object Authority (EDTOBJAUT) parancs segítségével megfelelő jogosultságot adhat a csoportnak az objektumokhoz vagy a megfelelő jogosultsági listához. Az "Egyedi jogosultságok beállítása" oldalszám: 98 mutat be példát ennek végrehajtására. A csoport minden tagja megkapja a jogosultságot a csoportjogosultság megadásakor.
2. Ha csoportjogosultságot ad egy bizalmas erőforráshoz, ellenőrizheti, hogy kik a csoport pillanatnyi tagjai. Használja a Display User Profile parancsot (DSPUSRPRF *csoportprofil neve* \*GRPMBR) a csoporttagok kilistázásához.

## Csoport egyéniesítésének módosítása

Szükség lehet a csoporttagok felhasználói környezetének módosítására. Például, ha az osztály saját nyomtatót kap, az új nyomtató lesz az osztály dolgozóinak (felhasználói csoport tagjainak) alapértelmezett nyomtatója. Vagy, amikor új alkalmazással bővül a rendszer, a csoport tagjai esetleg különböző kezdeti menüt kívánnak látni bejelentkezéskor.

A csoportprofil mintaként szolgál a csoporttagok egyedi profiljainak létrehozásához. Azonban, a csoportprofil egyéniesítése nincs hatással az egyedi profilokra, ha azokat már korábban létrehozta. Például, ha megváltoztatja a *Printer device* mezőt a csoportprofilban, ez nincs hatással a csoport tagjaira. Meg kell változtatnia a *Printer device* mezőt mindegyik egyedi felhasználói profilban.

Használhatja a Work with User Profile képernyőt, ha egyszerre több felhasználónak akarja egy paraméterét megváltoztatni. A példa kimeneti sor megváltoztatását mutatja be egy csoport minden tagjára:

1. Gépelje be a WRKUSRPRF \*ALL parancsot, és nyomja meg az **Enter** billentyűt.
2. Ha látja a Work with User Enrollment képernyőt, nyomja meg az **F21** (Select assistance level) billentyűt, hogy megváltozzon a Work with User Profile képernyő.

```
Work with User Profiles

Type options, press Enter.
 1=Create  2=Change  3=Copy  4=Delete  5=Display
12=Work with objects by owner

Opt      User Profile      Text
-----
2         HARRISOK         Harrison, Keith
          HOGANR          Hogan, Richard
          JONESS          Jones, Sharon
2         WILLISR         Willis, Rose
          :
                                     More...

Parameters for options 1, 2, 3, 4 and 5 or command
====> PRTDEV(PRT02)
F3=Exit  F5=Refresh  F12=Cancel  F16=Repeat position to  F17=Position to
F21=Select assistance level  F24=More keys
```

3. Gépeljen be **2** (Change) értéket minden módosítani kívánt profil mellé.
4. A paraméter sorban a képernyő alján adja meg a paraméter nevét és az új értéket. Ha nem tudja a paraméter nevét, nyomja meg az **F4** (Prompt) billentyűt.
5. Nyomja meg az **Enter** billentyűt. Megerősítő üzenetet kap minden módosított profilra.  
Ugyan a csoportprofil egyéniesítő mezőinek változása nincs hatással az egyedi tagokra, mégis segíti Önt a jövőben. A csoportprofil mintául szolgál, amikor új tagot vesz fel később a csoportba. Továbbá, a csoport szabványos mezőin lévő értékek egyfajta rögzítését is jelenti.

## Csoportelérés megadása új alkalmazáshoz

Amikor elérést kell biztosítani egy csoportnak az új alkalmazáshoz, elemeznie kell a csoportról és az alkalmazásról meglévő információkat. Következő eljárás a javasolt:

1. Nézze meg az új alkalmazásra vonatkozó Alkalmazást leíró űrlapot és a Csoportok, alkalmazások, könyvtárak diagramját, hogy az alkalmazás mely könyvtárakat használja. Vezesse fel a könyvtárakat a Felhasználói csoportot leíró űrlapra.
2. Frissítse fel a Csoportok, alkalmazások, könyvtárak diagramját, bemutatva a csoport és az alkalmazás között létrejövő új kapcsolatokat.
3. Ha a könyvtáraknak a csoport kezdeti könyvtárlistájában kell lenni, módosítsa a csoport jobbleírását a Change Job Description (CHGJOB) paranccsal. Olvassa el a "Jobleírás létrehozása" oldalszám: 81 részben leírtakat, ha segítségre van szüksége a jobleírások kezeléséhez.

**Megjegyzés:** Amikor hozzáad könyvtárakat a kezdeti könyvtárlistához a jobleírásban, a jobleírást használó felhasználói profilban semmilyen változtatásra nincs szükség. Amikor a felhasználó következő alkalommal bejelentkezik, a könyvtárak automatikusan felkerülnek a kezdeti könyvtárlistára.

4. Értékelje ki, vajon a kezdeti programot vagy a kezdeti menüt kell megváltoztatnia a csoport részére az új alkalmazás használatához. Minden egyes felhasználói profilban egyedileg kell megváltoztatnia a kezdeti menüt vagy a programot a CHGUSRPRF parancs segítségével.
5. Nézze át a Könyvtár leíró űrlapokon az alkalmazások által használt könyvtárakat. Döntse el, hogy a könyvtáraknál rendelkezésre álló nyilvános hozzáférés elegendő-e a csoport igényeinek kielégítésére. Ha nem, adjon csoportjogosultságot a könyvtárhoz, bizonyos objektumokhoz, vagy jogosultsági listákhoz. Használja az Edit Object Authority (EDTOBJAUT) és az Edit Authorization List (EDTAUTL) parancsokat a végrehajtáshoz. (Ha további információra lenne szüksége, olvassa el az "Erőforrás biztonság beállítása" című részt.)

Ha új alkalmazással bővíti rendszerét, olvassa el a "Bővítés új alkalmazással" című részt.

## Bővítés új alkalmazással

Minden új alkalmazásra ugyanúgy meg kell tervezni a biztonságot, mint amilyen óvatosan tette ezt az eredeti alkalmazásoknál. Kövesse ugyanazt az eljárást:

1. Készítse el az új alkalmazásra vonatkozó Alkalmazást leíró űrlapot és Könyvtár leíró űrlapokat.
2. Frissítse fel a Csoportok, alkalmazások, könyvtárak diagramját.
3. Kövesse az "Erőforrás biztonság tervezése" című részben leírt eljárásokat, és döntse el, hogyan védi az új alkalmazást.
4. Készítse el az Alkalmazás telepítési űrlapot az "Alkalmazások telepítésének tervezése" című részben leírt módszer szerint.
5. Értékelje ki, vajon van-e az alkalmazásnak védelmet igénylő, bizalmas információt hordozó nyomtatott listája. Módosítsa a Kimeneti sor és munkaállomás biztonság űrlapját, ha szükséges.
6. Kövesse a "Tulajdonjog és nyilvános jogosultság beállítása" és az "Erőforrás biztonság beállítása" című részekben leírt lépéseket az alkalmazás telepítéséhez és biztonságossá tételéhez.

Ha új munkaállomással bővíti rendszerét, olvassa el a "Bővítés új munkaállomással" című részt.

## Bővítés új munkaállomással

Mikor új munkaállomással bővíti a rendszert, legyen tekintettel a biztonsági követelményekre:

1. Az új munkaállomás elhelyezése jár-e biztonsági kockázattal? (Olvassa el a "Fizikai biztonság tervezése" című részt, hogy felfrissítse emlékezetét.)
2. Ha a munkaállomás biztonsági kockázatot hordoz, módosítsa a Kimeneti sor és munkaállomás biztonság űrlapját.
3. Amikor létrehoz egy új munkaállomást, rendszerint \*CHANGE nyilvános jogosultsággal teszi ezt. Ha ez nem felel meg a biztonsági igényeknek az adott munkaállomáson, használja az EDTOBJAUT parancsot az eltérő jogosultság megadásához.

Olvassa el a "Felhasználói felelősségek módosítása" című részt, ha felhasználói felelősséget kíván módosítani.

## Felhasználói felelősségek módosítása

Mikor egy felhasználó új munkát, vagy új felelősségeket kap a vállalatnál, meg kell vizsgálnia, milyen hatással van ez a felhasználói profilra.

1. Másik csoporthoz kell rendelni őt? Használhatja a CHGUSRPRF parancsot a csoport módosításához.
2. Valamilyen egyéniesítési jellemzőt kell a profilban módosítani, mint például nyomtatót vagy kezdeti menüt? Használhatja a CHGUSRPRF parancsot ezekhez a módosításokhoz is.
3. Az új csoport jogosultsága az alkalmazáshoz megfelelő ennek a személynek?
  - Használhatja a Display User Profile (DSPUSRPRF) parancsot a régi- és új csoportprofil jogosultságainak megjelenítéséhez.
  - Nézze meg az egyedi felhasználói profil jogosultságait is.
  - Ha szükséges, változtasson az EDTOBJAUT parancssal.
4. Birtokol a felhasználó objektumot? Meg kell változtatni az objektumok tulajdonjogát? Használja a Work with Objects by Owner (WRKOBJOWN) parancsot.
5. Végez rendszerfunkciókat a felhasználó? Az új munkakörében kell végeznie rendszerfunkciókat? Módosítsa a Rendszerfelelősségek űrlapját, és módosítsa a felhasználói profilt, ha szükséges.

Olvassa el a "Felhasználó eltávolítása a rendszerből" című részt, ha kíváncsi ennek folyamatára.

## Felhasználó eltávolítása a rendszerből

Ha valaki elhagyja a vállalatot, a felhasználói profilját azonnal el kell távolítani a rendszerből. Mielőtt a profilt törölné, az általa birtokolt objektumokat vagy máshoz kell rendelni, vagy törölni kell. Ehhez használhatja a WRKOBJOWN parancsot, vagy a **4** (Remove) opciót a Work with User Enrollment képernyőn.

Ha a **4** (Remove) opciót használja a Work with User Enrollment képernyőn a profil eltávolítására, további képernyőket lát, amelyek lehetőséget adnak a profil birtokolta objektumok kezelésére. Választhat, hogy az összes objektumot új felhasználónak adja, vagy egyedileg kezeli őket:

```
Remove User
User . . . . . : HOGANR
User description . . . . . : Sales and Marketing Department

To remove this user type a choice below, then press Enter.

1. Give all objects owned by this user to a new owner
2. Delete or change owner of specific objects owned by this user.
```

Ha az objektumok egyedi kezelését választja (**2** opció), a képernyő a felhasználó birtokában lévő összes objektumot felsorolja:

```
Remove User
User . . . . . : HOGANR
User description . . . . . : Sales and Marketing Department
New owner . . . . . Name, F4 for list
To remove this user, delete or change owner of all objects.
Type options below and press Enter.
  2=Change to new owner  4=Delete  5=Display details
Opt Object      Library      Description
  4 HOGANR      QUSRSYS    Hogan, Richard message queue
  4 QUERY1     DPTWH      Inventory Query
```

Ha az objektumok törlését választja a Confirm Delete képernyőt látja. Amint a rendszer törli az objektumokat, eltávolíthatja a felhasználói profilt. Utána ismét a Work with User Enrollment képernyőt fogja látni, a felhasználó eltávolításáról szóló rendszerüzenettel.

## Biztonsági információk mentése

Ez a rész áttekintést nyújt a biztonsági információk tárolásáról és visszatöltéséről. Mikor a rendszer mentését és visszaállítását tervezi, figyelembe kell venni, hogy a biztonsági információ ugyanolyan fontos, mint maga az információ. Olvassa el az Információs központ Mentés, helyreállítás és rendelkezésre állás című témakörét, ami segítséget nyújt a teljeskörű mentési és helyreállítási terv kidolgozásához.

A következő témakörök ismertetik a biztonság beállítása során előállt biztonsági adatok mentését és visszatöltését:

- Rendszerváltozók mentése.
- Csoport- és felhasználói profilok mentése.
- Joleírások mentése.
- Erőforrás biztonsági információk mentése.
- Alapértelmezett tulajdonosi profil (QDFTOWN) használata.
- Visszaállítás sérült jogosultsági listából.

## Rendszerváltozók mentése

A rendszerváltozók tárolása a QSYS rendszerkönyvtárban történik. Menti a QSYS könyvtárat, amikor az alábbiakat csinálja:

- Használja a Save System (SAVSYS) parancsot.
- Használja a Save menü Egész rendszer tárolása opcióját.
- Használja a Save menü Rendszerinformáció tárolása opcióját.
- Használja az Egész rendszer mentése opciót a Run Backup (RUNBCKUP) menüből.

Ha visszaállítja az egész rendszert, a rendszerváltozók automatikusan visszatöltésre kerülnek az operációs rendszerrel.

Következő terület a "Csoport- és felhasználói profilok mentése".

## Csoport- és felhasználói profilok mentése

A csoport- és a felhasználói profilok a QSYS könyvtárban vannak. Akkor menti őket, amikor a Save System (SAVSYS) parancsot használja, vagy ha kiválasztotta az Egész rendszer tárolása opciót.

Ugyancsak eltávolíthatja a profilokat a Save Security Data (SAVSECDDTA) parancs használatával.

A profilok visszatöltésére használhatja a Restore User Profile (RSTUSRPRF) parancsot. A műveletek sorrendje:

1. Az operációs rendszer visszatöltése, ami visszatölti a QSYS könyvtárat.

2. Felhasználói profilok visszatöltése.
3. Maradék könyvtárak visszatöltése.
4. Objektumok jogosultságainak visszatöltése a Restore Authority (RSTAUT) paranccsal.

Következő témakör a "Jobleírások mentése".

## Jobleírások mentése

Mikor egy jobleírást létrehoz, megadja annak a könyvtárnak a nevét, ahol található. Az IBM azt ajánlja, hogy a jobleírásokat a QGPL könyvtárban helyezze el.

A jobleírásokat elmentheti úgy, hogy az őket tartalmazó könyvtárakat menti el. Ehhez használja a Save Library (SAVLIB) parancsot. Ugyancsak elmentheti őket a Save Object (SAVOBJ) paranccsal.

A könyvtár tartalmát a Restore Library (RSTLIB) paranccsal töltheti vissza. Egyedi jobleírást a Restore Object (RSTOBJ) paranccsal tölthet be.

Következő témakör az "Erőforrás biztonsági információk mentése".

## Erőforrás biztonsági információk mentése

Az erőforrás biztonság, ami meghatározza, hogyan tudnak a felhasználók az objektumokkal dolgozni, különböző típusú információkból áll, amelyek különböző helyen vannak:

64. táblázat: Erőforrás biztonsági információk mentése és visszatöltése

Információ típusa	Tárolási helye	Tárolási módja	Visszatöltési módja
Nyilvános jogosultság	Objektummal együtt	SAVxxx parancs <sup>1</sup>	RSTxxx parancs <sup>2</sup>
Objektum felülvizsgálat	Objektummal együtt	SAVxxx parancs <sup>1</sup>	RSTxxx parancs <sup>2</sup>
Objektum tulajdonjog	Objektummal együtt	SAVxxx parancs <sup>1</sup>	RSTxxx parancs <sup>2</sup>
Elsődleges csoport	Objektummal együtt	SAVxxx parancs <sup>1</sup>	RSTxxx parancs <sup>2</sup>
Jogosultsági lista	QSYS könyvtár	SAVSYS vagy SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
Objektum és jogosultsági lista kapcsolata	Objektummal együtt	SAVxxx parancs <sup>1</sup>	RSTxxx parancs <sup>2</sup>
Magánjogosultság	Felhasználói profillal	SAVSYS vagy SAVSECDTA	RSTAUT

1. Az objektumok többsége elmenthető a SAVOBJ vagy SAVLIB parancsokkal. Csupán néhány típusú objektum (például konfiguráció) menthető speciális parancsokkal.
2. Az objektumok többsége betölthető a RSTOBJ vagy RSTLIB parancsokkal. Néhány típusú objektum (például a konfigurációk) csak speciális parancsokkal tölthetők be.

Amikor az alkalmazást vagy az egész rendszert kell visszaállítani, a lépéseket óvatosan meg kell terveznie, beleértve az objektumokhoz való jogosultságok helyreállítását is. A következő alapvető lépéseket kell megtenni, amikor egy alkalmazásra vonatkozó erőforrás biztonsági információkat akar visszaállítani:

1. Ha szükséges, töltsse vissza a felhasználói profilekat, beleértve az alkalmazást birtokló profilt is. A profilekat (egyedi vagy összes) a RSTUSRPRF paranccsal töltheti be.
2. Töltsse be az alkalmazás által használt jogosultsági listákat. Visszatölti a jogosultsági listákat, ha a RSTUSRPRF USRPRF(\*ALL) parancsot használja.

**Megjegyzés:** Ez visszatölti a felhasználói profil összes értékét a mentési médiáról, beleértve a jelszavakat is.

3. Töltsse vissza az alkalmazási könyvtárakat a RSTLIB vagy a RSTOBJ parancsokkal. Ez visszaállítja az objektumok tulajdonjogait, a nyilvános jogosultságokat, az objektumok és a jogosultsági listák közötti kapcsolatokat.
4. Töltsse vissza az objektumokra vonatkozó magánjogosultságokat a RSTAUT paranccsal. A RSTAUT parancs visszatölti a jogosultsági listákra érvényes felhasználói jogosultságokat is. Visszatöltheti a jogosultságokat csak bizonyos- vagy minden felhasználó számára.



Olvassa el az "Alapértelmezett tulajdonosi profil (QDFTOWN) használata" című részt, ha nem a rendszerén lévő objektumot és tulajdonosi profilt tölt vissza.

## Alapértelmezett tulajdonosi profil (QDFTOWN) használata

Ha visszatölt egy objektumot, és a tulajdonosi profil nincs a rendszerben, a rendszer átadja az objektum tulajdonjogát a QDFTOWN nevű alapértelmezett tulajdonosi profilnak. Ha egyszer visszatölti az eredeti tulajdonosi profilt vagy újra létrehozza, visszaadhatja az objektum tulajdonjogát a Work with Object by Owner (WRKOBJOWN) paranccsal.

Olvassa el a "Visszaállítás sérült jogosultsági listából" című részt, ha tájékozódni kíván a jogosultsági lista helyreállításáról.

## Visszaállítás sérült jogosultsági listából

Amikor jogosultsági lista véd egy objektumot, és a lista megsérül, csak azok a felhasználók érhetik el az objektumot, akik \*ALLOBJ jogosultsággal rendelkeznek.

A sérült jogosultsági lista helyreállítása két lépést igényel:

1. A felhasználók és jogosultságaik helyreállítása a listán.
2. A lista és az objektumok kapcsolatának helyreállítása.

\*ALLOBJ különleges jogosultsággal rendelkező felhasználó hajthatja végre ezeket a lépéseket.

### 1. lépés: Jogosultsági lista helyreállítása

Ha tudja a felhasználók jogosultságát a listához, törölje a listát, hozza létre újra és adja hozzá a felhasználókat.

Ha nem ismeri az összes felhasználói jogosultságot a listához, töltse vissza az utolsó SAVSYS vagy SAVSECDTA szalagokat a következő lépésekkel:

1. Törölje a sérült jogosultsági listát:  
DLTAUTL AUTL(*jogosultsági lista neve*)
2. Töltse vissza a jogosultsági listát:  
RSTUSRPRF USRPRF(\*ALL)
3. Rendelje a felhasználókat a jogosultsági listához a Restore Authority (RSTAUT) paranccsal.

### 2. lépés: Objektumok listához társításának helyreállítása

Mikor betöltötte vagy létrehozta újra a jogosultsági listát, létre kell hoznia a kapcsolatot a lista és az általa védendő objektumok között:

1. Használja a Reclaim Storage (RCLSTG) parancsot. Az RCLSTG parancs hozzárendeli a sérült vagy hiányzó listával védett objektumokat az alapértelmezett QRCLAUTL nevű listához.
2. Nyomtassa ki a QRCLAUTL listával védett objektumok listáját:  
DSPAUTLOBJ AUTL(QRCLAUTL)
3. A GRTOBJAUT paranccsal a megfelelő jogosultsági listához rendelheti az objektumokat. Például, ha a CUSTLIB könyvtárban lévő ARWRK01 fájl az ARLST01 jogosultsági listával kívánja védeni, gépelje be az alábbi parancsot:  
GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(\*FILE) +  
AUTL(ARLST01)

---

## Biztonság figyelése

Ez a rész alapelveket javasol a rendszerbiztonság hatékonyságának figyelésére.

A biztonság figyelésének alapvetően két célja van:

- Ellenőrizni, hogy megfelelően védi-e a vállalat erőforrásait.
- Észrevenni, ha a vállalat információihoz és a rendszerhez jogosulatlanok akartak hozzáférni.

Vizsgálja felül a biztonsági szabályzatot és a feljegyzést, amint eldöntötte, milyen figyelési tevékenységeket kell szabályozottan végrehajtani.

A biztonság figyeléséről további információkat kaphat az alábbi témakörökben:

- Biztonság figyelésének ellenőrzőlistája
- Biztonság ellenőrzése.

## Biztonság figyelésének ellenőrzőlistája

A rendszerbiztonság különböző aspektusai áttekintésére javasoljuk az alábbi ellenőrzőlistákat. Használja a terv elkészítésekor.

### Fizikai biztonság figyelése

- Védje meg a mentési adathordozót a sérüléstől és lopástól.
- Korlátozza a nyilvános helyen lévő munkaállomások elérhetőségét. Használja a DSPOBJAUT parancsot annak megnevezéséhez, hogy ki rendelkezik \*CHANGE jogosultsággal a munkaállomásokhoz.

### Rendszerváltozók figyelése

- Ellenőrizze hogy az értékek megegyeznek-e a Rendszerváltozók kiválasztására szolgáló űrlapon megadott értékekkel. Ehhez használja a Print System Security Attributes (PRTSYSSECA) parancsot.
- Vizsgálja felül döntéseit a rendszerváltozókról, különösen, ha új alkalmazást telepít.

### Csoportprofilok figyelése

- Ellenőrizze, hogy a csoportprofiloknak valóban ne legyen jelszavuk. Ellenőrizze a DSPAUTUSR paranccsal, hogy az összes csoportprofil \*NONE beállítással rendelkezik a jelszóra.
- Ellenőrizze, hogy megfelelő emberek a csoport tagjai. A csoport tagjainak kilitázásához használja a DSPUSRPRF parancsot \*GRPMBR opcióval.
- Ellenőrizze a különleges jogosultságokat minden csoportprofilnál. Ehhez használja a DSPUSRPRF parancsot. Ha 30-as, 40-es vagy 50-es biztonsági szinttel dolgozik, a csoportprofiloknak nem szabad \*ALLOBJ jogosultsággal rendelkezniük.

### Felhasználói profilok figyelése

- Ellenőrizze, hogy a felhasználói profilok az alábbi kategóriák egyikéhez tartoznak-e:
  - Jelenlegi felhasználók profilja
  - Csoportprofilok
  - Alkalmazás tulajdonosi profilok
  - IBM szolgáltatott profilok (Q-val kezdődők)
- Ha a felhasználót áthelyezi a vállalat, vagy ha a felhasználó elhagyja a vállalatot, távolítsa el a profilját. A Change Expiration Schedule Entry (CHGEXPSCDE) paranccsal automatikusan törölheti vagy letilthatja a profilt, amint a felhasználó eltávozott.
- Nézze meg a nem aktív profilokat és távolítsa el. Használja az Analyze Profile Activity (ANZPRFACT) parancsot, amely letiltja a bizonyos időn túl inaktív profilokat.

- Határozza meg, hogy melyik felhasználó használ profilnevével azonos jelszót. Ehhez használja az Analyze Default Passwords (ANZDFTPWD) parancsot. A parancs megfelelő opciójának használatával arra kényszerítheti a felhasználót, hogy változtassa meg jelszavát a következő bejelentkezéskor.

**Figyelem!** Ne távolítson el egyetlen IBM szolgáltatott profilt sem a rendszerből. Az IBM szolgáltatott profilek Q-val kezdődnek.

- Figyeljen oda ki van \*USER felhasználói osztálytól eltérő osztályban és miért. Használja a Print User Profile (PRTUSRPRF) parancsot, amellyel kilistáztathatja az összes felhasználót, felhasználói osztályukat és speciális jogosultságukat. A listának egyeznie kell a Rendszerfelelősségek űrlapján megadottakkal.
- Ellenőrizze, melyik profileknak van a *Korlátolt képességek* mezője \*NO értékre állítva.

### Fontos objektumok figyelése

- Vizsgálja felül, kinek van hozzáférése a fontos objektumokhoz. Használja a Print Private Authorities (PRTPVTAUT) és a Print Publicly Authorized Objects (PRTPUBAUT) parancsokat az objektumok figyeléséhez. Ha egy csoportnak van elérési joga, ellenőrizze a csoporttagokat a DSPUSRPRF parancs \*GRPMBR opciójával.
- Ellenőrizze, kik használják azokat az alkalmazási programokat, amelyek elérést biztosítanak bizonyos objektumokhoz más (például örökölt) biztonsági rendszeren keresztül. Ehhez használja a Print Adopting Objects (PRTADPOBJ) parancsot.

### Jogosulatlan elérések figyelése

- Utasítsa a rendszeroperátorokat, hogy haladéktalanul jelezzék, ha jogosulatlan elérésről szóló biztonsági üzenetet kapnak a QSYSOPR üzenetsorban. Különösen akkor jelezzék a biztonsági felelősnek, ha a sikertelen elérési kísérletről szóló üzenet ismétlődik. A biztonsági üzenetek tartománya 2200 - 22FF és 4A00 - 4AFF. Előazonosítójuk CPF, CPI, CPC és CPD.
- Állítsa be a biztonsági ellenőrzést az objektumok jogosulatlan elérésének naplózására.

Következő témakör a Biztonság ellenőrzése.

## Biztonság ellenőrzése

Amikor figyel a biztonságot, az operációs rendszer képes a rendszeren előforduló, bármely biztonsági esemény naplózására. A rendszer speciális rendszerobjektumokban, az úgynevezett **naplófogadókban** rögzíti az eseményeket. Beállíthatja a naplófogadókat különböző típusú biztonsági események rögzítésére, úgymint rendszerváltozó vagy profil változása, objektum jogosulatlan elérésének sikertelen kísérlete. A következő értékek vezérlik a rögzítésre kerülő események típusát:

- Audit control (QAUDCTL) rendszerváltozó
- Audit level (QAUDLVL) rendszerváltozó
- Audit level (AUDLVL) érték a felhasználói profilban
- Object auditing (OBJAUD) érték a felhasználói profilban
- Object auditing (OBJAUD) érték az objektumban

Az ellenőrzési naplóban lévő információ felhasználható:

- A biztonság megsértési kísérleteinek feltárására.
- Magasabb biztonsági szint tervezéséhez.
- Az érzékeny objektumok használatának figyelésére (mint például a bizalmas információt hordozó fájlok).

Több parancssal és különböző módokon tekintheti meg az ellenőrzési naplók információit.

---

## Alapvető rendszerbiztonság tervezési űrlapjai

Az űrlapokat a böngészőből másolhatja vagy nyomtathatja.

Ha a teljes dokumentációt akarja kinyomtatni, válassza a jobboldali keretet, majd kattintson a PDF ikonra az Információs központ fejlécén.

Ha csak egyetlen tervezési űrlapot kíván kinyomtatni, kattintson a nyomtatandó űrlaphoz tartozó hivatkozásra. Kattintson a jobboldali keretre, majd a böngésző Nyomtatás ikonjára. Így kézhez kapja a kinyomtatott űrlapot.

Az alapvető rendszerbiztonság tervezéséhez és alkalmazásához szükséges űrlapok teljes listája látható itt:

- Fizikai biztonság tervezési űrlap
- Alkalmazást leíró űrlap
- Elnevezési szabályok űrlap
- Könyvtárat leíró űrlap
- Rendszerváltozók kiválasztására szolgáló űrlap
- Rendszerfelelősségek űrlap
- Felhasználói csoportot azonosító űrlap
- Felhasználói csoportot leíró űrlap
- Egyedi felhasználói profil űrlapja
- Jogosultsági lista űrlapja
- Kimeneti sor és munkaállomás biztonság űrlapja
- Alkalmazás telepítési űrlap

## Fizikai biztonság tervezési űrlap

65. táblázat: Fizikai biztonság tervezési űrlap

Fizikai biztonság tervezési űrlap	
Készítette:	Dátum:
<b>Utasítások</b>	
<ul style="list-style-type: none"> <li>• Az űrlapot megismerheti az "Erőforrás biztonság tervezése" című részben.</li> <li>• Az űrlap a rendszeregység és a csatolt egységek fizikai helyéből adódó biztonsági utasítások leírására szolgál.</li> <li>• A rendszerre nem kell bevinni az űrlapon lévő információkat.</li> </ul>	
<b>Rendszeregység:</b>	
A rendszeregység biztonságáról végzett vizsgálatok eredménye (például zárt terem):	
Melyik kulcsár pozíció legyen használva?	
Hol legyen a kulcs tárolva?	
További megjegyzések a rendszeregységhez:	
<b>Mentési adathordozók és dokumentációk:</b>	
Hol legyenek a mentési szalagok a munkahelyen tárolva?	
Hol legyenek a mentési szalagok távolabbi helyen tárolva?	
Hol legyenek a jelszavak (biztonsági felelős, szerviz és DST) tárolva?	
Hol legyenek a fontos rendszerdokumentumok (szériaszám, konfiguráció) tárolva?	

Fizikai biztonság tervezési űrlap	Második rész
<b>További utasítások a 2. részhez:</b>	
<ul style="list-style-type: none"> <li>• Sorolja fel az összes munkaállomást és nyomtatót, amely helye miatt biztonsági veszélyt hordoz. Jelezze, milyen védelmi vizsgálatokat fog végezni. Soroljon fel példákat bizalmas riportokra a <i>Biztonsági helyzete</i> oszlopban a nyomtatókra vonatkozóan.</li> <li>• Ha megengedte, hogy a rendszer automatikusan konfigurálja a lokális egységeket, lehet, hogy nem tudja a munkaállomások és nyomtatók neveit a rendszer telepítésének befejezéséig. Ha nem tudja a neveket az űrlap készítésekor, töltsse ki a leírásokat (úgy mint helye) és a neveket adja hozzá később.</li> </ul>	

Munkaállomások és nyomtatók fizikai biztonsága			
Munkaállomás vagy nyomtató neve	Helye vagy leírása	Biztonsági helyzete	Védelem mértéke

## Alkalmazást leíró űrlap

66. táblázat: Alkalmazást leíró űrlap

Alkalmazást leíró űrlap	
Készítette:	Dátum:
<b>Utasítások</b> <ul style="list-style-type: none"> <li>Az "Alkalmazás leírása" és az "Erőforrás biztonság tervezése" című részekben tanulmányozhatja az űrlapot.</li> <li>Minden alkalmazásra külön űrlapot készítsen elő.</li> <li>A rendszerre nem kell bevinni az űrlapon lévő információkat.</li> </ul>	
Alkalmazás neve:	Rövidítés:
Az alkalmazás rövid leírása:	
Elsődleges menü:	Könyvtár:
Kezdeti program neve:	Könyvtár:
Az alkalmazás által fájlok és programok részére használt könyvtárak listája:	
Határozza meg az alkalmazás biztonsági elemeit, vajon van-e titkos információ:	

## Elnevezési szabályok űrlap

67. táblázat: Elnevezési szabályok űrlap

Elnevezési szabályok űrlap	
Készítette:	Dátum:
<b>Utasítások</b> <ul style="list-style-type: none"> <li>Az űrlapot megismerheti az "Alkalmazások leírása" című részben.</li> <li>A rendszerre nem kell bevinni az űrlapon lévő információkat.</li> <li>Az űrlap a rendszerobjektumok elnevezési struktúrájának tervezésére és hozzárendelésére szolgál. Adjon meg példákat mindegyikre.</li> </ul>	
Objektum típusa	Elnevezési szabályok
Csoportprofilok	
Felhasználói profilok	
Jogosultsági listák	
Könyvtárak	
Fájlok	

67. táblázat: Elnevezési szabályok űrlap (Folytatás)

Naptárak	
Egységek	
Szalagok	

## Könyvtár leíró űrlap

68. táblázat: Könyvtár leíró űrlap

Könyvtár leíró űrlap	Első rész
Készítette:	Dátum:
<b>Utasítások</b>	
<ul style="list-style-type: none"> <li>A "Felhasználói biztonság tervezése" és az "Erőforrás biztonság tervezése" című részekben tanulmányozhatja az űrlapot.</li> <li>Az űrlap a könyvtárak leírására és erőforrás biztonságuk követelményeinek meghatározására szolgál.</li> <li>Töltsön ki egy-egy űrlapot a rendszer minden fő alkalmazási könyvtárához.</li> <li>Az űrlap információinak bevitelét az "Erőforrás biztonság beállítása" című részben tanulmányozhatja.</li> </ul>	
Könyvtár neve:	Leírónév (szöveg):
A könyvtár funkciójának rövid leírása:	
Határozza meg a könyvtár biztonsági elemeit, vajon van-e titkos információ:	
Könyvtár nyilvános jogosultsága:	
Objektum nyilvános jogosultsága a könyvtárban:	
Új objektumok (CRAFT) nyilvános jogosultsága:	
Könyvtár tulajdonosa:	

Könyvtár leíró űrlap		Második rész		
Készítette:		Dátum:		
Könyvtár neve:				
<b>További utasítások a 2. részhez:</b>				
<ul style="list-style-type: none"> <li>Az alábbi táblázatban tüntesse fel az egyediségeket és objektumokat, melyek speciális jogosultságot igényelnek.</li> <li>Specifikálja a szükséges jogosultságokat: *ALL, *CHANGE, *USE vagy *EXCLUDE.</li> </ul>				
Különleges jogosultságok könyvtári objektumokhoz				
Csoport- vagy felhasználói profil	Objektum neve	Objektum típusa	Szükséges jogosultság	Jogosultsági lista

## Rendszerváltozók kiválasztására szolgáló űrlap

69. táblázat: Rendszerváltozók kiválasztására szolgáló űrlap

Rendszerváltozók kiválasztására szolgáló űrlap	Első rész
--	-----------

69. táblázat: Rendszerváltozók kiválasztására szolgáló űrlap (Folytatás)

Készítette:		Dátum:
<b>Utasítások</b>		
<ul style="list-style-type: none"> <li>Az űrlapot megismerheti az "Átfogó biztonsági stratégia tervezése" című részben.</li> <li>Az űrlap a biztonságra és az egyéniesítésre hatással lévő rendszerváltozók kiválasztásának rögzítésére szolgál.</li> <li>Használja az <b>1</b>-es opciót a SETUP menüben az űrlap első részének bevételéhez.</li> </ul>		
Értékek a Change System Options képernyőről		
<b>Rendszerváltozó/Hálózati tulajdonság</b>	<b>Javasolt választás</b>	<b>Saját választás</b>
Rendszer neve		
Dátum elválasztó (QDATSEP)		
Dátum formátum (QDATFMT)		
Idő elválasztó (QTIMSEP)		
Egység-elnevezés formátuma új egységekre (QDEVNAMING)	1 (iSeries rendszer)	
Rendszernyomtató (QPRTDEV)		
Biztonsági szint (QSECURITY)	40	
Engedély a biztonsági felelősnek, hogy bármely állomásról bejelentkezhet (QLMTSECOFR)	N	
Munkaelszámolási információk tárolása a befejezett listákról (QACGLVL)	N (*NONE)	

Rendszerváltozók kiválasztására szolgáló űrlap		Második rész
<b>További utasítások a 2. részhez:</b>		
<ul style="list-style-type: none"> <li>Az űrlap második részét a "Rendszerváltozók beállítása" című rész tárgyalja.</li> <li>A második rész adatainak bevételéhez használja a Work With System Value (WRKSYSVAL) parancsot.</li> </ul>		
Biztonsági rendszerváltozók		
<b>Rendszerváltozó</b>	<b>Javasolt választás</b>	<b>Saját választás</b>
Inactive job time-out interval (QINACTITV)	30 - 60	
Inactive job message queue (QINACTMSGQ)	*DSCJOB	
Limit device sessions (QLMTDEVSSN)	1 (Igen)	
Action to take for failed sign-on attempts (QMAXSGNACN)	3 (mindkettő letiltása)	
Maximum sign-on attempts allowed (QMAXSIGN)	3 - 5	
Password expiration interval (QPWDEXPITV)	30 - 60	
Maximum password length (QPWDMAXLEN)	8	
Minimum password length (QPWDMINLEN)	6	
Require different passwords (QPWDRQDDIF)	7 (6 egyedi jelszó)	
Egyéb rendszerváltozók		

Rendszerváltozó	Javasolt választás	Saját választás
Disconnected job time-out interval (QDSCJOBITV)	300	
<p><b>Megjegyzés:</b> Szándékában állhat néhány további, biztonsággal kapcsolatos rendszerváltozó beállítása. Nézze meg a <i>Biztonsági szakkönyv</i> (SC22-0282-04) könyv harmadik fejezetét, ahol megtalálhatja a biztonsággal kapcsolatos összes rendszerváltozót és ajánlott értékeiket.</p>		

## Rendszerfelelősségek űrlap

70. táblázat: Rendszerfelelősségek űrlapja

Rendszerfelelősségek űrlapja			
Készítette:		Dátum:	
<p><b>Utasítások</b></p> <ul style="list-style-type: none"> <li>Az űrlapot megismerheti az "Egyedi felhasználói profilok tervezése" című részben.</li> <li>Az űrlap a *USER osztálytól eltérő osztályú felhasználók számbavételére szolgál.</li> <li>Írja át az űrlap adatait az Egyedi felhasználói profil űrlap <i>Felhasználói osztály</i> oszlopába.</li> </ul>			
Elsődleges biztonsági felelős			
Másodlagos biztonsági felelős			
Profil neve	Felhasználó neve	Osztály	Megjegyzések

## Felhasználói csoportot azonosító űrlap

71. táblázat: Felhasználói csoportot azonosító űrlap

Felhasználói csoportot azonosító űrlap								
Készítette:					Dátum:			
<p><b>Utasítások</b></p> <ul style="list-style-type: none"> <li>Az űrlapot megismerheti a "Felhasználói csoportok tervezése" című részben.</li> <li>Az űrlap segítségével meghatározhatja a felhasználók azon csoportjait, amelyek hasonló alkalmazási igényekkel állnak elő. <ol style="list-style-type: none"> <li>Sorolja fel a fő alkalmazásokat az űrlap tetején.</li> <li>Sorolja fel a felhasználókat a baloldali oszlopban.</li> <li>Jelölje meg a szükséges alkalmazásokat minden felhasználó esetén.</li> </ol> </li> <li>A rendszerre nem kell bevinni az űrlapon lévő információkat.</li> </ul>								
					Alkalmazások elérési módja			
Felhasználó neve	Osztály	ALK:	ALK:	ALK:	ALK:	ALK:	ALK:	ALK:



71. táblázat: Felhasználói csoportot azonosító űrlap (Folytatás)


**Megjegyzés:**

- Ha biztonsági környezete *laza*, jelölje **X** betűvel mely alkalmazásokat igénylik a felhasználók.
- Ha biztonsági környezete *korlátozott*, használja a **C** (change) és a **V** (view) jelölést arra, hogy az alkalmazást *hogyan* használják a felhasználók.

## Felhasználói csoportot leíró űrlap

72. táblázat: Felhasználói csoportot leíró űrlap

Felhasználói csoportot leíró űrlap	Első rész
Készítette:	Dátum:
<p><b>Utasítások az 1. részhez</b></p> <ul style="list-style-type: none"> <li>• Az űrlapot megismerheti a "Felhasználói csoportok tervezése" című részben.</li> <li>• Az űrlap információinak bevitelét a "Felhasználói biztonság beállítása" című részben tanulmányozhatja.</li> <li>• Készítsen külön űrlapot minden csoportra, amelyik használja a rendszert.</li> <li>• Hozzon létre jobleírást a csoport számára a Create Job Description (CRTJOBDD) paranccsal. A jobleírás tartalmazza a csoport kezdeti könyvtárlistáját.</li> </ul>	
Csoportprofil neve:	
Csoport leírása:	
Csoport elsődleges alkalmazása:	
További alkalmazások listája:	
A csoport könyvtárigényének listája. Tegyen jelet (✓) minden olyan könyvtár elé, melynek a kezdeti könyvtárlistában kell szerepelnie:	
<p><b>Megjegyzés:</b> Nézze meg az Alkalmazást leíró űrlapot az előző szekcióban felsorolt minden alkalmazásra azért, hogy meghatározhassa, mely könyvtárakat használja az alkalmazás.</p>	

Felhasználói csoportot leíró űrlap	Második rész	
<p><b>További utasítások a 2. részhez:</b></p> <ul style="list-style-type: none"> <li>• Az alábbi táblázat tartalmazza a Create User Profile képernyőn megjelenő összes mezőt. A mezők két részre oszlanak: egyik rész tartalmazza az IBM által javasolt értékeket, míg a másik a saját választás beírására szolgál.</li> <li>• Használja a Work with User Profiles képernyőt vagy a Create User Profile (CRTUSRPRF) parancsot az űrlap ezen információinak beviteléhez.</li> </ul>		
<p><b>Válasszon értékeket a csoportprofil alábbi mezőire:</b></p>		
<b>Mező neve</b>	<b>Javasolt választás</b>	<b>Saját választás</b>
Csoportprofil neve		
Jelszó	*NONE	
Felhasználói osztály	*USER	
Aktuális könyvtár	<i>mint a csoportprofil neve</i>	
Hívandó kezdeti program (bejelentkezési program)		
Kezdeti programkönyvtár		
Kezdeti menü		

Kezdeti menükönyvtár		
Korlátolt képességek (korlátolt parancssor haszn.)	*YES	
Szöveg (felhasználó leírás)		
Jobleírás	<i>mint a csoportprofil neve</i>	
Jobleírás könyvtár		
Csoportprofil neve	*NONE	
Nyomtató egység		
Kimeneti sor	*DEV	
<b>Megjegyzés:</b> Az itt felsorolt mezők sorrendje megegyezik a Create User Profile képernyőn láthatóval (F4-t használva).		
<b>Használja a rendszer szolgáltatá (alapértelmezett) értékeket az alábbi mezőkre:</b>		
Accounting code	Keyboard buffering	Public authority
Assistance Level	Language ID	Set password to expire
Attention program	Limit device sessions	Sort sequence
Coded character set ID	Maximum storage	Special authority
Country or Region ID	Message queue	Special environment
Display sign-on information	Password expiration interval	Status
Document password	Priority limit	User options
<b>Megjegyzés:</b> Az opciók neveit hagyjuk angol nyelven, mivel a képernyőn is így találja. A mezőket itt alfabetikus sorrendben mutatjuk.		

## Egyedi felhasználói profil űrlapja

73. táblázat: Egyedi felhasználói profil űrlapja

Egyedi felhasználói profil űrlapja						
Készítette:				Dátum:		
<b>Utasítások</b>						
<ul style="list-style-type: none"> <li>Az űrlapot megismerheti az "Egyedi felhasználói profilok tervezése" című részben.</li> <li>Az űrlapot az egyedi felhasználók adatainak felvételére használhatja. Töltsön ki egy-egy űrlapot a rendszer minden egyes felhasználói csoportjára (csoportprofil) részére.</li> <li>Használja a jobboldali üres oszlopokat az egyedi felhasználók jellemzőinek megadására.</li> <li>Az űrlap információinak bevitelét az "Egyedi felhasználók beállítása" című részben tanulmányozhatja.</li> </ul>						
Csoportprofil neve:						
Létrehozott objektum tulajdonosa:				Csoportjogosultság az objektumokhoz:		
Csoport jogosultság típusa:						
A csoport minden tagját jegyezze fel:						
Felhasználói profil	Szöveg (leírás)	Felhasználói osztály	Korlátolt képesség			



75. táblázat: Kimeneti sor és munkaállomás biztonság űrlapja (Folytatás)

<b>Utasítások</b>				
<ul style="list-style-type: none"> <li>Az űrlapot megismerheti a "Nyomtatott lista védelme" című részben.</li> <li>Minden, speciális védelmet igénylő munkaállomást és kimeneti sort jegyezzen fel ezen az űrlapon.</li> <li>Az űrlap információinak bevitelét a "Munkaállomások védelme" című részben tanulmányozhatja.</li> </ul>				
<b>Korlátozott kimeneti sor paraméterlistája:</b>				
Kimeneti sor neve	Kimeneti sor könyvtára	Fájl megtekintése (DSPDTA)	Ellenőrzés jogosultság (AUTCHK)	Operátor vezérlés (OPRCTL)
<b>Biztonsági felelős munkaállomásai:</b>				
Ha megadott munkaállomásokra korlátozta a biztonsági felelőst (QLMTSECOFR rendszerváltozó = igen), az alábbiakban sorolja fel azokat a munkaállomásokat melyekre a biztonsági felelősnek és minden *ALLOBJ jogosultságú felhasználónak jogosultsága van.				
<b>Sorolja fel a jogosultságokat a korlátozott munkaállomásokra:</b>				
Munkaállomás neve	Jogosult csoportok vagy felhasználók (*CHANGE jogosultság)			
<b>Megjegyzés:</b> A korlátozott munkaállomások nyilvános jogosultsága *EXCLUDE értékű.				

## Alkalmazás telepítési űrlap

76. táblázat: Alkalmazás telepítési űrlap

Alkalmazás telepítési űrlap	Első rész	
Készítette:	Dátum:	
<b>Utasítások</b>		
<ul style="list-style-type: none"> <li>Az űrlapot megismerheti az "Alkalmazások telepítésének tervezése" című részben.</li> <li>Külön űrlapot készítsen minden telepítendő alkalmazásra.</li> <li>Az űrlap az alkalmazások betöltése után nyilvános jogosultságaik és tulajdonjogaik tervezésére szolgál.</li> <li>Az űrlap információinak bevitelét az "Erőforrás biztonság beállítása" című részben tanulmányozhatja.</li> </ul>		
Alkalmazás neve:		
Leírás:		
Az alkalmazás telepítéséhez szükséges profilok listája és magyarázata:		
<b>Könyvtár neve:</b>		
	Telepítés előtt	Telepítés után
Könyvtár tulajdonosa		
Objektum tulajdonosa		
Könyvtár nyilvános jogosultsága		
Objektum nyilvános jogosultsága		
Új objektumok nyilvános jogosultsága		
<b>Könyvtár neve:</b>		
	Telepítés előtt	Telepítés után

76. táblázat: Alkalmazás telepítési űrlap (Folytatás)

Könyvtár tulajdonosa		
Objektum tulajdonosa		
Könyvtár nyilvános jogosultsága		
Objektum nyilvános jogosultsága		
Új objektumok nyilvános jogosultsága		

Alkalmazás telepítési űrlap		Második rész
<b>Könyvtár neve:</b>		
	Telepítés előtt	Telepítés után
Könyvtár tulajdonosa		
Objektum tulajdonosa		
Könyvtár nyilvános jogosultsága		
Objektum nyilvános jogosultsága		
Új objektumok nyilvános jogosultsága		
<b>Könyvtár neve:</b>		
	Telepítés előtt	Telepítés után
Könyvtár tulajdonosa		
Objektum tulajdonosa		
Könyvtár nyilvános jogosultsága		
Objektum nyilvános jogosultsága		
Új objektumok nyilvános jogosultsága		
<b>Könyvtár neve:</b>		
	Telepítés előtt	Telepítés után
Könyvtár tulajdonosa		
Objektum tulajdonosa		
Könyvtár nyilvános jogosultsága		
Objektum nyilvános jogosultsága		
Új objektumok nyilvános jogosultsága		



---

## . Megjegyzések

Ez a tájékoztatás az Egyesült Államokban kínált termékekhez vagy szolgáltatásokhoz készült.

Az IBM lehet, hogy nem ajánlja az ebben a dokumentációban tárgyalt termékeket, szolgáltatásokat vagy kiegészítőket más országokban. Az adott országokban rendelkezésre álló termékekről és szolgáltatásokról a helyi IBM képviselők szolgálnak felvilágosítással. Az IBM termékekre, programokra vagy szolgáltatásokra vonatkozó hivatkozások sem állítani, sem sugallni nem kívánják, hogy az adott helyzetben csak az IBM termékeit, programjait vagy szolgáltatásait lehet alkalmazni. Minden olyan működésében azonos termék, program vagy szolgáltatás alkalmazható, amely nem sérti az IBM szellemi tulajdonjogát. A nem IBM termékek, programok és szolgáltatások működésének megítélése és ellenőrzése természetesen a felhasználó felelőssége.

A dokumentum tartalmával kapcsolatban az IBM-nek bejegyzett, vagy bejegyzés alatt álló szabadalmi lehetnek. Ennek a dokumentumnak az átadása azonban nem jelenti ezen szabadalmak licencjogának átadását is. Az írásos licenckérelmeket az alábbi címre küldheti:

IBM Director of Licensing  
IBM Corporation  
500 Columbus Avenue  
Thornwood, NY 10594-1785  
U.S.A.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatba az országában az IBM szellemi tulajdon osztályával, vagy írjon a következő címre:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106, Japan

**A következő bekezdés nem vonatkozik az Egyesült Királyságra és más olyan országra sem, ahol ez ütközik a helyi jogi szabályozással:** Az INTERNATIONAL BUSINESS MACHINES CORPORATION az "ITT ISMERTETETT MÓDON" adja közre ezt a kiadványt, MINDENFAJTA KIFEJEZETT VAGY SUGALLT GARANCIA NÉLKÜL, BELEÉRTVE - DE NEM KORLÁTOZVA ERRE - A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMİ ÉRTÉKESÍTÉSRE ÉS VALAMELY ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ GARANCIÁT. Egyes államok nem engedik meg a kifejezett, vagy bennfoglalt garanciák visszautasítását bizonyos ügyletek esetén, ennek következtében ez az állítás lehet, hogy nem vonatkozik mindenkire.

Ez a publikáció tartalmazhat technikai pontatlanságokat és nyomdahibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A könyvben a nem IBM Web helyekre történő hivatkozások csupán kényelmi célokat szolgálnak, és semmilyen módon sem kívánják azt a látszatot kelteni, hogy az IBM jóváhagyná ezeket a Web helyeket. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

Az ezen program licencével rendelkezők vegyék fel a kapcsolatot az alábbi címmel, ha információra van szükségük a következő célú engedélyezésekről: (i) információcsere függetlenül alkotott programok és más programok (ideértve ezt a programot is) között, és (ii) a kicserélt információ kölcsönös használata.

IBM Corporation  
Software Interoperability Coordinator, Department 49XA  
3605 Highway 52 N

Rochester, MN 55901  
U.S.A.

Az ilyen jellegű információk legtöbbször rendelkezésre állnak, bizonyos esetekben és körülmények között díjkötelesen.

Az itt említett engedélyezett programot és minden, ehhez rendelkezésre álló engedélyezett anyagot, az IBM a két fél között fennálló IBM Customer Agreement, IBM International Program License Agreement vagy ezzel egyenértékű egyéb megállapodás feltételei alapján biztosítja.

A nem IBM termékekre vonatkozó információk a termékek szállítóitól, illetve azok publikált dokumentációiból, valamint egyéb nyilvánosan hozzáférhető forrásokból származnak. Az IBM nem tesztelte ezeket a termékeket, így a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint egyéb állítások pontosságát. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítóhoz.

Az itt leírt információk csak tervezési célokat szolgálnak. Így az itt található információk módosulhatnak, mielőtt a leírt termékek beszerezhetők lennének.

Ez a dokumentum a napi üzleti műveletekből vett, példaként használt mintaadatokat és jelentéseket tartalmaz. A műveletek megfelelő szemléltetéséhez a példákban személyek, vállalatok, márkák és termékek nevei is előfordulnak. Ezek a nevek minden esetben kitalált nevek. Esetleges hasonlóságuk a valódi vállalatnevekhez és címekhez kizárólag a véletlen műve.

---

## Védjegyek

A következő kifejezések az International Business Machines Corporation védjegyei az Egyesült Államokban és/vagy más országokban:

Application System/400  
AS/400  
e (logó)  
IBM  
iSeries  
Operating System/400  
OS/400  
400

A Lotus, a Freelance és a WordPro az International Business Machines Corporation és a Lotus Development Corporation védjegyei az Egyesült Államokban és/vagy más országokban.

A C-bus a Corollary, Inc. védjegye az Egyesült Államokban és/vagy más országokban.

Az ActionMedia, a LANdesk, az MMX, a Pentium és a ProShare az Intel Corporation védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Microsoft, a Windows, a Windows NT és a Windows logó a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A SET és a SET embléma a SET Secure Electronic Transaction LLC védjegye.

A Java, valamint az összes Java alapú védjegy a Sun Microsystems, Inc. védjegye az Egyesült Államokban és/vagy más országokban.

A UNIX az Open Group bejegyzett védjegye az Egyesült Államokban és más országokban.

Egyéb cég-, termék- és szolgáltatásnevek mások áru-, vagy szolgáltatási védjegyei lehetnek.



---

## A kiadványok letöltésére és kinyomtatására vonatkozó feltételek

A letöltésre kiválasztott kiadványok használatára vonatkozó engedélyt az alábbi feltételek és kikötések elfogadásának jelzése adja meg.

**Személyes használat:** A Kiadványok reprodukálhatók személyes, nem kereskedelmi célú használatra, valamennyi tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem szabad a kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.

**Kereskedelmi használat:** A Kiadványok reprodukálhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalaton belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett engedélyének hiányában nem készíthetők ezen Kiadványokból származó munkák, nem reprodukálhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalaton kívül.

A jelen engedélyben foglalt, kifejezetten megadott engedélyeken túlmenően a Kiadványokra, illetve a bennük található információkra, adatokra, szoftverre vagy bármilyen szellemi tulajdonra semmilyen más kifejezett vagy vélelmezett engedély nem vonatkozik.

Az IBM fenntartja magának a jogot, hogy jelen engedélyeket saját belátása szerint bármikor visszavonja, ha úgy ítéli meg, hogy a Kiadványokat az IBM érdekeit sértő módon használják fel, vagy a fenti útmutatásokat nem megfelelően követik.

Jelen információk kizárólag valamennyi vonatkozó törvény és előírás betartásával tölthetők le, exportálhatók és reexportálhatók, beleértve az Egyesült Államok exportra vonatkozó törvényeit és előírásait is. Az IBM A KIADVÁNYOK TARTALMÁRA VONATKOZÓAN SEMMIFÉLE GARANCIÁT NEM NYÚJT. A KIADVÁNYOK "ÖNMAGUKBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA VÁLLALÁSA NÉLKÜL KERÜLNEK KÖZREADÁSRA, IDEÉRTVE, DE NEM KIZÁRÓLAG A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.

Valamennyi anyag szerzői jogának birtokosa az IBM Corporation.

A webhelyen található kiadványok letöltésével vagy nyomtatásával jelzi, hogy elfogadja jelen feltételeket és kikötéseket.







Nyomtatva Dániában