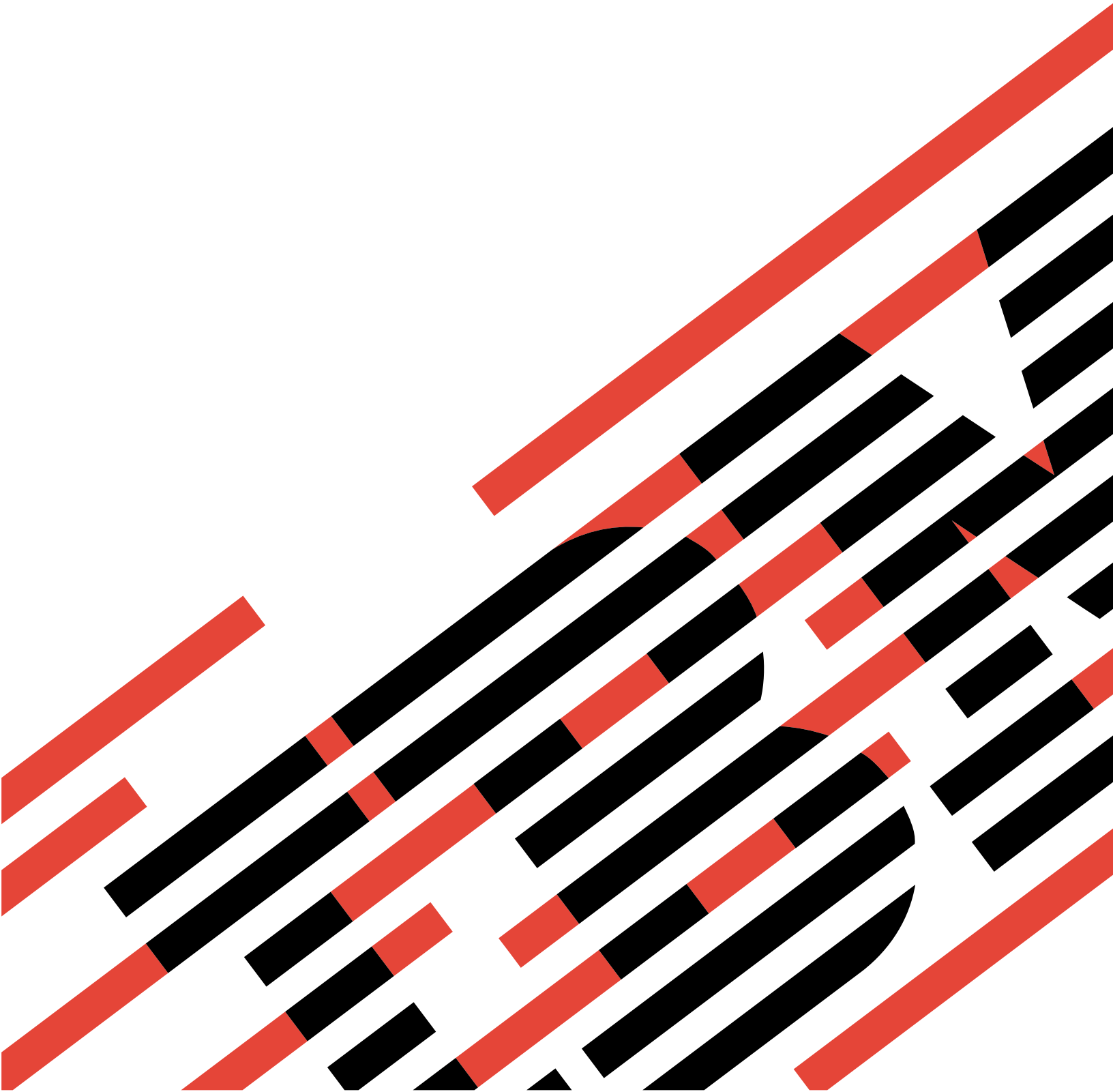
IBM

eserver

iSeries

基本系統安全及規劃



IBM

@server

iSeries

基本系統安全及規劃

目錄

第 1 篇 基本系統安全及規劃

基本系統安全及規劃提供您關於規劃及設定 iSeries 安全的詳細資訊。這個主題著重於提供規劃及格式，讓您規劃並記錄安全決策。它還提供基本系統安全的逐步設定說明。由於這個主題的活頁簿性質，您可能需要將它列印出來，仔細複查內容。

若要爲 iSeries 設定最佳安全，有兩組主要活動：規劃作業及配置作業。爲確保設定的安全符合企業需求，您必須複查這些規劃主題：

- 基本系統安全入門，提供一般系統安全概念概觀，以及回答基本系統安全問題。
- 規劃使用者安全，提供如何規劃系統使用者安全的相關資訊。這包括實體安全、應用程式安全、整體安全策略，以及系統中的使用者設定檔。
- 規劃資源安全，提供如何規劃系統物件安全性的相關資訊，包括檔案庫及檔案庫中的物件、印表機、印表機輸出以及工作站。

完成規劃活動後，您可以複查這些主題來協助您設定系統安全。

- 設定使用者安全，提供設定使用者及群組安全的明細。
- 設定資源安全，提供如何設定物件所有權、物件的公用或特定權限、印表機和工作站的安全等相關資訊。
- 測試安全，提供測試安全的相關資訊。
- 變更安全資訊，提供更新及修改使用者與群組設定檔和資源安全的相關資訊。
- 保存安全資訊，提供備份安全資訊的相關資訊。
- 監督安全，提供安全追蹤的核對清單，以及安全審核的相關資訊。

除了這些主題之外，您還可以使用規劃套表來撰寫規劃策略及安全決策的文件。

第 1 章 新增功能

V4R5「資訊中心」的新增功能有基本系統安全及規劃。這個資訊原本在*安全基本概念 (Security-Basic)* (SC41-5301-00) 一書中。它已經過更新，反映出 V4R5 系統安全設定的現行資訊。

第 2 章 列印本主題

您可以檢視本文件的 PDF 版本，或加以下載以便檢視或列印。若要檢視 PDF 檔，您必須有安裝 Adobe® Acrobat® Reader。該軟體可自 Adobe 首頁下載 

若要檢視或下載 PDF 版本，請選取基本系統安全與規劃 (950 KB 或 164 頁)。

若要將 PDF 儲存至您的工作站來加以檢視或列印，請執行下列步驟：

1. 在您的瀏覽器中開啓 PDF (按一下上方的鏈結)。
2. 在瀏覽器的功能表中，按一下**檔案**。
3. 按一下**另存新檔...**。
4. 導覽至要用於儲存此 PDF 的目錄。
5. 按一下**儲存**。

第 3 章 基本系統安全入門

從系統管理者到使用者，每個人都應該關心安全問題。系統安全可保護 iSeries 與您的重要商業資訊，使其不致遭受有意或無意的破壞。

您可以根據本身的安全環境與需求，來自訂系統安全機能。

安全機能就如同系統的門戶。您可以透過它來**鎖定**或防範資訊遭到擅用。

安全機能也可用來**釋放**系統的彈性，爲每位使用者量身打造適合的環境。

良好的安全計畫雖可保護您的系統，但無法保證您的設備與資訊的安全。因此您應該將維護系統安全的責任分派給多位員工，以確保沒有任何一個人員可以全權掌控整個系統。

「基本系統安全及規劃」會提供逐步作法，供您用於規劃及設定基本系統安全。本主題著重在規劃系統安全的重要性，並提供相關的規劃表單，讓您用於記錄安全決策。爲協助您制定安全方面的決策，本主題列有相關商業範例，以一家正在規劃安全事務的企業來作說明。

要確保能夠順利達成系統安全維護，良好且徹底的規劃是不可或缺的。請複查下列主題，以瞭解基本安全的相關需求以及安全規劃的重要性：

- 關於基本系統安全的常見問題
- 基本系統安全概觀
- 規劃基本系統安全的方法

您還要對系統上的所有資訊，訂立良好的備份及回復計劃。此外，亦須擁有遇到災害時的設備置換計劃。有關設計良好備份計劃的詳情，請參閱「資訊中心」下的備份及回復服務程式主題。

關於使用者安全的詳細規劃資訊

下列主題則會提供關於使用者安全的規劃技巧：

- 規劃應用程式的安全
- 規劃您的安全策略
- 規劃使用者群組
- 規劃個別使用者設定檔

關於資源安全的詳細規劃資訊

下列主題會提供系統化的方式，供您針對使用者來規劃資源安全。

- 瞭解權限的型類
- 規劃應用程式檔案庫的安全
- 決定檔案庫與物件的所有權
- 將物件分組
- 保護印表機輸出

- 保護工作站
- 規劃您的應用程式安裝

可列印的規劃表單

「基本系統安全及規劃」中列有可列印的套表，可供您記錄所有安全決策。您可以用 PDF 檔來列印整個主題，或透過瀏覽器的列印按鈕來列印個別的規劃套表。

基本系統安全的逐步設定指示

完成安全規劃後，本主題會列出如何使安全計劃生效的相關步驟。下列主題可協助您設定系統安全。
- 設定使用者安全
- 設定資源安全

關於基本系統安全的常見問題

複查下列關於安全之常見問題的回答，將有助於您進一步瞭解系統安全的重要性。

安全為何如此重要？

儲存在您系統上的資訊是您最重要的商業資產之一。當您思考要如何保護資訊資產之際，請切記三大目標：

- **機密性**：良好的安全措施可防止人員偷窺或披露機密資訊。
- **整合性**：就某種程度而言，設計完善的安全系統可確保您電腦上的資訊精確度。透過正確的安全機能，您將可防範資料在未經授權下遭致變更或刪除。
- **可用性**：若某人有意或無意地損壞了您系統上的資料，您勢必得等到這些資源回復後才可再加以存取。良好的安全系統將可避免發生此種損壞。

當人們提到系統安全時，多半會想到防止外人 (例如商業對手) 進入其系統。實際上，防止適當使用者的好奇行爲或系統意外，往往是設計完善之安全系統的最大強處。在不具良好安全特性的系統中，使用者可能會無意地刪除掉重要檔案。而設計完善的安全系統就能防止此類意外發生。

當您要決定系統所需的安全程度時，請自問下列問題：

- 您的電腦 (以及儲存在其上的資料) 對您的業務有多重要？
- 您的公司是否訂有相關原則來要求某種安全層次？
- 您的審核員是否要求您的電腦上儲存的資訊需要具備某種安全層次？
- 您在可見的未來是否需要某種程度的安全？

為何要自訂您的系統？

iSeries 的使用者遍及廣泛的範圍。一套小型的系統可能只有三到五位使用者，而且僅執行少量應用程式。若是大型系統則可能擁有數千位使用者，並透過大型通信網路執行許多應用程式。

iSeries 具有許多彈性化的設計，可容納各種範圍的使用者與狀況。從使用者所看到的系統外觀到相關的執行方式，有許多事項都可由您自行變更。

系統剛送達時，您可能不需或不想執行過多自訂作業。IBM 在出貨時即已對許多選項作好起始設定，稱爲**預設值**。這些預設值通常是新機安裝時最適用的選項。

註: 所有新系統出貨時皆已預設在安全層次 **40**。此安全層次除可確保只有經您定義的使用者能夠使用系統外，還能避免會破壞安全的程式對整合性或安全性所造成的潛在風險。

不過，若能執行一些自訂作業，您的系統對使用者而言將會成爲更簡單好用且更具效率的工具。例如，您可以確保使用者在登入時都能取得正確的功能表。還可確保每位使用者的報表都能送往正確的印表機。所以若能執行一些起始自訂作業，讓系統成爲更具親和力的工具，使用者將對系統更具信心。

誰該負責？

不同的企業會採行不同的安全措施。有時是由程式設計師負責所有安全事務的重任。也有可能是由管理系統的人員兼任安全重責。如果您不確定要如何指派貴公司的安全責任，以下是我們建議的作法：

- 您的資源安全規劃方法應取決於貴公司是否外購或自行開發應用程式。如果是自行開發，便應在開發階段提出您的資源安全需求。如果是外購應用程式，則須瞭解並配合應用程式設計者。不論是何種情況，設計應用程式的人都應在設計時將安全事項納入考慮。
- 設定安全機能應該是安全主管的責任。安全主管須定義系統使用者以及他們對系統的存取權限。安全主管通常還負責其他系統事務，例如備份及回復資訊。
- 安全主管亦須自訂您的系統，因爲許多安全要件在系統自訂作業中都扮演了重要角色。

不論您是以哪種方式來指派安全責任，都應**發佈安全原則**。最好由貴公司的經理主管以書面向大家宣達，指出電腦中的資訊是一項非常重要的資產。此種資訊應和其他公司資產一樣受到保護。有關安全原則的範例，請參閱《範例：JKL Toy Company 的安全原則》。

現在您已瞭解了系統安全上的需求，接下來應複查系統安全注意事項的概觀。

基本系統安全概觀

爲能有效地進行規劃，您必須充份瞭解自己所要達成的目標與系統工具兩者之間的關聯。您需要知道使用者與系統此類特性可在哪些方面協助您達成目標。

下列主題將介紹有關安全與自訂方面的重要事項，並說明其配合方式。這些主題旨在預先提供概要觀念，以利您展開規劃作業。此處所介紹的所有觀念將會在規劃過程中進一步闡釋。

- 內建系統安全
- 基本術語
- 使用者對安全的觀點
- 用於安全和自訂作業的系統工具

內建系統安全

系統端的各部安全元件皆已內建在系統中。他們不是分開購買的單獨產品。此種整合作法具有數項優點：

- 整個作業系統皆具備一致的安全性。它將使用相同的顯示器、指令及術語。
- 使用者將無法略過安全機能，因爲它已遍及整個系統。
- 經妥善設計的安全機能對效能影響極微。
- 隨著新軟體的開發，安全機能也會與時並進。當新的功能出現時，這些功能的安全機能也會同時現身。

iSeries 出貨時已設定在安全層次 40，此層次可防止未經授權的使用者登入系統。還能避免會破壞安全的程式對整合性或安全性所造成潛在風險。不過，您仍可自訂特定的安全設定值或變更安全層次。有關安全層次的說明，請參閱主題《選擇您的安全層次》。

現在您已進一步瞭解了內建安全機能的運作方式，接下來應熟悉常用的 iSeries 術語。

基本術語

以下的一般術語對瞭解 iSeries 的安全性而言十分重要：

物件 所謂物件是指系統上可供操作的具名空間。最常見的物件範例是檔案與程式。其他類型的物件包括指令、佇列、檔案庫及資料夾。系統上的物件是以物件名稱、物件類型和物件所在的檔案庫來識別。系統上的每一個物件皆可加以保護。

檔案庫 檔案庫是一種特殊類型的物件，可用於將其他物件組合在一起。系統上的許多物件皆常駐在某一檔案庫中。

目錄 目錄是用來在系統上將物件劃分組的另一種方式。物件可以常駐在某一目錄中。目錄亦可常駐於另一目錄中，形成階層式結構。

現在您已進一步瞭解了 iSeries 安全性的一般術語，接下來您可能會想要瞭解使用者對安全的觀點。

使用者對安全的觀點

就使用者的觀點而言，安全會影響其在系統上運用及完成作業的方式。其中包括他們是如何與系統互動來完成這些作業。因此，務必要考量使用者是如何看待安全。例如，將密碼設成每五日即到期，就會貶抑和干擾使用者完成其作業的能力。反之，過於鬆弛的密碼原則卻又會導致安全問題。

爲求提供適當的系統安全，您必須將其區分成特定的部份，以便加以規劃、管理和監督。從使用者的觀點來看，您可以將系統安全分成以下數個部份：

對系統的實體存取

實體安全可以保護主機、所有系統裝置以及備份儲存媒體 (例如磁片、磁帶或 CD)，使其不致遭受有意或無意的遺失或損壞。

就系統而言，您用來確保系統實體安全的大部份措施多半屬於外部行動。不過，系統本身附有按鍵鎖定或電子閂鎖，可防止主機遭到侵入使用。

主題《規劃實體安全》即列有詳細資訊，可協助您規劃系統的實體安全。

使用者如何登入

登入安全主要是用來防範不明人員登入系統。若要登入系統，個別人員必須輸入使用者 ID 與密碼的有效組合。

您可以同時運用系統值和個別使用者設定檔，來確保登入安全不會遭到侵害。例如，您可以要求定期變更密碼。也可排除使用易於猜測的密碼。

允許使用者執行的作業

界定使用者所能執行的作業，是安全與系統自訂作業的重任之一。就安全觀點而言，這多半是屬於一種**限制性**機能，例如防止有人看到某些特定資訊。但就系統自訂的觀點而言，則是屬於**授權**機能。經適當自訂的系統可汰除不必要的作業與資訊，使人員可以作好份內工作。

在界定使用者所能執行之作業的方法中，有些適合安全主管來處理，有些則是程式設計師的責任。本文主要著眼於安全主管的任務。有關各類系統值的說明，請參閱 *Security-Reference* (SC41-5302) 的第 3 章《Security System Values》。

個別使用者設定檔、工作說明和類別中皆提供有相關參數，可用來控制使用者在系統上所能執行的作業。下列清單會簡述可用的各類技巧：

限制使用者只能存取少數功能

您可以根據使用者設定檔，限制使用者只能使用特定程式、功能表、功能表集和少數系統指令。一般來說，安全主管會負責建立及控制使用者設定檔。

限制系統功能

系統功能可供您儲存及復置資訊、管理印表機輸出以及設定新的系統使用者。每個使用者設定檔皆會指定使用者能執行哪些常用系統功能。

在 iSeries 上，您是透過控制語言 (CL) 指令與應用程式設計介面 (API) 來執行系統功能。由於每個指令與 API 都是物件，因此您可用物件權限來控制誰能夠加以使用及完成系統功能。

決定誰可使用檔案與程式

資源安全可提供相關功能來控制系統上每個物件的使用情形。對任何物件而言，您可以指定誰能加以使用以及使用方式。例如，您可以指定一位使用者只能查看某檔案中的資訊；另一使用者可變更此檔案的資料；第三位使用者則可變更檔案或刪除整個檔案。

防止濫用系統資源

您的系統處理能力會與系統所儲存的資料一樣，對業務而言非常重要。安全主管應協助確保使用者不會誤用系統資源，例如優先處理其工作、優先列印其報表或佔用過多磁碟儲存體。

您的系統如何與其他電腦通信

如果您的系統會與其他電腦或可程式工作站相通信，將可能需要額外的安全措施。因爲若無適當的安全管制，別人便可不經登入程序，從網路中的其他電腦啓動您電腦上的工作或存取其上的資訊。

您可以同時利用系統值與網路屬性，來控制是否允許遠端工作、遠端存取資料或遠端 PC 存取您的系統。如果允許遠端存取，亦可指定要施行何種安全作業。有關各類系統值的說明，請參閱 *Security-Reference* (SC41-5302) 的第 3 章《Security System Values》。

如何儲存您的安全資訊

您必須定期備份系統資訊。除了儲存系統上的資料外，您還須儲存安全資訊。如果發生災害，您須能回復系統使用者的相關資訊、授權資訊和系統資訊。

主題《保存安全資訊》即在解釋如何儲存安全資訊。「資訊中心」下的備份及回復服務程式主題，則列有關於備份及回復安全資料的詳細資訊。

如何監督您的安全計劃

本系統提供有數種工具，可用來監督安全效益：

- 當發生特定的安全違規狀況時，會傳送訊息告知系統操作員。
- 各類與安全有關的異動皆會記錄在特殊的審核日誌中。

主題《監督安全》即在討論此類工具的一般使用方式。有關安全審核的進一步詳情，可參閱 *Security-Reference* (SC41-5302) 的第 9 章《Auditing Security on the System》。

要進一步瞭解如何自訂您的系統，您應瞭解如何從使用者的觀點來進行自訂。

使用者對自訂系統的觀點

您可以自訂系統，以協助使用者完成其日常工作。爲能自訂最適合使用者使用的系統，請思考他們需要哪些事物才可順利完成工作。您可以自訂系統，使其以多種方式來顯示功能表與應用程式：

顯示使用者想看到的內容

多數人會安排整理自己的桌子與辦公室，以便能輕鬆取得常用的事物。請用相同的觀點來看待使用者對系統的存取。在登入系統後，使用者應該先看到最常使用的功能表或顯示器。您可以藉由設計使用者設定檔，輕易達成此目的。

汰除不必要的內容

大部份的系統上會有許多不同的應用程式。但多數使用者只想看到工作上所需的事物。限制他們只使用少數系統功能，將可簡化其工作。透過使用者設定檔、工作說明及適當的功能表，您就可爲每位使用者提供專用的系統環境。

將事物傳送到正確處所

使用者不應該擔心如何讓報表送達正確的印表機或如何執行批次作業。系統值、使用者設定檔和工作說明即可負責解決這些事項。

提供輔助

不論系統自訂的再完善，使用者仍會問「我的報表在哪裡？」或者「我的工作執行了沒有？」。**作業輔助程式**顯示器提供有簡單的系統功能介面，可協助使用者找出這些問題的答案。不同版本的系統顯示器 (稱爲**輔助層次**) 可爲技能層次不同的使用者提供協助。當您的系統送達時，即已內建適用所有使用者的「作業輔助程式」顯示器。不過，您的應用程式在設計上可能會要求您變更使用者存取「作業輔助程式」功能表的方式。

iSeries 提供有相關的系統工具，可讓您自訂系統安全，以便在使用者存取您的資源時加以保護。

用於安全和自訂作業的系統工具

爲能有效地進行規劃，您必須充份瞭解自己的安全目標與系統所提供之工具兩者間的關聯。這些系統工具可用來自訂您的系統安全。

安全層次

IBM 在交付所有新的 iSeries 時已將安全層次設爲 40。安全層次 40 可提供密碼與資源安全以及系統整合。若想變更系統作用中的安全層次，您可以變更 QSECURITY 系統值。不過，IBM 強烈建議您最好將安全層次訂在 40。若要變更安全層次，使用者須有 *SECOFR 使用者類別或 *ALLOBJ 與 *SECADM 特殊權限。

本系統具備四種安全層次，如下表所示：

表 1. 系統上的安全層次

安全層次	說明
安全層次 20	僅提供密碼安全。
安全層次 30	提供密碼與資源安全。
安全層次 40	提供密碼與資源安全；整合性安全。
安全層次 50	提供密碼與資源安全；強化整合性保護。

主題《選擇您的安全層次》會詳述如何決定最適合您需求的安全層次。

系統值

您可以設定系統值來控制特定作業系統功能在 iSeries 上的運作方式。系統值可視同公司政策。因爲系統值適用於每個使用系統的人員，除非有特殊狀況 (如使用者設定檔) 才可置換系統值。

系統值可決定多種事項，例如主要的印表機、系統如何顯示日期以及多久需要變更密碼等。

網路屬性

網路屬性可定義系統與其他電腦 (包括些個人電腦) 通信時的某些性質。網路屬性適用於整個系統。

群組設定檔

群組設定檔可定義一群使用者。群組設定檔就如同部門政策。您可以將群組設定檔作爲樣版，用於建立個別的使用者設定檔。它也可用來定義群組成員對系統物件的存取權限。有關群組設定檔的詳情，請參閱主題《規劃使用者群組》。

使用者設定檔

使用者設定檔是系統上最具威力且用途最廣的物件之一。其中包含諸如使用者密碼以及使用者登入後所見到的功能表等事項。使用者設定檔可定義人員在系統上可以及不可以執行的事項。它會決定使用者對系統的獨特觀點。主題《規劃使用者安全》即在討論使用者設定檔的規劃秘訣。

工作說明

工作說明可運用系統值與使用者設定檔，來決定系統如何處理使用者的工作。工作說明會設定使用者的起始檔案庫清單，進而決定使用者登入後所能存取的檔案庫。

資源安全

安全主管可藉由決定誰有權使用資源以及使用者如何存取此類物件，來保護系統上的資源 (物件)。安全主管可設定個別物件或物件群組的物件權限 (授權清單)。雖然檔案、程式和檔案庫是最常需要保護的物件，不過系統安全允許您針對系統上的任何物件設定物件權限。

如果事先規劃好全面且直接的相關措施，您就能簡單有效地管理資源安全。未經規劃的資源安全保護方法易流於複雜且沒有效率。主題《規劃資源安全》即在討論如何規劃您的資源安全。

系統已提供數種工具，來協助您設計直接可行的資源安全保護方法：

- **群組設定檔**：您可以將類似的使用者劃分在同一個群組設定檔下。讓這個使用者群組共用相同的物件權限。
- **授權清單**：您可以將具有類似安全需求的物件劃分在同一個清單中。如此即可授權給整個清單，不用單獨授權給個別物件。
- **物件所有權**：系統上的每個物件都有其擁有者。群組設定檔或個別使用者都能擁有物件。適當分派物件所有權將有助於您 (1) 管理應用程式，以及 (2) 委派資訊安全責任。
- **主群組**：您可以針對物件指定主群組權限。系統會將主群組權限與物件一起儲存。使用主群組權限將可簡化您的權限管理作業，並增進權限檢查效能。
- **檔案庫權限**：您可以將需要保護的檔案與程式放入檔案庫中，再限制對此檔案庫的存取。此種作法較限制個別物件的存取來得簡易。若要保護重要物件，您最好同時保護物件與檔案庫。
- **物件權限**：倘若對檔案庫的存取限制仍嫌不足，您還可限制個別物件 (例如檔案) 的存取權限。
- **公用權限**：就每一物件而言，您都可爲任何對此物件不具其他權限的系統使用者，定義可用的存取權限。公用權限在保護不具機密的物件上是一個相當有效的方式，且能提供良好的系統效能。
- **目錄權限**：目錄權限的使用方式與檔案庫權限相同。您可以將物件劃分在某一目錄下，進而保護整個目錄而非個別物件。
- **權限儲存器**：當您刪除物件時，也會一併刪除物件的權限資訊。對於遭到刪除並由應用程式再次建立的程式定義檔案，權限儲存器即可保存其權限資訊。您可以利用權限儲存器來輔助 System/36 的移轉作業。

安全工具

安全工具可協助您管理及監督 iSeries 的安全環境。您還可利用使用者設定檔工具來協助您：

- 查明哪些使用者設定檔具有預設密碼。
- 將使用者設定檔排定在每天或每一週特定時間上無法使用。
- 排定使用者設定檔於員工離職時即予移除。
- 查明哪些使用者設定檔具有特殊權限。
- 查明誰對系統上的物件採用權限。

物件安全工具可用來追蹤機密物件的公用與專用權限。您可以定期 (例如，每個月) 列印這些報表，協助您將安全工作重點放在最新的議題上。也可執行報表，使其只顯示距上次執行後所變更的內容。

具有監督能力的其他工具：

- 觸發程式
- 通信登錄、子系統說明、輸出佇列、工作佇列及工作說明中的安全相關值。
- 受到改變或干擾的程式

現在您已瞭解系統安全的重要性，下來請複查本主題作爲範例的規劃方法說明。

規劃基本系統安全的方法

您應該以從外向內、從一般到特定的方式來規劃安全。以規劃使用者設定檔爲例，應先思考使用者該看到哪些內容 (從外)。然後是決定如何加以實現 (向內)。

您首先要規劃系統值與群組設定檔 (一般)，然後再決定個別使用者的不同狀況 (特定)。

請依序完成『規劃使用者安全』的各項作業。它們會提供一個邏輯化的進程，來說明您要如何計畫使用您的系統，並決定如何加以保護及自訂。在這些主題中，請使用規劃工作表來提供有關安全決策與施行方面的記錄。請務必將這些規劃表存放在安全的處所。您在各主題中利用規劃工作表所蒐集的資訊，可於稍後協助您設定安全機能。

在規劃及設計系統安全時，您必須從頭作起。以最基本的安全機能爲開頭，再逐步處理較複雜的安全議題。從系統的實體安全著手，再進行說明您的應用程式與系統值。最後，您必須考量系統上的使用者與物件的安全。

在這些規劃主題中，您都可找到相關範例，範例中一家典型的公司 JKL Toy Company 即採行所描述的作法。雖然這是一家虛構的公司，但足可代表眞實世界中的許多企業。主題《範例：JKL Toy Company 簡介》即在描述此家範例公司。

範例：JKL Toy Company 簡介

範例可讓事物更加淺顯易懂。因此，本主題將以 JKL Toy Company 作爲範例。JKL Toy Company 是一家快速成長中的小型玩具製造商，正要在 iSeries 系統上設定安全機能。該公司總裁 John Smith 希望其新的 iSeries 系統可舒緩 JKL Toy Company 因爆炸性成長所帶來的負擔。

John 特別指派會計經理 Sharon Jones 出任系統管理員與安全主管。她必須確保整個安裝作業的順遂，包括安全機能。Sharon 深信規劃的重要。雖然該公司現在仍是小型企業，而且多數員工皆可存取大部份的資訊。但是 Sharon 知道，這些情況會隨著公司的成長不斷改變。她想在一開始就把事情作好。

開始時，JKL Toy Company 打算在系統上執行下列應用程式：「客戶訂單」、「庫存控制」、「合約與計價」及「應收帳款」。當您在閱讀相關的規劃主題時，將會學到更多關於 JKL Toy Company 處理安全機能的方式。

主題《規劃處理的步驟》即在說明規劃系統安全時應遵循的各個步驟。

安全規劃處理的相關步驟

下圖所示爲規劃處理的各個步驟，以及該步驟與其餘處理作業的關連。

表 2. 安全規劃處理的相關步驟

步驟	您在此步驟中的行動	此步驟與其他步驟的關連
規劃實體安全	說明您打算要如何保護主機、裝置及備份媒體。	此種資訊多半與其餘處理無關。您並不需要將實體安全規劃資訊輸入系統；不過，您需要一些此類資訊來規劃系統值與資源安全。
規劃您的應用程式	說明所有應用程式的用途、主功能表及檔案庫。	可爲其餘的規劃處理以及其他安全決策提供作業基準。此種資訊不需要輸入系統中。
規劃您的整體措施	決定您對安全事宜的整體措施。選擇可支援該措施的系統值。	可使用您的應用程式規劃資訊來協助決定整體措施。您所選擇的系統值會影響您規劃使用者與群組設定檔的方式。
規劃使用者群組	決定如何將使用者劃分成群組。決定每一個群組的性質，以及如何在系統上加以定義。	可使用您的應用程式說明來決定系統上的群組。您所定義的使用者群組會影響您在系統上規劃個別使用者的方式。
規劃個別使用者設定檔	將每一個系統使用者指派給某個群組。定義每一個使用者，包括與該群組其餘使用者不同的性質。例如，使用者需要不同於群組其餘成員的權限，來存取應用程式或檔案庫。	可使用應用程式規劃與使用者群組規劃資訊來協助定義個別使用者。
規劃資源安全	決定應將哪些應用程式開放給系統上的每個人使用。如須限制某些應用程式，則決定要允許哪些使用者或群組可加以使用。	可使用應用程式規劃與群組設定檔資訊來協助規劃資源安全。
規劃您的應用程式安裝	決定如何建立應用程式檔案庫的所有權與公用權限。	可使用資源安全規劃資訊來規劃您的應用程式安裝作業。

您應該從規劃使用者安全來展開安全規劃處理。

第 4 章 規劃使用者安全

規劃使用者安全係指規劃所有會影響系統上的使用者的安全事務。其間您必須說明下列事項：

實體安全

實體安全意指保護您的 iSeries 使其不致遭受意外 (或故意) 損壞與竊盜。此外，還包括所有的工作站、印表機和儲存媒體。《規劃實體安全》載有關於規劃實體安全、風險及 IBM 建議事項的進一步資訊。

應用程式安全

應用程式安全旨在處理哪些應用程式應儲存至系統上，以及如何保護這些應用程式而同時讓使用者加以存取。《規劃應用程式的安全》載有關於說明應用程式及其命名慣例的詳情。

整體安全策略

規劃您的整體安全意指擬訂安全計劃，同時考量您目前的業務狀況以及未來的計劃。《規劃您的整體安全策略》載有關於決定安全原則、安全層次、密碼注意事項及系統值的進一步資訊。

使用者群組安全

使用者群組是一群須以相同方式使用相同應用程式的使用者。規劃使用者群組安全涉及決定打算使用系統的工作群組，以及此類群組的應用程式需求。《規劃使用者群組》載有關於辨識使用者群組、規劃群組設定檔、選擇系統值及決定使用者環境的詳細資訊。

個別使用者安全

決定好所需的使用者群組後，您即可規劃需要的個別使用者設定檔。《規劃個別使用者設定檔》載有關於系統使用者命名、決定個別使用者責任及選擇系統值的進一步資訊。

這些主題中皆列有相關規劃套表的鏈結，供您用於記錄規劃決策。

規劃實體安全

當您準備安裝 iSeries 時，應藉由詢問下列問題來建立實體安全計劃：

- 主機要放置在何處？
- 各顯示站要安放在何處？
- 印表機要安放在何處？
- 還需要哪些額外設備，例如配線、電話線、家俱或儲存區？
- 您要採取哪些措施來防止系統發生緊急狀況，例如失火或斷電？

實體安全應列入您的整體安全規劃的一部份。取決於您放置系統及其裝置的處所，您可能會需要特殊措施來加以保護。

您可以用「實體安全規劃」套表來記錄有關系統實體安全方面的決策。爲確保您已慮及實體安全的各個層面，請複查下列主題：

- 主機的實體安全，提供系統本身的相關安全詳情。

- 系統文件與儲存媒體的實體安全，內含如何保護系統文件與儲存媒體的相關資訊。
- 工作站的實體安全，討論如何保護工作站。
- 印表機與印表機輸出的實體安全，提供如何實際保護印表機及其輸出的詳情。
- 規劃您的安全原則，說明如何編訂使用者準則與安全原則。

每一部主機皆設有控制面板供維修機器及執行特殊系統作業之用，例如開啓和關閉系統電源。爲防止有人未經授權而執行此類系統作業，各主機皆配有按鍵鎖定開關或電子閂鎖。這些機制雖可對主機提供局部保護，但按鍵鎖定開關或電子閂鎖並不足以承擔整個實體安全。

主機的實體安全

iSeries 並不需要具有特殊環境控制的電腦室。反之，您經常會發現主機是位於人來人往的辦公室中。客戶就是喜歡 iSeries 的小尺寸與容易維護；不過，這些特性也會招致安全上的風險。例如，別人可以輕易地竊走主機或從中取走高價元件。

因此您應該設法確保將主機放置在安全的場所。而最好的地點是一個專用且上鎖的房間。不然，至少應將主機放在下班後可上鎖的地方。

主機的相關風險

除了主機或其元件會遭竊外，下面是一些因主機實體安全不足而可能發生的其他風險：

意外妨礙系統作業

許多安全問題主要是來自經過合法授權的系統使用者。假設系統上有某一個顯示站遭致鎖定。而系統操作員正在開會不在其位置上。此時工作受阻的顯示站使用者走向主機，心理想著「或許我按下這個按鈕，一切就會恢復正常」。不過，那個按鈕可能會在仍有許多工作正在執行的情況下，關閉或重新載入系統。於是您還得花上數小時時間來救回已局部更新的檔案。此種險狀可透過主機按鍵鎖定開關來防範。

使用專用服務工具 (DST) 功能來繞過安全機制

安全機能並不管制系統所執行的服務功能，因爲當您需要執行此類功能時，您的系統軟體可能會無法正確運作。而知曉或能夠猜出「服務工具」使用者 ID 和密碼的老手，將會對您的系統造成嚴重損壞。若要進一步瞭解「服務工具」，請參閱「資訊中心」下的服務工具主題。

建議

- 最好將您的主機放在上鎖的房間中。不然，至少放在外人無法出入之處。此外，所選擇的場地應有專人負責監督。下面的實體安全特性可協助您防範系統遭致有意或無意的干擾：
- 使用電子閂鎖或按鍵鎖定：
  - 若想能夠啓動系統而不需使用鑰匙，可將作業模式設成「正常」。
  - 若打算使用「自動開關」功能來啓動或關閉系統，可將作業模式設成「自動」。
  - 取下鑰匙並存放在安全的處所。
- 安裝好系統後以及服務人員加以使用後，立即變更「服務工具 (DST)」的使用者 ID 和密碼。「資訊中心」下的服務工具主題會進一步說明如何執行此項作業。

在您開始規劃系統文件與儲存媒體的實體安全之前，您可以先行參閱 JKL Toy Company 的主機安全計劃範例。

範例：JKL Toy Company 的實體安全規劃套表--主機部份

下列範例是 Sharon Jones 在系統上使用的實體安全規劃套表的主機部份：

表 3. JKL Toy Company 的實體安全規劃套表：主機範例

實體安全規劃套表	
準備人員：Sharon Jones	日期：9/2/99
主機：	
說明保護主機的安全措施 (如：房間上鎖)：	主機在會計區。會計人員一律全天在此區域，可以監視主機。會計人員也負責處理零用金及重要記錄。下班時，會鎖住此區域。
一般使用的按鍵鎖定位置爲何？	正常
鑰匙的存放位置？	Sharon 辦公室內的小型保險箱內。
有關主機的其他說明：	主機存取容易。提醒會計區域人員提防人員篡改主機。

規劃主機的實體安全之後，您可以規劃系統文件及儲存媒體的實體安全。

系統文件與儲存媒體的實體安全

實體安全計劃的另一要務是處理如何存放重要系統文件與儲存媒體。系統文件包括 IBM® 隨系統所附的資訊、密碼資訊、規劃套表，以及系統所產生的任何報表。

隨著系統的不同，備份媒體可包括磁帶、光碟、磁片或 DVD 儲存體。系統文件與備份媒體應同時存放在您的辦公處所以及另一遠端位置。倘若發生災害，您將需要此資訊來回復系統。下面將建議一些方式供您用於儲存系統文件與儲存媒體。待您決定好方法後，將您的選擇記錄至實體安全規劃套表的「備份媒體與文件」部份。

妥善存放系統文件

服務工具與安全主管密碼對您的系統作業而言十分重要。您應記下這些密碼，並儲存在安全、機密的處所。此外，在其他地方保留一份這些密碼的記錄，可協助您從災害中回復。

考慮將其他重要系統文件，例如配置設定與主要應用程式檔案庫，存放在辦公地點以外的地方，以便在發生災害時協助您重建。

妥善存放您的儲存媒體

當您安裝系統時，應擬訂計劃以便定期將系統上的所有資訊儲存至磁帶或其他儲存媒體上。這些備份內容可讓您在必要時回復您的系統。您也應將這些備份內容妥善存放在其他安全之處。

風險

- 備份媒體損壞：如果發生災害或有人破壞您的系統備份媒體，您將無法回復系統上的資訊，只能藉助列印的報表。
- 備份媒體或密碼遭竊：您的備份媒體上可能存有機密的商業資訊。而箇中老手可用其他電腦來重建此資訊，再加以列印或處理。

建議

- 將所有密碼及備份媒體存放在可上鎖且防火的櫃子中。
- 定期 (例如至少每週一次) 將備份媒體的複本存放在其他安全之處。

您最好先參閱 JKL Toy Company 的系統文件儲存計劃範例，然後再開始規劃工作站的實體安全。

範例：JKL Toy Company 的實體安全規劃套表--備份媒體及文件部份

JKL Toy Company 的 Sharon Jones 完成了實體安全規劃套表的「備份媒體及文件」部份，請參閱下表：

表 4. JKL Toy Company 的實體安全規劃套表：備份媒體及文件範例

實體安全規劃套表	
準備人員：Sharon Jones	日期：9/2/99
備份媒體及文件：	
企業存放備份磁帶的位置？	放在大型防火保險箱內。
工作區外存放備份磁帶的位置？	放在公司會計人員辦公室的防火保險箱內。
安全主管、服務程式及 DST 密碼的保存位置？	放在 John Smith 辦公室中的保險箱內。
重要系統文件 (如：序號及配置資料) 的保存位置？	放在離站會計人員辦公室中的大型保險箱內。

規劃儲存體及文件安全之後，您可以規劃您的工作站的實體安全。

規劃工作站的實體安全

在大多數情況下，您會希望使用者能在任何可用的工作站上登入並執行所有已授權的功能。不過，如果您的工作站屬於非常公用或專用，您最好採行特殊的預防措施。例如，可記憶按鍵動作的顯示站以及個人電腦皆需要特殊考量的。本段落將協助您完成實體安全規劃套表的第 2 部份 (工作站與印表機的實體安全)。

工作站的相關風險

使用公用位置的工作站進行未授權作業

如果外人可以輕易進出公司內部場所，他們極可能會看到機密資訊。如果系統使用者登入後離開工作站，外人即可接近並取走機密資訊。

使用專用位置的工作站進行未授權作業

放置在極私密場所的工作站可讓入侵者長時間進行破解而不被發現。

在顯示站上利用播放功能或 PC 登入程式來破解安全措施

許多顯示站皆具有記錄及播放功能，供使用者儲存常用的按鍵順序，並藉由按下單一按鍵來加以重複執行。使用個人電腦作爲 iSeries 系統的工作站時，您可以撰寫程式將登入作業自動化。由於使用者經常用到登入處理，他們可能會決定儲存其使用者 ID 和密碼，而非每次登入時重新鍵入一次。

建議

在設定工作站的實體安全時，請考慮下列建議事項：

- 儘可能避免將工作站放置在極公開或私密的位置。
- 對系統使用者強調離開工作站前即應登出的重要性。您應該將登出程序納入安全原則中。

- 強調將密碼儲存在顯示站或 PC 程式中的行爲違反系統安全原則。您應將記錄密碼資訊的規定納入安全原則。
- 透過非作用中計時器系統值 (QINACTITV 與 QINACTMSGQ) 方法，來防範使用者離開公用位置之工作站卻未登出系統的情形。
- 藉由僅允許具有有限權限的使用者可使用公用工作站，來限制使用者可在公用工作站上執行的功能。
- 防止具有安全或服務權限的使用者於專用工作站上登入。使用 QLMTSECOFR 系統值來控制使用者透過此類權限進行登入的處所。
- 限制使用者不得同時在多個工作站進行登入。使用能夠限制裝置階段作業的系統值 (QLMTDEVSSN) 來控制使用者的登入處所。

若要使這些建議事項生效，請參閱主題《選擇會影響登入的系統值》與《規劃工作站的資源安全》，以瞭解相關詳情。

對實體安全規劃套表而言，您必須界定哪些工作站易因所在實體位置而召致風險。您最好參考相關範例，瞭解 Sharon Jones 如何規劃 JKL Toy Company 的工作站實體安全。

規劃好工作站安全後，您即可規劃印表機與印表機輸出的實體安全。

印表機與印表機輸出的實體安全

一旦資訊開始進行列印，系統安全機能就無法控制它會被哪些人所看到。爲降低有人看到敏感商業資訊的機會，您應保護印表機與印表機輸出。此外還必須訂立相關原則來因應商業機密資訊的列印。

印表機與印表機輸出的相關風險

以下風險可能會出現在您的業務狀況中。這些都是有關印表機與印表機輸出的最常見安全風險。不過，您仍應探究是否有其他風險存在於您專有的業務狀況中。

- 位於公用位置的印表機可能會使未經授權的人員便於存取機密資訊。
- 隨意放在桌上的印表機輸出可能會洩漏資訊。
- 您的系統可能只擁有一到兩台印表機。而您可能需要列印寶貴或機密的資訊 (例如薪資單)，供公司員工使用。

建議

下列建議事項可協助您減少有關印表機與印表機輸出方面的安全風險。

- 對系統使用者強調保護機密印表機輸出的重要性。將有關印表機的實體安全決策納入安全原則中。
- 避免將印表機放在公用位置。
- 安排高度機密輸出的列印時程，並由獲得授權的人員在印表機進行列印時負責在旁看守。

《規劃印表機與印表機輸出的安全》將會討論有關處理機密印表機輸出的建議事項。

在您開始規劃您的安全原則前，最好先參閱 JKL Toy Company 的印表機安全計劃範例。

範例：JKL Toy Company 的實體安全規劃套表--工作站及印表機部份

下列範例是 Sharon Jones 在 JKL Toy Company 中使用的「實體安全規劃」的第 2 部分：

表 5. JKL Toy Company 的實體安全規劃套表：工作站及印表機範例

實體安全規劃套表			2 / 2
工作站及印表機的實體安全			
工作站或印表機名稱	它的位置或說明	安全暴露	採取的保護措施
DSP06	裝載處	過於公開	自動登出。限制可以在工作站上完成的功能。
DSP09	客戶服務台	過於公開	自動登出。限制可以在工作站上完成的功能。
RMT12	遠端行銷辦事處	過於隱密	不讓安全主管登入。
PRT02	會計，靠近主機	可以看見重要資訊，如：價格清單	派人監督印表機輸出

完成實體安全規劃套表後，請繼續執行規劃您的安全原則主題。

規劃您的安全原則

如能對所有員工發佈安全準則，強調有關實體與系統安全的公司政策，對您將有極大助益。對於以後才新增至系統的新使用者，您也可提供相同的準則。

在這些準則中，您應該納入一些一般指示，闡明如何保護系統安全，例如登出工作站以及不要共用密碼。此外，準則中還須包含您訂定的特定安全決策的相關資訊。

當您閱讀本文件時，請寫下您在本身的安全準則中應包含哪些要點。而且最好就您的安全原則記錄其重點。

例如，JKL Toy Company 的 Sharon Jones 在規劃系統的實體安全時，就爲其安全準則記錄了以下要點：

務必對裝載處、客服部門、及遠端業務處要求登出。會計人員要看守主機。

待您填妥實體安全規劃套表後，即可開始規劃應用程式的安全。

規劃您的應用程式安全

若要爲您的應用程式規劃正確的安全機能，您必須知道：

- 您要在系統上儲存何種資訊？
- 誰須存取此資訊？
- 人員應具備何種存取權限？他們是否須變更資訊或只是加以檢視？

當您讀過這些應用程式規劃主題時，就可回答第一個問題，也就是要在系統上儲存什麼資訊。接下來，決定誰需要該資訊以及人們需要哪種存取權限。雖然您不用將應用程式規劃資訊輸入系統；不過，當您在設定使用者與資源安全時都需用到它。

何謂應用程式？

在應用程式安全的第一個規劃步驟中，您必須說明要在系統上執行的應用程式。所謂應用程式是一群在邏輯上彼此互屬的功能。以 JKL Toy Company 爲例，輸入訂單、出貨及列印發票等都是「訂單處理」應用程式的一部份。

一般而言，您的 iSeries 會執行兩種類型的應用程式：

- **商業應用程式**：外購或自行開發以執行特定商務功能 (例如訂單處理或庫存管理) 的應用程式。
- **特殊應用程式**：您提供用來在公司中執行各類與商務程序無關的應用程式。

您需要哪些套表？

請使用下列套表來協助您規劃應用程式安全：

- 應用程式說明套表
- 檔案庫說明套表
- 命名慣例套表

若要列印這些套表，請先按一下相關鏈結，再選取正確的頁框，然後按一下瀏覽器中的**列印**圖示。

閱讀下列資訊，以協助您填妥這些規劃套表。

- 說明您的應用程式
- 說明命名慣例
- 說明檔案庫資訊
- 繪製應用程式圖解

說明您的應用程式

此時，您必須蒐集一些關於您的各種商業應用程式的一般資訊。按下述方式，將您的應用程式相關資訊新增至應用程式說明套表的適當欄位。稍後，您可以用此資訊來協助您規劃使用者群組與應用程式安全：

應用程式名稱與縮寫

爲應用程式指定簡短的名稱與縮寫，可作爲填寫各類套表速記之用，或用來爲應用程式所用的物件命名。

說明資訊

扼要說明應用程式的功用。

主功能表與檔案庫

界定哪個功能表是存取應用程式時所用的主功能表。指明該功能表所在的檔案庫。主功能表多半會通往具有特定應用程式功能的其他功能表。使用者喜歡在登入系統後，立即看到其主要應用程式的主功能表。

起始程式與檔案庫

應用程式有時會執行起始程式，來設定使用者的背景資訊，或執行安全檢查。若應用程式具有起始程式或設定程式，請將其列於套表上。

應用程式檔案庫

每支應用程式通常會有用來存放檔案的主檔案庫。請列出應用程式所用的全部檔案庫，包括程式檔案庫與其他應用程式所擁有的檔案庫。例如，JKL Toy Company 的客戶訂單應用程式即使用庫存檔案庫來取得料品餘額與說明。

您可以利用檔案庫與應用程式之間的關係，來決定需存取各種檔案庫的人員。

尋找關於應用程式的資訊

如果尚不清楚所需的應用程式相關資訊，您便須洽詢您的程式設計師或應用程式供應商。

如果您無權存取關於系統所執行之應用程式的資訊，可用下列方法自行加以蒐集。

- 應用程式使用者或許能告訴您主功能表與檔案庫的名稱，要不然您可觀看其登入系統。
- 若使用者在登入後立即見到應用程式，請查看其使用者設定檔的**起始程式**欄位。此欄位含有該應用程式的起始程式。您可用 DSPUSRPRF 指令來檢視此起始程式。
- 您可列出系統上所有檔案庫的名稱與說明。請使用 DSPOBJD *ALL *LIB。如此即會顯示系統上所有的檔案庫。
- 您可以在使用者執行應用程式時，觀察作用中的工作。請用具備中階輔助層次的「處理作用中的工作 (WRKACTJOB)」指令，來取得關於交談式作業的詳細資訊。顯示相關工作並觀看其檔案庫清單及其物件鎖定，以查明所用的檔案庫。
- 您可用「處理使用者工作 (WRKUSRJOB)」指令，來顯示應用程式中的批次工作。

爲確保蒐集到您規劃應用程式安全時所需的全部資訊，請先完成下列作業後再繼續進行：

- 針對您的每種商業應用程式，完成「應用程式說明」套表。填妥整份套表，保留安全需求區段。該區段將用來規劃應用程式的資源安全，如主題《規劃資源安全》所述。
- 必要時，爲每支特殊的應用程式準備一份「應用程式說明」套表。此套表可協助您決定如何提供應用程式的存取權限。

註: IBM 的特殊應用程式，例如 IBM Query for iSeries，並不一定需要「應用程式說明」套表。存取此類應用程式所使用的檔案庫並不需要任何特別規劃。不過，蒐集其資訊並準備相關套表將極有助益。

在您進行說明命名慣例前，最好先參閱 JKL Toy Company 的「應用程式說明」套表範例。

範例：JKL Toy Company 的應用程式說明套表

Sharon Jones 在「應用程式說明套表」中列出公司所有的應用程式及縮寫。她也簡短說明使用者如何使用這些應用程式。

客戶訂單 (CO)

訂單的輸入、追蹤及出貨。列印發票。

庫存控制 (IC)

成品及物料的庫存管理層次。處理所有的庫存轉移。

合約與計價 (CP)

管理客戶的特殊計價與合約。

應收帳款 (AC)

追蹤目前的餘額。列印每月的報告單。

下表是 Sharon Jones 說明「客戶訂單」應用程式。她很有系統地準備套表，先從一個應用程式開始，然後再說明其餘的應用程式。

表 6. JKL Toy Company 的應用程式說明套表：範例

應用程式說明套表	
準備人員：Sharon Jones	日期：9/3/99
應用程式名稱：客戶訂單	縮寫：CO
應用程式的簡短說明：	輸入客戶訂單、出貨前的追蹤、訂單出貨，以及列印發票和出貨單。
主功能表名稱：COMAIN	檔案庫：COPGMLIB
起始程式名稱：NA	檔案庫：NA
列出應用程式使用的檔案庫及程式庫： • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
定義應用程式的安全目標，如：是否有機密資訊：	

除了「客戶訂單」應用程式之外，Sharon Jones 也爲 JKL Toy Company 系統上的這些的應用程式準備了「應用程式說明套表」：

- 庫存控制
- 合約與計價
- 應收帳款

接下來，您可以爲系統中的物件說明命名慣例。

說明命名慣例

當您知道系統是如何爲物件命名後，便能夠規劃及監督安全、解決問題、規劃備份及回復作業。大部份的應用程式對於指派名稱給物件 (例如檔案庫、檔案及程式) 皆訂有相關規則。如果您的應用程式是取自不同的來源，它們可能各有獨特的命名系統。

請務必在命名慣例套表上記錄所有應用程式與物件的命名慣例。請在「命名慣例」套表上，列出應用程式在爲檔案庫與檔案命名時所用的規則。您最好用空白行來記錄其他命名慣例，例如程式與功能表。如果您的應用程式是取自不同的來源，它們可能各有獨特的命名慣例。請說明各應用程式的命名慣例。您可能需要準備一份以上的「命名慣例」套表。

在您開始說明檔案庫資訊之前，最好先參閱 JKL Toy Company 的系統物件命名慣例範例。

範例：JKL Toy Company 的命名慣例套表

下表僅顯示檔案庫及檔案的命名慣例。您還需要說明系統中其他物件類型的命名慣例。「命名慣例套表」中只有一些一般物件，您可能還需要準備其他物件。

表 7. JKL Toy Company 的命名慣例套表：範例

命名慣例套表

表 7. JKL Toy Company 的命名慣例套表：範例 (繼續)

準備人員：Sharon Jones	日期：9/3/99
物件類型	**命名慣例**
檔案庫	檔案庫中的檔案庫名稱檔案名稱是有意義的，如：CONTRACTS 或 ITEMLIB。程式庫使用應用程式縮寫加上 PGMLIB，如：ICPGMLIB。
檔案	主要檔案的名稱是有意義的，如：CUSTMAST 代表「客戶主要檔案」，ITEMMAST 代表「項目主要檔案」。其他應用程式檔案 (僅程式設計師瞭解使用原因) 則是使用應用程式縮寫加上 FILE 及一個數字來命名，如：ICFILE14。

完成命名慣例套表後，您就可以開始說明檔案庫資訊。

說明檔案庫資訊

說明命名慣例後，您應說明系統上的檔案庫。檔案庫可用來識別及組織您系統上的物件。將類似檔案集中放入同一檔案庫，可讓使用者便於存取重要的應用程式與檔案。您還可自訂使用者的權限，使其只能存取部份檔案庫。請針對各個應用程式，說明系統上的所有檔案庫。您將需要準備多份檔案庫說明套表。

註: 只填寫關於檔案庫的說明資訊。當您規劃檔案庫的資源安全時，再填寫「檔案庫說明」套表的其餘部份。稍後您需要將權限的相關資訊新增至檔案庫。有關如何填寫「檔案庫說明套表」剩餘部份的詳情，請參閱《規劃應用程式檔案庫的安全》。

繼續之前，請務必完成下列事項：

- 填寫「命名慣例套表」的檔案庫與檔案部份。
- 針對每個應用程式檔案庫，在「檔案庫說明」套表上填寫說明資訊。

在您繪製應用程式圖解之前，您最好參閱範例，瞭解 JKL Toy Company 的 Sharon Jones 如何說明檔案庫。

範例：JKL Toy Company 的檔案庫說明套表

下列兩個表格說明 JKL Toy Company 的「客戶訂單應用程式」使用的兩個檔案庫。第一個表格說明檔案庫，第二個表格說明程式庫。

表 8. JKL Toy Company 的檔案庫說明套表：檔案庫範例

檔案庫說明套表	
準備人員：Sharon Jones	日期：9/3/99
檔案庫名稱：CUSTLIB	描述性名稱 (文字)：客戶記錄檔案庫
簡短說明這個檔案庫的功能：	保存所有客戶檔案，包括訂單及應收帳款。

表 9. JKL Toy Company 的檔案庫說明套表：程式庫範例

檔案庫說明套表	
準備人員：Sharon Jones	日期：9/3/99
檔案庫名稱：COPGMLIB	描述性名稱 (文字)：客戶訂單程式庫
簡單說明這個檔案庫的功能：	保存客戶訂單應用程式的所有程式。

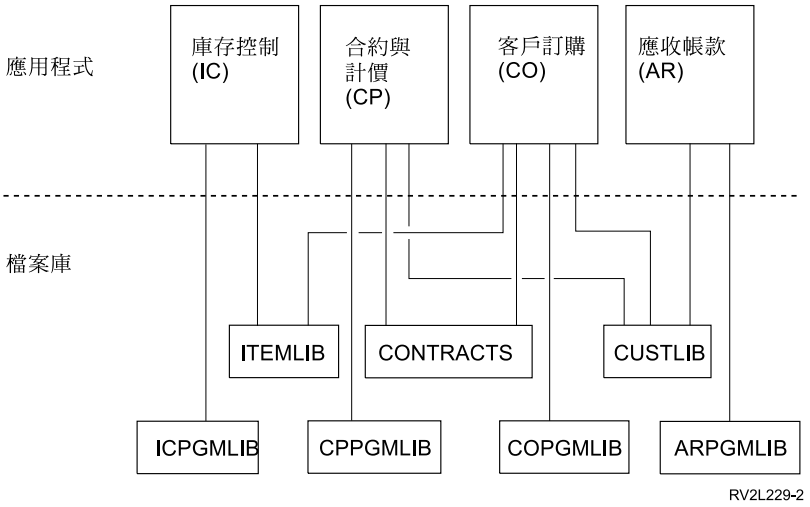
說明檔案庫後，您應該爲系統繪製應用程式圖解。

繪製應用程式圖解

當您準備「應用程式說明」套表與「檔案庫說明」套表時，若能繪製詳列應用程式與檔案庫之間關係的圖解將十分有用。圖解可以協助您規劃使用者群組與資源的安全。

下圖所示爲 Sharon Jones 就 JKL Toy Company 的應用程式與檔案庫所繪製的圖解：

JKL Toy Company 的應用程式與檔案庫圖解



此時開始蒐集一些關於應用程式與檔案庫的資訊，未來將可協助您完成許多安全方面的決策。它提供了一個很好的機會，讓您更加瞭解所用的系統與應用程式。

爲確保您蒐集到所需的應用程式資訊，您應該：
- 針對系統上的各個商業應用程式，填寫應用程式說明套表。
- 必要時，爲系統上的各種特殊應用程式準備一份應用程式說明套表。
- 填寫命名慣例套表的檔案庫與檔案區段。
- 爲各個應用程式檔案庫準備一份檔案庫說明套表。
- 將應用程式與檔案庫之間的關係繪成圖解。

完成這些套表後，即可開始規劃您的整體安全策略。

規劃您的整體安全策略

待您規劃應用程式的安全後，即可開始規劃整體安全策略。首先，您必須決定系統安全的整體措施。進行此類決策時，應妥善拿捏公司目前以及未來的需求。

本文可協助您進行規劃處理，以決定您的安全原則與目標。同時也可協助您選擇會影響所有系統使用者的基本系統值。

您需要哪些套表？

若要完成應用程式規劃，請使用系統值選項套表。

當您參閱相關主題以決定系統值時，應使用先前填妥的「實體安全計劃」套表與「應用程式說明」套表。

請複查下列主題，來規劃您的安全策略：

- 撰寫安全原則
- 選擇您的安全層次
- 選擇會影響登入的值
- 選擇會影響密碼的系統值
- 使用系統值來自訂您的系統

撰寫安全原則

在您開始進行規劃前，請先就系統安全事項準備一份公司政策聲明。此聲明是您與公司高層主管之間的協議。它將協助您制定決策，並訂出重要事項。您的安全原則應載明您所採取的整體措施，以及哪些資訊資產須加以保護。

每個系統都應具有安全機能。您可以採用下列安全措施之一：

- **嚴密**：有人稱此爲需知式安全保護方法。在嚴密的安全環境下，您授權使用者只能存取執行其作業時所需的資訊與功能。所有其他事項都排除在授權範圍之外。許多審核員皆推薦採用嚴密方式。
- **一般**：一般安全保護方法是根據您指派給使用者的權限，來讓使用者存取物件。
- **寬鬆**：在寬鬆式安全保護的環境下，您允許經授權的使用者存取大部份的系統物件。您會限制其對重要或機密資源的存取。單一部門或小型企業通常會採用寬鬆式安全保護。

您的整體措施可協助您制定關於特定安全需求的決策。您的系統安全措施應與您對存取公司資訊的理念相符。如果不確定要採用何種措施，請嘗試：

- 用您填妥的「應用程式說明」套表來決定誰應有權或無權存取這些應用程式。
- 檢查您的公司所用的技術。例如，若您打算將系統或網路連上 Internet，您會需要更具限制的安全環境，以保護系統不受外部 Internet 使用者干擾。
- 與其他組織成員 (例如安全審核員) 商討，來決定更深入的安全需求。

請記得，您可以隨時變更您的原則。大部份的企業會隨著成長而需要更嚴密的安全。本文可協助您設定一套安全保護方法，並允許您隨後加添其他安全機能，而不須作大量變更或重新測試您的應用程式。

要保護哪些內容

除了在安全原則中闡明您的整體安全措施外，您還必須界定貴公司的重要資訊資產。您的安全系統應針對保護此類資產來設計。您可根據以下數種基本要求來決定重要資產：

- **機密性**：不對一般公司人員開放的資訊。例如薪資就是機密資訊。
- **競爭力**：使您具有競爭優勢的資訊，例如產品規格及配方。
- **作業**：電腦上與您日常業務息息相關的資訊，例如客戶記錄與庫存餘額。

安全主管 Sharon Jones 與公司總裁 John Smith 合作編訂了一份有關安全原則的聲明。John Smith 即利用這些要點草擬了 JKL Toy Company 的安全原則。您可以參考其在規劃與設定安全機能後，JKL Toy Company 對所有員工所發佈的安全原則。請記得，當您閱讀這些規劃主題時，記下您要新增至安全原則中的事項。

表 10. JKL Toy Company 的安全原則：範例

整體措施

寬鬆式：多數人員須存取大部份資訊。

重要資訊

- 合約與特殊計價
- 薪資
- 客戶與庫存記錄僅開放給公司員工使用。

一般規則

- 每個系統使用者將具有使用者設定檔。使用者不得共用設定檔或密碼。
- 使用者每隔 60 天即須變更其密碼。

訂好安全原則的要點後，您即可選擇您的安全層次。

選擇安全層次

QSECURITY 系統值可讓您控制系統上所需的安全層次。若要瞭解安全層次的運作方式，可將您的系統視爲一棟建築物，而且有人嘗試從外面進入。

層次 20：密碼保護

如果選擇需求層次 20，您將擁有部份的安全保護。建築的警衛會要求身份識別與密碼。只有同時具備此兩者的人才可進入。但一旦進入後，他們可以隨處走動或做任何想做的事。

如果有人偷聽到密碼，並用它來通過警衛，就如入無人之境。

層次 30：密碼與資源安全

層次 30 除了提供層次 20 的所有機能外，還可讓您控制誰可以前往建築物中的特定處所，以及到達該處後可以做什麼動作。您可以將建築物的某些部份指定爲公用場所，其餘處所則由警衛管制進出。

您可以讓有權進出管制區的人做他們想做的任何事，也可以規定他們須向經過授權的詢問櫃檯 (程式) 提出要求。以他人密碼闖入者仍可通過內部警衛而到達管制區。

層次 40：整合性保護

在層次 40，您可以取得層次 30 的所有保護，不過系統還會驗證使用者的進出情形。建築內部的警衛會檢查密碼並登記所有進入管制區的使用者。

層次 50：進階整合性保護

在層次 50，警衛將採取更嚴格的措施，藉由確認登記者的身份，來防止有心人闖關。

建議

iSeries 出貨時已設定在安全層次 40。不論您的安全原則是嚴密、一般或寬鬆，對大部份的安裝系統而言，安全層次 40 是最佳的選項。如果採行寬鬆方式，您可對系統上大部份的資源設定公用權限。藉由一開始便啓用安全層次 40，您將具有足夠彈性讓系統在未來更加安全，而且不必執行許多變更。

如果您是外購應用程式，請先洽詢供應商以確定該程式已通過層次 40 的測試。部份應用程式所用的作業會在安全層次 40 造成錯誤。如果您的應用程式未作過層次 40 或 50 的測試，請由層次 30 開始設定。然後透過審核日誌來查看您的應用程式是否有記載權限失敗的情況。如果沒有，即可變更爲層次 40 或 50。

安全層次 50 可防範多數系統通常不會發生的事件。每當程式在您的系統上執行時，系統都會執行額外的檢查。不過此額外檢查可能會減損系統效能。

待您在系統值選項套表上輸入安全層次選項後，即可選擇會影響登入的系統值。

選擇會影響登入的系統值

在選擇安全層次後，您即可利用系統值來自訂使用者所能看到的顯示器內容，以及其與系統的互動方式。您將須規劃此類系統值，並用系統值選項套表來記錄您的選項。

下表將說明本主題中所用的系統值。

表 11. iSeries 系統值及其說明

系統值	說明
QMAXSIGN	限制連續登入嘗試次數。
QMAXSGNACN	指定若屆達連續登入嘗試次數時，系統應採取的行動。
QLMTDEVSSN	決定使用者是否可在多部工作站上以相同的使用者設定檔登入。
QINACTITV	決定系統何時對非作用中工作採取動作。
QINACTMSGQ	決定若交談式作業維持非作用中的時間長度達到在 QINACTITV 系統值所指定的值時，系統應採取的動作。
QDSCJOBITV	控制系統是否要以及何時結束暫時斷線的工作。
QLMTSECOFR	限制擁有系統上所有物件之權限的安全主管只能使用特定裝置。

限制登入嘗試次數 (QMAXSIGN 與 QMAXSGNACN)

有兩種系統值會決定某人嘗試登入您系統的次數，以及一旦到達限制次數後系統將執行的動作。

最大登入嘗試次數 (QMAXSIGN) 系統值可決定在系統採取行動前，所容許的連續錯誤登入嘗試次數。所謂錯誤登入嘗試是指某人試圖使用特定的使用者設定檔，但使用了無效密碼或沒有適當的工作站授權。

最大登入動作 (QMAXSGNACN) 系統值則會指定如果某人嘗試連續登入過多次時，系統應執行的動作。可能的值有：

1 防止再對裝置進行登入嘗試。又稱爲停用裝置。此時無人可登入該裝置，需要由獲授權的人員利用 WRKCFGSTS 指令來重新啓用該裝置。此選項通常不具足夠的保護能力，特別是在有人嘗試透過個人電腦或遠端系統登入您的系統時。

系統操作員或對該裝置具有 *USE 權限的任何人皆可重新啓用該裝置。

2 可防止使用者設定檔的進一步登入嘗試。又稱爲停用使用者設定檔。沒有人可再透過該設定檔進行登入，要由獲授權的人員利用「變更使用者設定檔 (CHGUSRPRF)」指令重新加以啓用。

若要啓用使用者設定檔 (變更狀態)，您必須是具備該設定檔使用權限的安全管理者。

3 同時停用使用者設定檔與裝置。

風險與建議

有些搗蛋份子很喜歡猜測密碼和侵入系統。藉由限制登入嘗試次數，您便可對其猜測行爲設限。

最大無效登入次數 (QMAXSIGN) 系統值可決定您所允許的登入嘗試次數。將此數目設得夠高，可避免對使用者造成妨礙。如果將其設得夠低，則可避免發生打字錯誤情形，並讓入侵者無法進行多次猜測。您的最大登入嘗試次數應設在 3 到 5 之間。

所建議的最大登入動作 (QMAXSGNACN) 爲 3，雖然這會同時停用裝置與使用者設定檔，進而造成系統使用者的不便。位於專用位置的工作站會讓入侵者有機會試用多種不同的使用者設定檔與密碼組合。如果您的系統沒有任何會因所在位置而導致風險的工作站，只停用使用者設定檔可能即已足夠。

檢查您完成的「實體安全套表」。如果您有位於遠端位置的工作站或是擁有遠端使用者 (透過電話線路或 VPN 連線來存取您的系統之使用者)，您最好嚴格限制登入作業。請務必將您的 QMAXSIGN 與 QMAXSGNACN 選項新增至系統值選項套表的第 2 部份。

在選擇會限制使用者一次只能使用一部工作站的系統值之前，最好先參考範例，來瞭解這些系統值如何限制登入嘗試次數。

範例：限制登入嘗試: Sharon Jones 將登入嘗試次數限制爲 3 次 (QMAXSIGN 爲 3)，並選擇若超過此限制即同時停用設定檔與裝置 (QMAXSGNACN 爲 3)。以下是屆達這些值時所可能發生的情況：

1. Roger 連續兩次鍵入錯誤密碼。
2. 第二次嘗試後，他接獲訊息，警告他若再一次登入錯誤即會停用其使用者設定檔。
3. 他又犯了一次錯誤。
4. 系統停用了他的設定檔，且工作站不再顯示「登入」畫面。如果 Roger 嘗試在另一部工作站登入，他會收到錯誤訊息。
5. 現在他必須請 Sharon 啓用他的設定檔，然後才可重試。 Sharon 或系統操作員還必須重新啓用 Roger 的工作站。如果 Roger 不記得密碼，Sharon 可以給他一個臨時密碼，而他重新登入後必須加以變更。

接下來您可以複查會限制使用者一次只能登入一部工作站的系統值。

限制使用者一次只能使用一部工作站

「限制裝置階段作業 (QLMTDEVSSN)」系統值可決定同一使用者是否能同時在多部工作站上進行登入。可能的值有：

0 系統允許不限數量的使用者同時用相同的使用者設定檔進行登入。

1 一個使用者設定檔一次只能用於一個裝置。使用者可在同一裝置上擁有多個階段作業。

風險與建議

讓使用者一次只能登入一個工作站可建立良好的安全習慣。怠惰的安全習慣會召致安全風險：

- 限制使用者只能使用一個裝置，可減少共用使用者 ID 和密碼的情況。如果人們共用使用者 ID，您將會喪失控制權與評量能力。您將無法知道誰在系統上執行了哪些功能。
- 使用者在使用另一工作站前，必須記得先登出目前的工作站。如果工作站保持在登入狀態而且未作使用，將隨時可能發生安全風險。

系統值 QLMTDEVSSN 的建議設定是 1，它會限制使用者只能使用單一裝置。提供給每位系統使用者獨一的使用者 ID 和密碼以及適當權限，然後限制他們一次只能使用一部工作站。確定將您的 QLMTDEVSSN 選項新增至系統值選項套表的第 2 部份。

您現在可以開始規劃非作用中工作的系統值。

規劃非作用中工作的系統值

當使用者忘記登出工作站時，有三種系統值可共同決定系統所採取的因應動作。

非作用中工作逾時間隔 (QINACTITV)

QINACTITV 系統值可決定如果顯示器已登入但在指定時限內仍爲非作用中時，系統應採取的行動。

註: 非作用中係指使用者在指定時限內未按下 Enter 鍵或功能鍵。

非作用中工作訊息佇列 (QINACTMSGQ)

您設定的 QINACTMSGQ 系統值，可決定當屆滿您以系統值 QINACTITV 所指定的時限時，系統應採取何種動作。如果選取 ENDJOB，系統會結束已超過 QINACTITV 逾時間隔且未作用的任何工作。如果選取 DSCJOB，系統將把非作用中的工作斷線。如果指定訊息佇列的名稱，系統會在工作未作用的時間過長時，傳送警告訊息到該佇列。

當系統將工作站的工作**斷線**時，即會暫停該工作。而工作站會回到登入顯示器。當該系統使用者再次於同一工作站登入時，斷線工作即會回復。

斷線工作逾時間隔 (QDSCJOBITV)

QDSCJOBITV 系統值可控制系統是否會以及何時要結束已暫時斷線的工作。系統可根據 QINACTITV 與 QINACTMSGQ 系統值，自動將工作斷線。使用者也可利用「作業輔助程式」功能表的選項或「工作斷線 (DSCJOB)」指令，請求將其工作暫時登出 (斷線)。

風險與建議

如果 Sharon 忘記在離開前登出工作站，John 可以走近此工作站並執行 Sharon 權限範圍內的任何功能。

您之所以須管理非作用中顯示器的原因主要有二：

- 您訂有相當嚴密的安全保護環境，且系統上存有機密資訊。
- 您有一些工作站放在易爲外人進出的位置。

使用者常因職務所需而暫時中斷工作離開工作站。請善用此三種系統值，讓出現暫時中斷的情況時，系統仍受到保護。

爲消弭這些風險，IBM 建議合併使用 QINACTITV、QINACTMSGQ 及 QDSCJOBITV 三種系統值，以便允許正常的工作中斷且仍然保護您的系統安全。

非作用中工作逾時間隔 (QINACTITV)：合理縮短此間隔可減少發生工作站無人看管的情形，但勿過短以免造成使用者不便。建議設定爲 30 分鐘。當工作未作用達 30 分鐘，系統便會採取「非作用中工作訊息佇列」中所指定的動作。

非作用中工作訊息佇列 (QINACTMSGQ)：選擇將工作斷線。系統會將未作用時間達到「非作用中工作逾時間隔」時限的工作予以斷線。系統將暫停該工作並登出顯示器。當同一使用者再次登入時，工作即會回復到斷線前的狀態。

此作法對使用者較爲方便，因爲系統是暫停而非結束其工作。切斷未作用的工作和結束工作對保護系統而言效果相同。

註: 有些工作是系統無法斷線的。如果系統無法切斷某一未作用的工作，它會改而結束該工作。而這可能會造成資訊流失。請考慮設定 QINACTMSGQ 來傳送訊息至系統操作員訊息佇列。

斷線工作逾時間隔 (QDSCJOBITV)：鼓勵系統使用者須短暫離開工作站時應暫時登出系統，如須長時間中斷使用則應完成工作並登出。

在系統開始進行夜間處理作業 (例如「自動清除」) 前，以 QDSCJOBITV 來結束已斷線的工作。將其設成合理的時間長度，一則足供使用者在上班時間中回到工作站，一則可在夜間處理作業開始前結束工作。選擇 300 分鐘 (五小時) 較爲適宜，既可留下足夠時間完成夜間作業，亦不致干擾到使用者的工作。

註: 爲避免兩位使用者同時嘗試變更相同的資訊，系統在加以更新前會先**鎖定**記錄。當系統切斷使用者的工作時，任何資源鎖定仍保持有效。取決於您的應用程式設計以及系統使用者數目，此類鎖定有時會造成系統效能問題。請洽詢您的程式設計師或應用程式供應商，來決定鎖定功能是否會影響您的效能。

您最好先參閱範例，瞭解如何運用這些系統值來處理系統上的非作用中工作。

待您將有關非作用中工作的決策記錄到「系統值選項」套表後，便可決定如何限制安全主管的登入位置。

範例：使用 QINACTITV、QINACTMSGQ 及 QDSCJOBITV 系統值來處理非作用中工作: 假設您已將非作用中工作逾時間隔 (QINACTITV) 設定爲 30 分鐘。系統會切斷非作用中工作 (QINACTMSGQ 是 DSCJOB)。斷線工作逾時間隔 (QDSCJOBITV) 爲 300 分鐘 (5 小時)。例如，如果 Sharon 忘記在 9:30 a.m. 登出，系統會在 10:00 a.m. 切斷她的工作，並於 3:00 p.m. 結束該工作。

請在「系統值選項套表」的第 2 部份中，選擇系統值 QINACTITV、QINACTMSGQ 及 QDSCJOBITV。

在「系統值選項套表」中記下非作用中工作的決策後，接著您可以決定如何限制安全主管的登入位置。

限制安全主管的登入位置

對於有權變更安全及控制物件的使用者，您最好限制其只能使用某些工作站。如此可防止他們從遠端位置登入工作站而未讓您知曉。系統值 QLMTSECOFR (限制安全主管)

即可讓您達成此目的。如果將 QLMTSECOFR 設爲 1，則具備所有物件 (*ALLOBJ) 或服務 (*SERVICE) 等特殊權限的使用者，將只能在主控台或您指定的其他工作站來進行登入。

QLMTSECOFR 可限制安全主管 (有權使用系統上所有物件的使用者) 與服務人員只能使用主控台。您可以用「授予物件權限 (GRTOBJAUT)」指令來授予這些使用者存取其他裝置的權限。

註: 要讓 QLMTSECOFR 系統值有作用，您的系統安全層次須爲 30 或更高。

風險與建議

最好將 QLMTSECOFR 系統值設爲 1。即使有人竊聽或猜出具備安全主管設定檔者的密碼，他們還必須使用能允許其登入的裝置。

將您的 QLMTSECOFR 選項填入系統值選項套表的第 2 部份後，您即可選擇會影響密碼的系統值。

選擇會影響密碼的系統值

您應讓使用者自行指派其密碼，而不是由安全主管代爲指派。使用者在建立自己的密碼時，通常不須加以寫下。寫下的密碼常存放在明顯之處，因此也易召致安全風險。

建立密碼時的要訣

您的使用者可能會不知如何想出較好的密碼。此時可建議他們下列技巧：使用易記的句子來幫您建立不好破解的密碼。例如，休假過後您可用句子 ″July 4th fishing was poor (7 月 14 那天釣魚成績很破)″ 來建立密碼 J4FWP。

有一些系統值可用來管理密碼。您可以控制使用者多久即須變更密碼。此外您還可建立許多規則，防止使用易於猜出的密碼。在這些系統值中，有許多是適用於大型組織。只有少數適用於所有人。

透過 ASSIST 功能表的選項或「變更密碼 (CHGPWD)」指令，使用者即可自行指派密碼。當使用者變更自己的密碼時，系統會根據密碼系統值來檢查新密碼。但如果使用者是用 CHGUSRPRF 指令來變更密碼，系統將不會根據此安全系統值來檢查新密碼。

註: 如果您已設定任何密碼系統值，系統將不允許新密碼和使用者設定檔名稱相同，除非您是用 CHGUSRPRF 指令來設定密碼。

下表所示即爲影響密碼及其定義的各類系統值：

表 12. iSeries 密碼相關的系統值

系統值	說明
QPWDEXPITV	要求使用者在指定期間後變更密碼。
QPWDMAXLEN	可讓您指定密碼的最大字元長度。
QPWDMINLEN	可讓您指定密碼的最小字元長度。
QPWDRQDDIF	防止使用者替換使用兩個不同的密碼。

下列主題將提供有關此類系統值的進一步詳情：

- 決定密碼的可用期限

- 決定密碼的長度
- 限制重複的密碼

請在 CL 指令行中鍵入 WRKSYSVAL *SEC，即可在線上檢視開頭字元爲 QPWD 之系統值的相關資訊。

決定密碼的可用期限

QPWDEXPITV 系統值可決定使用者多久即須變更密碼。

接近密碼到期日時，系統會向使用者提出警告。如果密碼已到期，系統會在使用者下次登入時提示他們變更密碼。

建議

使用者應定期變更密碼。如此可減少與他人共用密碼的情形。再者，未經授權的使用者即使得知某人的密碼，也只能使用短暫的時間。密碼效期應妥善設定，若過短會干擾使用者，過長則會影響安全。要避免這些問題出現，效期最好訂在 45 到 60 天之間。

在系統值選項套表的第 2 部份輸入您的 QPWDEXPITV 系統值選項後，即可決定密碼長度。

決定密碼的長度

有些使用者並不喜歡打字。如果能夠選擇，他們寧可使用一個字母的密碼或姓名縮寫。不幸的是，簡短的密碼會讓入侵者更容易破解。QPWDMINLEN 系統值即可讓您設定您的系統上所有密碼的最小長度。

如果您的系統會與其他系統通信，使用者將可能在兩套電腦間交換密碼。某些通信方法會將密碼長度限制在 8 個字元以下。而 QPWDMAXLEN 系統值即可讓您指定密碼的最大長度。

建議

將密碼最小長度設爲 6。如此可防止有人使用縮寫，並鼓勵使用者更加愼選密碼。如果您的系統須與其他系統通信，請將最大密碼長度設爲 8。

在系統值選項套表的第 2 部份輸入了 QPWDMINLEN 與 QPWDMAXLEN 系統值選項後，您即可決定要如何限制重複的密碼。

限制重複的密碼

「變更密碼 (CHGPWD)」指令會要求新的密碼不同於舊的密碼。不過，使用者仍可切換使用兩個不同的密碼，除非您用 QPWDRQDDIF 系統值加以制止。下表所示即爲 QPWDRQDDIF 系統值的各種選項：

表 13. QPDRQDDIF 系統值的各種相關值

值	須檢查重複情形的密碼數
0	0 允許重複密碼。
1	32
2	24
3	18
4	12
5	10
6	8

表 13. QPDRQDDIF 系統值的各種相關值 (繼續)

值	須檢查重複情形的密碼數
7	6
8	4

建議

使用密碼過期間隔與重複密碼值，來要求密碼在一年內必須是唯一的。例如，若密碼在 60 天內到期，則爲 QPWDRQDDIF 系統值選取 7。

在系統值選項套表的第 2 部份輸入了 QPWDRQDDIF 系統值選項後，您即可決定要如何使用系統值來自訂您的系統。

使用系統值來自訂您的系統

iSeries 會利用系統值與網路屬性來控制安全以外的許多事物。系統與應用程式的程式設計師將用到大部份的此類系統值與屬性。安全主管則應設定一些系統值與網路屬性，來自訂您的系統。

為您的系統提供名稱

您可以使用 SYSNAME 網路屬性來指派您的系統名稱。系統名稱會顯現在登入顯示器的右上角與系統報表中。當您的系統與另一系統或透過 iSeries Access for Windows 與個人電腦進行通信時，也會用到系統名稱。

當您的系統與其他系統或個人電腦進行通信時，系統名稱可用來識別及區分您的系統與網路上的其他系統。每當電腦進行通信時便會互相交換系統名稱。一旦指派了系統名稱，即不應加以變更，否則將會影響網路中的其他系統。

建議

爲您的系統選擇具有意義且唯一的名稱。即使您目前不會與其他電腦進行通信，也不代表未來不會。如果您的系統屬於某一網路，網路管理員可能會告訴您應該使用何種系統名稱。

例如，JKL Toy Company 的 Sharon Jones 即決定將系統命名爲 JKLTOY。

在系統上顯示日期與時間

您可以設定當系統列印或顯示日期時，年月日的出現順序。也可指定年 (Y)、月 (M)、日 (D) 之間應使用的字元。

系統值 QDATFMT 即可決定日期格式。下圖所示爲系統在列印日期 16 June 2000 時的各種可能選項：

表 14. QDATFMT (系統日期格式)

您的選項	說明	結果
YMD	年、月、日	00/06/16
MDY	月、日、年	06/16/00
DMY	日、月、年	16/06/00
JUL	羅馬曆日期	00/168

註: 以上範例都是使用斜線 (/) 日期分隔字元。

系統值 QDATSEP 可用來決定系統在年月日之間使用的字元。下表所示即爲可用的選項。您要用數字來指定選項：

表 15. QDATSEP (系統日期分隔字元)

分隔字元	QDATSEP 值	結果
/ (斜線)	1	16/06/00
- (連字號)	2	16-06-00
. (句點)	3	16.06.00
, (逗點)	4	16,06,00
(空白)	5	16 06 00

註: 上述範例皆採用 DMY 格式。

QTIMSEP 系統值可決定當系統顯示時間時，用於分隔時、分、秒的字元。您要用數字來指定您的選項。下表所示即爲上午 10:30 在各種選項值下的格式：

表 16. QTIMSEP (系統時間分隔字元)

分隔字元	QTIMSEP	結果
: (冒號)	1	10:30:00
. (句點)	2	10.30.00
, (逗點)	3	10,30,00
(空白)	4	10 30 00

決定如何為系統裝置命名

如果您將任何新的顯示站與印表機附加至您的系統，系統即會自動加以配置。它也會爲每一新的裝置提供名稱。QDEVNAMING 系統值即可決定如何來指派名稱。下圖所示即爲系統如何命名所附加的第三部顯示站與第二部印表機：

表 17. 系統裝置命名

您的選項	命名格式	顯示站名稱	印表機名稱
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	裝置的位址	DSP010003	PRT010002

註: 在上面的範例中，顯示站與印表機都是接到第一條纜線。

建議

使用 iSeries 命名慣例，除非您是執行需要 S/36 命名慣例的軟體。iSeries 的顯示站與印表機名稱遠比採用裝置位址的名稱來得簡易。顯示站與印表機名稱會顯現在數種「作業輔助程式」顯示器上。印表機名稱亦會用於管理印表機輸出。

當系統配置好新的裝置後，請用「變更顯示裝置 (CHGDEVDSP)」指令或「變更印表機裝置 (CHGDEVPRT)」指令，爲裝置輸入有意義的說明。請在說明中同時納入裝置的實際位址及其位置，例如*會計室，第一條線，位址 6*。

選擇您的系統印表機

以 QPRTDEV 系統值來指派您的系統印表機。此系統值、使用者設定檔再加上工作說明，將決定工作所使用的印表機。除非使用者設定檔或工作說明另有指定印表機，不然工作都是使用系統印表機。

建議

通常，您的系統印表機應該是系統上最快的印表機。請將系統印表機用於列印較長的報表與系統輸出。

註: 在您安裝且配置好系統後，您才會得知印表機的名稱。現在請記下您系統印表機的相關位置。稍後再填寫印表機名稱。

允許顯示已完成的印表機輸出

系統會提供使用者尋找其印表機輸出的功能。「查看印表機輸出」顯示器會列出目前正在列印或等待列印的所有輸出。您也可允許使用者查看已完成之印表機輸出清單。此顯示器會顯示相關輸出的列印時間以及所用的印表機。這對尋找遺失的報表十分有用。

工作帳戶功能與 QACGLVL 系統值可讓您顯示已完成的印表機輸出。QACGLVL 系統值的 *PRINT 選項則可用來儲存關於已完成印表機輸出的資訊。

建議

儲存已完成印表機輸出的相關資訊極佔系統空間。除非您覺得使用者會列印許多報表，否則不需提供此功能。請在「系統值選項」套表中輸入「否」。此值會將工作帳戶層次設成 *NONE。

- 請確定已爲您的公司撰寫類似於 JKL Toy Company 範例中，Sharon Jones 與 John Smith 所編訂的安全原則聲明。
- 同時確定已在系統值選項套表中輸入系統值的選項。
- 記下您想納入安全備忘錄中的內容。

在您於「系統值選項」套表中輸入所有系統選項並撰寫了安全原則後，即可規劃使用者群組。

範例：JKL Toy Company 的安全原則

下列備忘錄說明 JKL Toy Company 總裁 John Smith 傳給員工的安全原則。他使用他和 Sharon 建立的附註來開發該安全備忘錄。

表 18. 範例：JKL Toy Company 的安全備忘錄

寄件者：John Smith 總裁

JKL Toy Company

收件者： 全體 JKL Toy Company 員工

主旨： 新系統的安全

各位都已經參加過新系統的資訊會議。需要使用這套系統的人員也已經開始接受訓練，並且將於下週開始處理客戶訂單。我們預期這套系統很快會成爲企業成功的重要關鍵。

現在我要複查我們的安全決策及原則，並且強調它的重要性。設計這些原則，是爲了保護企業的重要資訊。

- Sharon Jones 負責新系統安全。Ken Harrison 從旁輔助。如果各位有任何問題或任何安全上的疑慮，請與他們連繫。
- 我們根據現有資訊政策，決定誰能執行系統功能。例如：
  - 合約及特殊計價是機密資訊，絕不能洩露給公司外的任何人員。
  - 只有「會計人員」可以設定及變更客戶的信用限制。
- 需要使用這套系統的人員，都會收到一個使用者 ID 及密碼。第一次登入系統時，必須變更您的密碼，以後每 60 天變更一次。請選擇一個您記得住，但又不過於明顯的密碼。您收到的使用者 ID 時還附有一個套表，裡面是建立密碼的相關建議。
- *請不要將您的密碼告訴任何人*。您應該可以在系統上執行工作上需要的任何動作。如果您需要存取資訊，請與 Sharon 或 Ken 連繫。如果您忘記密碼，Sharon 或 Ken 可以立即爲您設定新的密碼。任何人不得使用別人的使用者 ID 和密碼登入系統。
- 您可能已經學會如何使用工作站上的記錄和播放功能來節省輸入時間。*請勿*使用這個方法儲存您的密碼。
- 離開座位時，工作站必須登出。您在訓練期間已經學過如何暫時登出工作站。需要暫時離開座位時，請使用這個功能。如果需要離開很長的時間，請結束工作並使用正常程序登出。

  尤其在裝載處、客戶服務區以及遠端行銷辦事處等接近公眾處，離開工作站時更應該登出系統，這點十分重要。
- 雖然主機非常堅固，但仍應避免猛烈撞擊或在上面置物。主機的控制面板通常不啓用，但請勿觸摸。會計部人員必須確保無人篡改主機資料。

請記住，新系統主要在簡化我們工作，進而改善企業效能。我們的安全原則對您應該是一種助力而非阻力。如果您有任何問題或顧慮，請與 Sharon、Ken 或我連繫。

建立安全原則草稿之後，您可以開始規劃使用者群組。

規劃使用者群組

規劃處理的第一個步驟 - 決定您的安全策略 - 就好比訂定公司政策。現在您已準備就緒要開始規劃使用者群組，而它就像是在決定部門政策。

何謂使用者群組？

使用者群組就如同其名：一群須以相同方式來使用相同應用程式的人員。一般來說，使用者群組包含在同一部門中具有類似工作職責的人員。您可以藉由建立群組設定檔來定義使用者群組。

群組設定檔的的功用為何？

群組設定檔在系統上有兩項作用：

- **安全工具**：群組設定檔可提供簡單的方式，來統籌管理誰可以使用系統上的特定物件 (物件權限)。您可以針對整個群組而非各個群組成員來定義物件權限。
- **自訂工具**：您可以將群組設定檔當作樣版，用於建立個別的使用者設定檔。相同群組中的大部份人皆具有相同的自訂需求，如起始功能表及預設印表機。您可以在群組設定檔中定義這些需求，再將其複製到個別的使用者設定檔。

群組設定檔可簡化相關作業，使您在安全與自訂上維持簡單、一致的架構。

您需要哪些套表？

若要規劃您的使用者群組，您將需要下列套表：

- 「使用者群組識別」套表
- 「使用者群組說明」套表

註: 對於系統上的每一個使用者群組，您都須準備一份「使用者群組說明」套表。

請參閱下列主題來協助您完成這些套表：

- 界定使用者群組。
- 規劃群組設定檔。
- 選擇會影響登入的值。
- 選擇會限制使用者作業的值。
- 選擇用於設定使用者環境的值。

界定使用者群組

當您規劃您的使用者群組時，須先界定您的系統上的使用者群組。如此可讓您規劃這些群組所需的資源存取權限。請儘量用簡易的方法來界定您的使用者群組。先思考哪些部門或工作群組會用到系統。然後參閱您先前所繪製的應用程式圖解。看看工作群組與應用程式之間是否存有自然的關係：

- 您是否能找出每個工作群組的主要應用程式？
- 您是否知道每個群組需要哪些應用程式？以及它們不需要哪些應用程式？
- 您是否知道哪個群組應擁有各應用程式檔案庫中的資訊？

如果您對這些問題都可回答「是」，便可開始規劃您的使用者群組。不過，如果回答的是「有時候」或「也許」，那麼您最好改用系統化的方法來界定您的使用者群組。

您可以參考如何用此方法來界定使用者群組的範例。

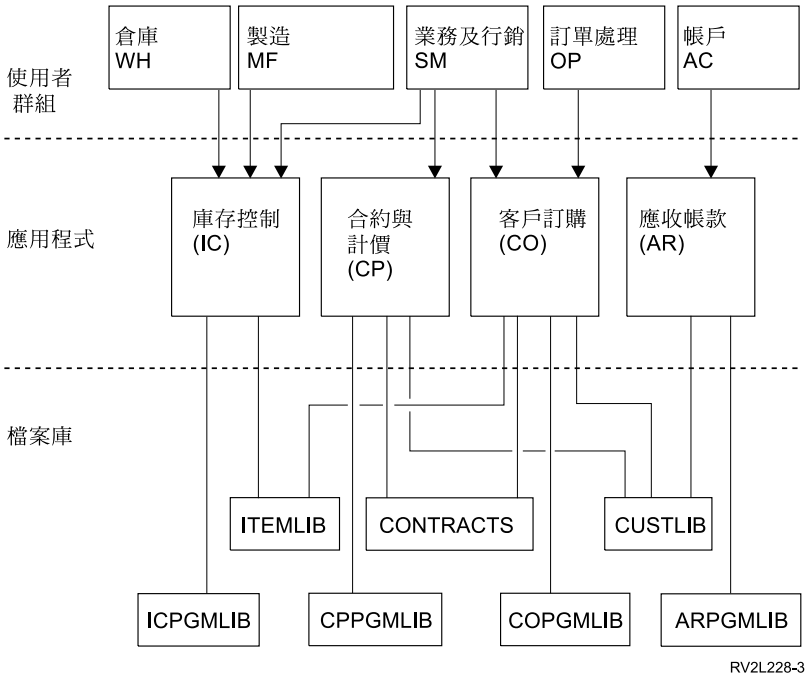
註: 讓使用者僅屬於一個群組設定檔的成員可以簡化您的安全管理作業。不過，有某些情況較適合讓使用者屬於多個群組設定檔。

讓使用者屬於多個群組設定檔，通常比授予許多專用權限給個別使用者設定檔來得容易管理。

範例：界定使用者群組

若工作群組與應用程式之間的關係顯得相當複雜或曖昧，使用諸如使用者群組識別套表的矩陣技術可讓情況較爲明確。當您在矩陣上繪製系統使用者及其應用程式需求時，應看到類似的型樣浮現。除了填寫「使用者群組界定」套表外，Sharon Jones 還用到應用程式圖解來界定哪些使用者群組須存取應用程式。

下圖所示即爲 JKL Toy Company 的應用程式圖解。



如果您的安全措施是採寬鬆式，請用 X 來指出使用者需要應用程式。如果您的安全措施採限制式，您必須考慮人員使用應用程式的方式。若有人只須查看應用程式中的資訊，則應使用 V (檢視) 而非在矩陣中放置 X。若有人須變更此資訊，應使用 C (變更)。若有人對資訊擁有主要責任則使用 O (擁有者)。

以 JKL Toy Company 爲例，即有不同的群組需要「計價與合約」應用程式：

- 業務及行銷部門負責訂價及建立客戶合約。他們*擁有*計價與合約資訊。
- 客戶訂單部門則會間接變更合約資訊。當其處理訂單時，合約上的數量即會變更。他們必須*變更*計價與合約資訊。
- 訂單處理人員須查看信用額度資訊以便來規劃工作，但無權加以變更。他們必須*檢視*信用額度檔案。

表 19. JKL Toy Company 的使用者群組識別套表：範例

使用者群組識別套表					
準備人員：Sharon Jones		日期：9/2/99			
		所需的應用程式存取權限			
使用者名稱	部門	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	訂單處理 (OP)	O	C	C	C
Karen R.	訂單處理 (OP)	O	C	C	C
Kris T.	會計 (AC)	V		V	O
Sandy J.	會計 (AC)	V	C	V	O
Peter D.	會計 (AC)	C		V	O
Ray W.	倉儲 (WH)	V	O	V	
Rose Q.	倉儲 (WH)	V	O	V	

表 19. JKL Toy Company 的使用者群組識別套表：範例 (繼續)

Roger T.	業務及行銷 (SM)	C	C	O	C
Sharon J.	經理 (MG)	C	C	C	C

註:

- 如果您的安全環境爲*寬鬆式*，請用 X 來標示使用者需要哪些應用程式。
- 如果您的安全環境爲*一般式*，請用 A 來標示哪些使用者對哪些應用程式具有權限。
- 如果您的安全環境爲*嚴密式*，您必須使用 C (變更)、V (檢視) 和 O (擁有者)來指定*如何*使用應用程式。

Sharon Jones 在準備矩陣時記下了一些決策：

- 訂單處理與會計部門可成為彼此的代理。目前，他們需要類似的應用程式。不過，他們應分屬不同群組，因為日後隨著人員擴編，他們將更加專司其職。
- 雖然我們不允許訂單處理人員直接變更庫存或合約，但當其建立及填寫訂單時，料品與合約餘額會自動變更。這在以後是否會成為安全議題？
- 業務及行銷人員會參與所有業務並使用各種應用程式。他們為料品訂立價格和說明。也負責建立新客戶，雖然信用限制是由會計部門訂定。他們還須設定所有的合約條款與價格。

決定您的使用者群組爲何。如有需要，填寫「使用者群組識別」套表來幫助您決定。

將使用者新增至「使用者群組識別」套表後，您便可規劃群組設定檔。

規劃群組設定檔

當您完成界定您的使用者群組後，即可開始規劃各群組的設定檔。您所作的許多決策會同時影響安全與自訂作業。例如，當您指定起始功能表時，您可能會限制使用者只能看到該功能表。不過，這也可確保使用者在登入後會看到正確的功能表。

爲某個使用者群組準備一份使用者群組說明套表來作爲範例。待完成第一份套表後，回頭爲所需的其他群組填寫相關套表。

iSeries 上將安全與自訂作業設計得極具彈性。本主題中的規劃方法爲設計群組設定檔與工作說明提供了良好的途徑，不過您的程式設計師或應用程式供應商可能會建議不同的方法。

為群組設定檔命名

由於群組設定檔就宛如特殊類型的使用者設定檔，您可能希望能在清單與顯示器上輕易找出群組設定檔。因此您必須爲其指派特殊的名稱。若希望群組設定檔能一起顯示在清單上，它們的名稱應以相同字元爲開頭，如 GRP (代表群組) 或 DPT (代表部門)。請在爲使用者群組命名時遵照下列準則：

- 使用者群組名稱最長可到 10 個字元。
- 名稱可包含字母、數字和特殊字元：井號 (#)、金錢符號 ($)、底線 (_) 及小老鼠符號 (@)。
- 名稱不可用數字開頭。

註: 對每一個群組設定檔而言，系統會爲其指派群組識別碼 (*gid*)。一般而言，您可以交由系統來產生 *gid*。如果您將系統用於網路中，您可能要指派特定的 gid 給群組設定檔。請洽詢您的網路管理者來驗證您是否須指派 gid。

您應在「命名慣例」套表的適當欄位中，填入您的群組設定檔命名系統。例如，Sharon Jones 即選擇 DPT 作爲群組設定檔的命名慣例。她也填寫了「命名慣例套表」的適當區段。

表 20. JKL Toy Company 的命名慣例套表：群組設定檔範例

物件類型	命名慣例
群組設定檔	使用字元 DPT 其後接上部門縮寫。群組設定檔的文字說明應該是部門名稱。

決定使用者群組需要哪些應用程式與檔案庫

如果您尚未執行此作業，請將您的使用者群組新增至您先前所繪的應用程式圖解以及檔案庫中。此影像可協助您決定各群組的資源與應用程式需求。

在「使用者群組說明套表」的第 1 部份指出群組的主要應用程式，也就是其最常用的應用程式。列出群組所需的其他應用程式。

參閱您的「應用程式說明套表」以及應用程式圖解，查看各群組所需的檔案庫。洽請程式設計師或應用程式供應商，查明哪種方法最適合用來存取這些檔案庫。大部份的應用程式都是採用下列技巧之一：

- 應用程式併入使用者起始檔案庫清單上的檔案庫。
- 應用程式執行安裝程式，將檔案庫放入使用者的檔案庫清單。
- 檔案庫不須在檔案庫清單中。應用程式一律指定檔案庫。

系統會使用檔案庫清單來尋找您在執行應用程式時所需的檔案與程式。**檔案庫清單**是一份列有相關檔案庫的清單，供系統搜尋使用者所需的物件。它包含兩個部份：

1. **系統部份**：以 QSYSLIBL 系統值來指定，用於 OS/400 檔案庫。此系統值的預設值不須變更。
2. **使用者部份**：QUSRLIBL 系統值會提供檔案庫清單的使用者部份。使用者的工作說明將指定使用者登入後的起始檔案庫清單或指令。如果您具有起始檔案庫清單，它會置換 QUSRLIBL 系統值。應用程式檔案庫應納入至檔案庫清單的使用者部份。

使用工作說明

當使用者登入系統時，其工作說明會定義許多的工作性質，包括工作的列印方式、批次工作如何執行、以及起始檔案庫清單。您的系統隨附有一個工作說明，稱爲 QDFTJOBD，可在建立群組設定檔時使用。不過，QDFTJOBD 會指定 QUSRLIBL 系統值爲起始檔案庫清單。如果想讓不同的使用者群組有權在登入時存取不同的檔案庫，您須爲各個群組建立唯一的工作說明。

在「使用者群組說明套表」上列出該群組所需的各個檔案庫。如果檔案庫應納入群組工作說明的起始檔案庫清單中，請在該套表上標示各檔案庫的名稱。

在您開始選擇會影響登入的值之前，您最好先複查範例瞭解 Sharon Jones 如何說明 JKL Toy Company 的使用者群組。

範例：JKL Toy Company 的使用者群組說明套表

第一個表格顯示 Sharon 爲業務及行銷部門準備的「使用者群組說明套表」的第 1 部份。請注意，她並未將 CONTRACTS 及 CPPGMLIB 檔案庫放入群組的起始檔案庫清單中。應用程式會自動將它們新增至檔案庫清單中，而不是放在 DPTSM 起始檔案庫清

單。使用者結束應用程式時，系統會從檔案庫清單中移除這些檔案庫。這樣可以加強這些檔案庫的安全，因爲您只能透過應用程式來存取它們。

表 21. JKL Toy Company 的使用者群組說明套表：描述性資訊範例

使用者群組說明套表	1 / 2
準備人員：Sharon Jones	日期：9/5/99
群組設定檔名稱：DPTSM 群組說明：業務及行銷部門	
群組的主要應用程式：合約與計價 列出群組需要的其他應用程式：庫存 (輸入項目說明及價格)、客戶訂單	
列出群組需要的每一個檔案庫。請以 (✓) 標示應該放在群組起始檔案庫清單中的每一個檔案庫： • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • CONTRACTS	

此外，Sharon 還爲倉儲部門準備了「使用者群組說明套表」。

表 22. 使用者群組說明套表：描述性資訊

使用者群組說明套表	1 / 2
準備人員：Sharon Jones	日期：9/5/99
群組設定檔名稱：DPTWH 群組說明：倉儲部門	
群組的主要應用程式：庫存控制 列出群組需要的其他應用程式：無	
列出群組需要的每一個檔案庫。請勾選 (✓) 要放在群組起始檔案庫清單中的每一個檔案庫。 • ✓ITEMLIB • ✓ICPGMLIB	

完成「使用者群組說明套表」的第 1 部份後，您可以開始選擇會影響登入的值。

選擇會影響登入的系統值

待您在系統上規劃群組設定檔後，即須選擇會影響登入的系統值。請於「使用者群組說明」套表的第 2 部份中輸入您的選擇。請記得，您所選的值會被複製用來爲群組成員建立個別設定檔。首先是輸入您所選取的群組設定檔名稱以及群組的簡短說明 (文字)。

如果您有適當地自訂您的系統，使用者只需要在「登入」顯示器上輸入其使用者 ID 和密碼。他們的使用者設定檔將會提供其他登入值。

密碼

將群組設定檔的密碼設成 *NONE。如此就可防止任何人利用群組設定檔來登入。之後，當您複製群組設定檔以建立個別使用者設定檔時，您再爲各使用者設定密碼。

起始程式與起始程序

使用者的起始程式又稱爲**登入程式**，會在系統顯示第一個功能表之前執行。請在群組設定檔中輸入該程式名稱及其檔案庫，即使其檔案庫是起始檔案庫清單的一部份也一樣。藉由指定此兩項目，可確保系統執行正確的程式，而且讓您不須擔憂檔案庫清單的變更。

使用起始程式或程序是基於下列原因之一：

- 某些應用程式以起始程式來設定應用程式環境。
- 您希望讓使用者僅執行一支程式，而且永遠看不到功能表。以 JKL Toy Company 爲例，在裝載處使用工作站的人員只能執行收貨程式。如此可防止位於公共場所的工作站暴露安全機能。

將使用者的**限制功能**欄位設成 *YES 或 *PARTIAL，可防止使用者於「登入」顯示器變更起始程式。

請洽詢程式設計師，查明您的應用程式是否需要起始程式或程序。

起始功能表與起始功能表檔案庫

起始功能表又稱**第一個功能表**，是使用者登入後所見到的第一個功能表。起始程式會在起始功能表出現前執行。如果起始程式會帶出任何顯示器，使用者將先見到這些顯示器，然後才是系統所顯示的起始功能表。

一般而言，群組的起始功能表須爲該群組的主要應用程式的主功能表。請指定此功能表名稱及其檔案庫。

如果將使用者的**限制功能**欄位設成 *YES，使用者即不允許在「登入」顯示器變更起始功能表。如果將使用者的*限制功能*欄位設成 *PARTIAL，則表示允許使用者在「登入」顯示器變更起始功能表。

現行檔案庫

現行檔案庫又稱爲**預設檔案庫**。爲使用者指定現行檔案庫時，會發生數種情況：

- 如果使用者建立任何物件，例如查詢程式，除非使用者指定不同的檔案庫，不然系統會將這些物件放入現行檔案庫。
- 系統自動將現行檔案庫新增至檔案庫清單的使用者部份。它可併入到工作說明的起始檔案庫清單中，但不必非得如此。
- 現行檔案庫成爲檔案庫清單之使用者部份的第一個檔案庫。系統在搜尋使用者檔案庫清單中的檔案庫前，會先在現行檔案庫中搜尋檔案與程式。
- 如果未指定使用者的現行檔案庫，系統將指派 QGPL (一般用途) 檔案庫。

建議

如果您打算使用 IBM Query for iSeries 授權程式或其他類似程式，現行檔案庫將極爲重要。請採用下列措施之一：

- 建立一檔案庫供群組中的每個人共用。將群組的所有查詢程式與檔案放入該檔案庫中。將其命名爲和群組設定檔相同的名稱，並使之成爲群組的現行檔案庫。
- 爲每位要使用「查詢」的使用者提供個人檔案庫。將檔案庫命名爲和使用者設定檔的名稱同名。於群組成員的個別設定檔而非群組設定檔上，將此檔案庫指定爲現行檔案庫。

在「使用者群組說明」套表的第 2 部份中，將您的選項填入會影響登入的相關欄位。

待您選妥影響登入的值後，即可選擇會限制使用者作業的值。

選擇會限制使用者作業的值

在「使用者群組說明套表」的第 2 部份輸入會影響登入的值選項後，您應該考慮限制使用者在系統上所能執行的作業。其原因有數個：

- 防止有人使用 CL 指令。他們可能只是試加使用，卻不慎造成損壞。
- 限制使用者只能使用特定應用程式與功能。
- 提供簡單的環境，讓使用者不受非必要的選項所混淆。

使用者所能執行的作業是由許多因素所決定：

- 應用程式設計
- 系統值
- 資源安全
- 群組設定檔
- 使用者設定檔
- 工作說明

群組或使用者設定檔中的兩個欄位，即**限制功能**與**使用者類別**，可決定使用者能夠置換您所作的哪些決策。

限制功能

限制功能欄位又稱爲**限制指令行使用**。您可以限制使用者是否能變更「登入」顯示器的值、輸入指令、以及變更其 Attention-key-handling 程式。您可以選擇嚴密限制 (*YES)、普通限制 (*PARTIAL) 或無限制 (*NO)。下表所示即爲每種值所允許的作業：

表 23. 限制功能值所允許的功能

限制功能值	變更起始程式	變更起始功能表	變更現行檔案庫	變更忽斷程式	輸入指令
*YES	否	否	否	否	一些[1]
*PARTIAL	否	是	否	否	是
*NO	是	是	是	是	是

1 允許這些指令：SIGNOFF、SNDMSG、DSPMSG、DSPJOB、DSPJOBLOG 及 STRPCO。使用者不得從任何「作業輔助程式」功能表或顯示器，使用 F9 來顯示指令行。

使用者類別

使用者類別又稱**使用者類型**，可決定使用者在「作業輔助程式」功能表與系統功能表上所能看到的選項。除非您已在**特殊權限**欄位中列出相關權限，不然也可以決定允許使用者執行哪些系統功能。

對限制功能與使用者類別的建議事項

大部份使用者並不需要或想要存取 CL 指令或系統功能。「作業輔助程式」顯示器已可爲使用者提供足夠的相關資訊，以及對其本身工作的控制項。下列建議可讓使用者只存取完成其作業所需的系統資源：

- 在每個群組設定檔中，將**限制功能**欄位設成 *YES。並將*使用者類別*欄位設成 *USER。
- 置換需要系統功能之個別使用者的相關規格。
- 確定您的功能表可提供切換不同應用程式的方法 (如果使用者有此需要)。

在「使用者群組說明」套表的第 2 部份輸入使用者類別與限制功能的選項後，您即可選擇用於設定使用者環境的值。

選擇用於設定使用者環境的值

在「使用者群組說明」套表的第 2 部份輸入限制使用者所能執行的系統作業後，即可選擇用於決定使用者作業環境的值。使用者設定檔中有許多欄位可決定使用者的作業環境：該使用哪個印表機、訊息要傳到哪裡、工作的執行優先順序爲何。對許多此類欄位而言，建議您使用預設設定。下列各段落將說明其中的部份欄位。

- **工作說明與工作說明檔案庫**：設定檔中的這些欄位會告訴系統，當使用者登入時應使用哪種工作說明。工作說明中含有起始檔案庫清單。每個使用者群組都須具有工作說明，且其名稱須與群組設定檔相同。工作說明通常是放在 QGPL 檔案庫中。
- **印表機裝置與輸出佇列**：使用者所建立的任何印表機輸出，都會被送往設定檔中所列的印表機裝置，除非您用特定的列印工作將其送往其他印表機。使用者群組的成員通常會位於相近位置並共用相同的印表機。您可以在群組設定檔中指定該印表機，並將其複製到每一個別的使用者設定檔中。使用者的印表機裝置亦稱爲**預設印表機**。

  輸出佇列則含有尚未列印的印表機輸出。一般來說，每個印表機裝置都有本身的輸出佇列而且使用相同的名稱。您可以爲輸出佇列指定 *DEV，來告訴系統使用印表機裝置的輸出佇列。

  在使用者群組說明套表上，填寫工作說明及其檔案庫的名稱、以及預設印表機和輸出佇列等欄位。
- **設定作業輔助程式介面**：您的系統在出貨時，所有使用者的「作業輔助程式」功能表是設定成岔斷鍵處理程式。當使用者按下岔斷鍵時，將會看到「作業輔助程式 (ASSIST)」功能表。如果您的應用程式使用了不同的岔斷鍵處理程式，您應提供不同方法讓使用者前往「作業輔助程式」功能表：
  - 利用 GO ASSIST 或 CALL QEZAST，將「作業輔助程式」功能表加入您的主應用程式功能表成爲一個選項。
  - 讓使用者從指令行鍵入 GO ASSIST。

如果使用者設定檔中的**限制功能**欄位已設成 *YES，使用者將無法用 GO 指令來顯示功能表。此時，您必須提供方法讓「作業輔助程式」的使用者能夠存取 ASSIST 功能表。

您最好參考相關範例，瞭解 Sharon Jones 爲 JKL Toy Company 的「使用者群組說明」套表選了哪些值。

爲完成這些規劃步驟，您應該：

- 爲公司中的每個使用者群組，填寫使用者群組說明套表。
- 在命名慣例套表上，說明您如何爲使用者群組命名。
- 將使用者群組新增至您的應用程式與檔案庫圖解中。

完成這些作業後，即可開始規劃個別使用者設定檔。

範例：JKL Toy Company 的使用者群組說明套表--第 2 部份

Sharon Jones 爲市場行銷人員準備使用者群組說明套表時，她寫了一些有關「業務及行銷部門及倉儲部門」的新附註。

- 市場行銷人員經常使用 IBM Query for iSeries。每一個使用者應該有專用檔案庫。倉儲可以有一個群組檔案庫。
- 在接收處工作的倉儲人員需要的是起始程式而非起始功能表。

Sharon 爲這兩個部門準備了使用者群組說明套表的第 2 部份。

表 24. JKL Toy Company 的使用者群組說明套表：業務及行銷部門範例

欄位名稱	建議值	您的選擇
群組設定檔名稱 (使用者)		DSTSM
密碼	*NONE	*NONE
使用者類別 (使用者類型)	*USER	*USER
現行檔案庫 (預設檔案庫)	*與群組設定檔同名*	(讓群組空白；填寫個別設定檔)
呼叫的起始程式 (登入程式)		
起始程式庫		
起始功能表 (第一個功能表)		CPMAIN
起始功能表檔案庫		CPMAINLIB
限制功能 (限制指令行使用)	*YES	*PARTIAL
文字 (使用者說明)		市場行銷
工作說明	*與群組設定檔同名*	DPTSM
工作說明檔案庫		QGPL
群組設定檔名稱 (使用者群組)	*NONE[1]	*NONE
列印裝置 (預設印表機)		PRT03
輸出佇列	*DEV	*DEV

表 25. JKL Toy Company 的使用者群組說明套表：倉儲部門範例

欄位名稱	建議值	您的選擇
群組設定檔名稱 (使用者)		DPTWH
密碼	*NONE	*NONE
使用者類別 (使用者類型)	*USER	*USER
特殊環境		
現行檔案庫 (預設檔案庫)	*與群組設定檔同名*	DPTWH
呼叫的起始程式 (登入程式)		

表 25. JKL Toy Company 的使用者群組說明套表：倉儲部門範例 (繼續)

欄位名稱	建議值	您的選擇
起始程式庫		
起始功能表 (第一個功能表)		ICMAIN
起始功能表檔案庫		ICPGMLIB
限制功能 (限制指令行使用)	*YES	*YES
文字 (使用者說明)		倉儲部門
工作說明	*與群組設定檔同名*	DPTWH
工作說明檔案庫		QGPL
群組設定檔名稱 (使用者群組)	*NONE[1]	*NONE
列印裝置 (預設印表機)		PRT04
輸出佇列	*DEV	*DEV
1 群組設定檔的群組設定檔名稱必須是 *NONE。群組設定檔不能是另一個群組的成員。		

現在您可以開始規劃個別使用者設定檔。

規劃個別使用者設定檔

現在您已決定了整體安全策略，並規劃好使用者群組，接下來便可規劃個別的使用者設定檔。

您需要哪些套表？

請使用下列套表來規劃個別使用者設定檔：:

- 「個別使用者設定檔」套表
- 「系統責任」套表

您還須用到下列已完成套表的資訊：

- 「使用者群組定義」套表
- 「命名慣例」套表
- 您的應用程式圖解

為使用者設定檔命名

您的使用者設定檔名稱就是系統用以識別您的憑藉。您可在「登入」顯示器的**使用者 ID** 欄位輸入您的使用者設定檔名稱。您的任何工作以及所建立的印表機輸出都會與您的使用者設定檔名稱關聯在一起。

在決定如何爲使用者設定檔命名時，請考慮下列事項：

- 使用者設定檔名稱最長不超過 10 個字元。某些通信方法會將使用者 ID 限制在 8 個字元。
- 使用者設定檔名稱可包含字母、數字和特殊字元：井號 (#)、金錢符號 ($)、底線 (_) 及小老鼠符號 (@)。但開頭不得爲數字或底線 (_)。
- 系統並不區分使用者設定檔名稱中的大小寫字母。如果輸入小寫英文字元，系統會將其轉爲大寫字元。

- 管理使用者設定檔時所用的顯示器與清單，會按使用者設定檔名稱的字母順序加以顯示。
- 所有 IBM 提供的設定檔皆以字母 Q 爲開頭。若要使您的設定檔有所區別，請勿指派開頭爲 Q 的使用者設定檔名稱。

建議

指派使用者設定檔名稱的技巧之一是使用姓氏的頭 7 個字元，後面再加上名字的第一個字元。以下是 Sharon 在 JKL Toy Company 對使用者設定檔所採行的命名慣例：

表 26. JKL Toy Company 的命名慣例套表：使用者設定檔範例

使用者名稱	使用者設定檔名稱
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

此方法可讓使用者設定檔名稱簡單好記。而且，您的清單與顯示器會按姓氏的字母順序來排列。

例如，JKL Toy Company 的 Sharon Jones 打算採用此命名技巧。她填寫了「命名慣例套表」的適當區段。

表 27. JKL Toy Company 的命名慣例套表：使用者設定檔範例

物件類型	命名慣例
使用者設定檔	採用使用者姓氏的頭 7 個字元，後面再加上其名字的第一個字元。使用者設定檔的說明則是「姓氏，名字」。

在「命名慣例」套表中說明了使用者設定檔的命名方式後，您便可決定誰該負責系統功能以及選擇每一個使用者的值。

決定誰該負責系統功能

在規劃個別使用者設定檔時，您必須先決定系統上每個人的責任。爲使系統有效運作，您需要有人來定期執行各類的管理及維護功能。而執行這些作業的人則需要相關權限，來下達指令和執行系統功能。

選擇會限制使用者作業的值討論**使用者類別**與**限制功能**欄位如何控制使用者所能存取的系統功能。一般而言，您不應允許大部份的使用者執行系統功能 (將使用者類別設爲 *USER，並將限制功能設爲 *PARTIAL 或 *YES)。不過，有些使用者會需要額外權限，以使系統有效運作。

下表所示爲一些重要的系統管理作業。另外還指出您對具有此類責任之人員所能指派的使用者類別與特殊權限。此清單可協助您決定哪些使用者需要特殊權限。不過，它並不是用來操作及維護系統的完整規劃工具。此表格所列的使用者類別與特殊權限適用於大多數系統。但隨著系統的不同，您可能需要指派不同的權限。

當您在設定檔中指派 *USER 以外的使用者類別時，使用者會自動收到某類特殊權限，來執行系統功能。您可以爲使用者指派異於使用者類別欄位中的特殊權限，但不一定有此必要。

表 28. 系統責任、使用者類別和特殊權限

系統功能[1]	說明	所需的使用者類別 [2]	所需的特殊權限 [3]
系統作業	管理印表機輸出、回應系統訊息、監督一般作業、執行起始程式載入 (IPL)。	*SYSOPR	*JOBCTL
系統管理	執行系統管理功能，例如建立自動清除時程表以及監督磁碟用量。	*SYSOPR	*JOBCTL
系統備份	定期儲存應用程式檔案庫、系統檔案庫和安全資訊。有關這些功能的詳情，請參閱「資訊中心」的備份及回復服務程式主題。	*SYSOPR	*SAVSYS
設定檔管理	新增使用者設定檔、維護現有設定檔。	*SECADM	*SECADM
資源安全管理	維護對系統物件的權限。	*SECOFR	*ALLOBJ
程式維護	將定期程式變更 (PTF) 套用至 IBM 所提供的檔案庫。變更應用程式檔案庫。	*SECOFR	*ALLOBJ
安全審核	設定安全審核功能。決定哪些事件、使用者和物件應予審核。		*AUDIT [4]
系統配置	新增、變更及移除系統裝置。		*IOSYSCFG[5]

1 針對具有這些責任的使用者，將「限制功能」欄位設成 *NO。

2 這是所需的最低使用者類別。此種類別提供執行功能時所需的相關指令與功能表選項的權限。取決於您的資源安全，您可能還需要額外的物件權限。

3 此種特殊權限係工作責任所需。其使用者類別可提供額外的特殊權限。

4 *AUDIT 特殊權限沒有對應的使用者類別。*SECOFR 使用者類別包含 *AUDIT 特殊權限。不過，您的審核員可能不需要 *SECOFR 使用者類別的其他功能。您應該爲需要控制審核作業的每位個別使用者，指定 *AUDIT 特殊權限。

5 *IOSYSCFG 特殊權限沒有對應的使用者類別。 *SECOFR 使用者類別包含 *IOSYSCFG 特殊權限。您應該只爲需配置您的系統的人員，指定 *IOSYSCFG 特殊權限。此人將可建立線路、控制器與裝置，或者配置 TCP/IP。不過，負責配置您系統的使用者可能不需要 *SECOFR 使用者類別的其他功能。

建議

使用上表來規劃由誰負責執行系統功能。至少，您應指派兩位人員來管理系統安全，加上兩位人員負責管理作業與備份。

以「系統責任」套表爲工具，來管理及審核您的系統。追蹤掌握系統上每位具有特殊權限的人，並瞭解其爲何需要此權限。

在您選擇每一個使用者的值之前，最好先參閱範例瞭解 Sharon Jones 如何決定使用者責任。

範例：JKL Toy Company 的系統責任套表

下列範例是 Sharon Jones 完成的「系統責任套表」：

表 29. JKL Toy Company 的系統責任套表：範例

誰是您的主要安全主管？ Sharon Jones 誰是您的代理安全主管？ Ken Harrison			
設定檔名稱	使用者名稱	類別	說明
JONESS	Sharon Jones	*SECOFR	Sharon 是主要安全主管及系統管理員。
HARRISOK	Ken Harrison	*SECOFR	Ken 是 Sharon 的整體系統管理員代理人。
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy 的主要責任是系統作業及備份。
ROGERSK	Karen Rogers	*SYSOPR	Karen 會協助 Sandy 執行作業及系統備份。
WILLISR	Rose Willis	*SYSOPR	Rose 負責晚班系統操作。

完成「系統責任套表」後，您可以開始爲每一位使用者選擇值。

選擇每一個使用者的值

當您決定了系統使用者的責任後，即可開始選擇每位使用者的值。規劃了群組設定檔來作爲個別使用者設定檔的型樣後，您即已完成大部份的工作。請用「個別使用者設定檔」套表將每個使用者指定給正確的群組，並定義群組中各使用者的差異。您應先用某一使用者群組爲範例來填寫「個別使用者設定檔」套表，然後再回頭爲其餘使用者群組準備「個別使用者設定檔」套表。

在個別使用者設定檔套表的頂端，填寫群組設定檔名稱和其他說明資訊。

範例：JKL Toy Company 個別使用者設定檔套表的說明資訊

以下是 Sharon Jones 填寫「個別使用者設定檔」套表頂端部份的內容。

表 30. JKL Toy Company 的個別使用者設定檔套表：說明資訊範例

個別使用者設定檔套表	
準備人員：Sharon Jones	日期：9/5/99
群組設定檔名稱：DPTOP	
所建物件的擁有者：	群組對所建物件的權限：
群組權限類型：	

決定群組成員的值

在您的「個別使用者設定檔」套表上，寫下每一群組成員的設定檔名稱與說明 (使用者名稱)。下段內容會說明如何決定各群組成員的值。

請記得，群組設定檔是個別使用者設定檔的型樣。在「個別使用者設定檔」套表上，您只需指明與群組不同的事項即可。

- **指派密碼**：指派起始密碼給使用者的最簡單方式是讓密碼和設定檔名稱相同。然後您可藉由將密碼設爲到期，來要求使用者於初次登入時變更密碼。在主題將密碼設爲到期中，您會學到如何在複製群組設定檔時自動執行此動作。如果您要執行此動作，便不須在「個別使用者設定檔」套表上列出密碼。

- **使用者類別與限制功能**：參閱您的「系統責任」套表，以瞭解各群組有哪些成員須在**使用者類別**與**限制功能** 等欄位使用不同的值。針對任何須用到不同於群組設定檔之值者，於「個別使用者設定檔」套表上填寫適當資訊。
- **指定其他值**：查明是否有特定使用者需要不同於「使用者群組說明」套表中爲群組所指定的值。在「使用者群組說明」套表上，**使用者類別**與**限制功能**欄位是列於頂端，因爲其值對某些群組成員而言經常不同。請就您所處理的群組成員，列出任何其他可能不同的欄位。

要完成此規劃步驟，請務必：

- 完成您的系統值選項套表。
- 在命名慣例套表上，說明您要如何爲使用者設定檔命名。
- 爲您公司中的每個使用者群組，準備一份「個別使用者設定檔」套表。

在您規劃規劃資源安全之前，最好先參考相關範例瞭解 Sharon 用於個別使用者的資訊。

範例：JKL Toy Company 的個別使用者設定檔套表

在 JKL Toy Company 裝載處工作的人員，只能執行一種程式。 Sharon 限制這些使用者只能執行少許功能，因爲一般大眾都能接觸他們工作的工作站。這些「倉儲部門」成員有起始程式，但沒有起始功能表。「訂單處理部門」有兩台區域印表機以及一台位於遠端行銷辦事處的印表機。因此，Sharon 指派給部份使用者的印表機不同於群組的印表機。

下列是 Sharon Jones 爲 JKL Toy Company 的「倉儲部門」及「訂單處理部門」完成的「個別使用者設定檔套表」。請注意，她只填寫了他們有別於群組設定檔的欄位值。

表 31. JKL Toy Company 的個別使用者設定檔套表：倉儲部門範例

群組設定檔名稱：DPTWH					
每個群組成員製作一個登錄：					
使用者設定檔	**本文 (說明)**	**使用者類別**	**限制功能**	**起始程式/檔案庫**	**起始功能表/檔案庫**
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	無
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	無
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

表 32. 個別使用者設定檔套表：訂單處理部門範例

群組設定檔名稱：DPTOP				
每個群組成員製作一個登錄：				
使用者設定檔	**本文 (說明)**	**使用者類別**	**限制功能**	**列印裝置**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

接下來，您可以開始規劃資源安全。

第 5 章 規劃資源安全

現在您已完成了規劃系統使用者的處理，接下來就可規劃資源安全，來保護系統上的物件。在《設定資源安全》中，您將學習如何在系統上設定資源安全。

系統值與使用者設定檔會控制誰有權存取您的系統，同時防止未經授權的使用者登入。資源安全則可控制經授權的使用者在順利登入後，所能執行的動作。資源安全將在您的系統上支援各項主要的安全目標，進而保護：

- 資訊的機密性
- 資訊的精確，防止未經授權的變更
- 資訊的可用性，防止意外或有意的損壞

依據您的公司是否自行開發應用程式或加以採購，您的資源安全規劃方式將會不同。就自行開發應用程式而言，您應該在進行應用程式設計階段，將資訊安全方面的需求傳達給程式設計師。如果是採購應用程式，您將必須決定安全需求，並確定這些需求和供應商所設計的應用程式相符。不論是何種情況，此處所提的技巧都能爲您提供助益。

本主題將提供用於規劃資源安全的基本手法。其間將介紹各項主要技巧，並顯示如何加以運用。此處所述的方法並不一定適用於每家公司和每種應用程式。當您在規劃資源安全時，請諮詢您的程式設計師或應用程式供應商。

請複查下列主題，來協助您規劃資源安全：

- 決定資源安全的目標
- 瞭解權限的類型
- 規劃應用程式檔案庫的安全
- 決定檔案庫與物件的所有權
- 將物件分組
- 保護印表機輸出
- 保護工作站
- 資源安全建議摘要
- 規劃您的應用程式安裝

您需要哪些套表？

請影印下列套表，並在您閱讀本主題的同時加以填寫。針對某一應用程式完成整個程序，然後針對其他每一個應用程式重複此程序。

表 33. 規劃資源安全時所需的規劃套表

套表名稱	所需份數
授權清單套表	數份
印表機輸出與工作站安全套表	一份

將資訊填入您先前所處理的下列套表中：

表 34. 將會變更的規劃套表

套表名稱	準備階段
檔案庫說明套表	說明檔案庫資訊
使用者群組說明套表	規劃群組設定檔

請參閱您先前所準備的下列套表：

表 35. 完成資源安全時所需的規劃套表

套表名稱	準備階段：
檔案庫說明套表	繪製應用程式圖解與界定使用者群組
應用程式說明套表	說明應用程式資訊
個別使用者設定檔套表	選擇每一個使用者的值
使用者群組識別套表	訂定使用者群組
系統責任套表	決定誰該負責系統功能
實體安全規劃套表	規劃實體安全

決定資源安全的目標

要開始規劃資源安全，您必須先瞭解您的目標。iSeries 具備彈性化的資源安全施行方式。它可提供您所需的力量，用於保護關鍵的資源。但是資源安全也會對您的應用程式帶來額外的執行時間。例如，每當應用程式需要物件時，系統須先檢查使用者對該物件的權限。因此，您必須在機密性需求與效能成本之間取得平衡。也就是當您進行資源安全的決策時，須衡量安全的價值與相關的成本。

要防止資源安全導致應用程式的效能降低，請遵循下列準則。

- 資源安全保護方法應力求簡單。
- 僅保護必要的物件。
- 透過資源安全來補充 (而非取代) 用於保護資訊的其他工具，例如：
  - 限制使用者只能存取特定功能表與應用程式。
  - 防止使用者輸入指令 (使用者設定檔中的限制功能)。

請藉由定義您的目標，來展開資源安全規劃作業。您可以使用應用程式說明套表或檔案庫說明套表來定義您的安全目標。

至於要使用何種套表，則取決於您是如何在檔案庫中組織相關資訊。

在查看可用於資源安全的權限類型之前，您最好先複查 JKL Toy Company 的安全目標範例。

範例：JKL Toy Company 的安全目標

JKL Toy Company 的 Sharon Jones 使用「檔案庫說明套表」來說明「客戶記錄」檔案庫 (CUSTLIB) 的安全基本要求：

表 36. JKL Toy Company 的檔案庫說明套表：安全目標範例

檔案庫說明套表	1 / 2

表 36. JKL Toy Company 的檔案庫說明套表：安全目標範例 (繼續)

定義檔案庫的安全目標，如：是否有機密資訊：	如今，公司人員都能查看客戶資訊及客戶訂單。為保護資訊的精確度，我們應該限制人員變更資訊。

Sharon 使用「合約與計價」應用程式的「應用程式說明套表」來說明整個應用程式的安全目標。

表 37. JKL Toy Company 的應用程式說明套表：安全目標範例

應用程式說明套表	1 / 2
定義檔案庫的安全目標，如：是否有機密資訊：	關於合約及特殊計價的資訊是機密。只有少數獲得授權的人員可以查看及變更： • 「市場行銷」人員及所有管理者都需要建立、變更及分析合約。他們需要使用檔案和程式。 • 「訂單處理」人員在輸入及訂單出貨時，可以間接地變更合約及檢視價格。但是，他們不可以查看合約與計價，除非是要輸入或變更訂單。

請在「應用程式說明套表」或「檔案庫說明套表」中，寫下應用程式的安全目標。接著，您可以複查一些可用來規劃資源安全的權限類型。

瞭解權限的類型

在您決定資源安全的目標，並將所作決策記錄至「檔案庫說明」套表後，即可開始規劃權限類型。資源安全可定義使用者如何存取系統上的物件。

權限意指某人獲得何種授權來使用物件。例如，您可能具有檢視資訊或變更系統資訊的權限。系統提供有數種不同的權限類型。 IBM 將這些權限類型區分爲不同種類，稱爲**系統定義的權限**，它們可滿足大部份人的需求。下表所列即爲相關種類，以及如何將其用於保護檔案與程式。

註: 當您要規劃權限時，請參閱下列表格。

表 38. 系統定義的權限

權限名稱	允許對檔案執行的作業	不允許對檔案執行的作業	允許對程式執行的作業	不允許對程式執行的作業
*USE	檢視檔案中的資訊。	變更或刪除檔案中的任何資訊。刪除檔案。	執行程式。	變更或刪除程式。
*CHANGE	檢視、變更及刪除檔案中的記錄。	刪除或清除整個檔案。	變更程式的說明。	變更或刪除程式。
*ALL	建立及刪除檔案。新增、變更及刪除檔案中的記錄。授權他人使用檔案。	無	建立、變更及刪除程式。授權他人使用程式。	變更程式的擁有者，如果該程式採用權限。
*EXCLUDE[1]	無	可隨意存取檔案。	無	可隨意存取程式。

表 38. 系統定義的權限 (繼續)

權限名稱	允許對檔案執行的作業	不允許對檔案執行的作業	允許對程式執行的作業	不允許對程式執行的作業
1 *EXCLUDE 會置換您公開或透過群組設定檔所授予的任何權限。				

瞭解物件權限與檔案庫權限如何一起運作

若要設計簡單的資源安全，可嘗試規劃整個檔案庫的安全。爲達此目的，您必須瞭解系統定義的權限是如何應用至檔案庫，如下表所示：

表 39. 系統定義的檔案庫權限

權限名稱	允許的作業	不允許的作業
*USE	• 對檔案庫中的物件而言，特定物件權限所允許的任何作業。 • 對檔案庫而言，檢視說明資訊。	• 新增物件至檔案庫。 • 變更檔案庫說明。 • 刪除檔案庫。
*CHANGE	• 對檔案庫中的物件而言，特定物件權限所允許的任何作業。 • 新增物件至檔案庫。 • 變更檔案庫說明。	• 刪除檔案庫。
*ALL	• 所允許的任何變更動作。 • 刪除檔案庫。 • 授權他人使用檔案庫。	• 無

您還須瞭解檔案庫與物件權限彼此如何運作。下表所示即爲物件與檔案庫所需的權限範例：

表 40. 檔案庫權限與物件權限如何一起運作

物件類型	作業	所需的物件權限	所需的檔案庫權限
檔案	變更資料	*CHANGE	*USE
檔案	刪除檔案	*ALL	*USE
檔案	建立檔案	*ALL	*CHANGE
程式	執行程式	*USE	*USE
程式	變更 (重新編譯) 程式	*ALL	*CHANGE
程式	刪除程式	*ALL	*USE

目錄權限類似於檔案庫權限。您須具有物件路徑名稱中所有目錄的權限，才可存取該物件。

現在您已準備就緒，可以開始規劃應用程式檔案庫的安全。

規劃應用程式檔案庫的安全

當您已決定資源安全的目標後，便可開始規劃應用程式檔案庫的安全。請在參考此處所述之處理的同時，選擇一個您的應用程式檔案庫來進行處理。如果您的系統是將檔案與程式分開存放在不同的檔案庫中，請選擇內含檔案的檔案庫。完成此主題後，再針對其餘應用程式檔案庫重複這些步驟。

複查您就應用程式與檔案庫所收集的相關資訊：

- 「應用程式說明」套表
- 「檔案庫說明」套表
- 需要該檔案庫之任何群組的「使用者群組說明」套表
- 您的應用程式、檔案庫及使用者群組圖解

思考哪些群組需要檔案庫中的資訊，之所以需要的原因，以及它們如何加以使用。

決定檔案庫的內容

應用程式檔案庫含有重要的應用程式檔案。另外也可能包含其他物件，其中大多數是用來使應用程式正確運作的程式設計工具，例如：

- 工作檔
- 資料區與訊息佇列
- 程式
- 訊息檔
- 指令
- 輸出佇列

除了檔案與輸出佇列外，物件多半不會造成安全缺口。它們通常只含少量的應用資料，且所採用的格式不易遭到破解。您可以利用「顯示檔案庫」指令，列出檔案庫中所有物件的名稱與說明。例如，要列出 CONTRACTS 檔案庫的內容：`DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)`

接著，您必須決定對應用程式檔案庫與程式檔案庫而言您需要哪種公用權限。

決定應用程式檔案庫的公用權限

就資源安全的目的而言，**公用**意指您授權其登入您的系統的任何人。如果您對物件沒有更特定的存取權限限制，**公用權限**可允許使用者存取該物件。除了爲檔案庫中的既有物件決定公用權限外，您還可對稍後新增至檔案庫的任何新物件指定公用權限。欲達此目的，您可以使用**建立權限 (CRTAUT)** 參數。一般情況下，檔案庫物件的公用權限應和新物件的檔案庫建立權限相同。

QCRTAUT (建立權限) 系統值會決定新物件的全系統公用權限。 IBM 出貨時已將 QCRTAUT 系統值設成 *CHANGE。請避免變更 QCRTAUT，因爲許多系統功能都會用到它。如果針對應用程式檔案庫的「建立權限 (CRTAUT)」參數指定 *SYSVAL，它將使用 QCRTAUT 系統值 (*CHANGE)。

儘可能使用公用權限，如此可提高簡易度與效能。若要決定檔案庫應採行的公用權限，請提問下列問題：

- 公司中的每個人是否都應該有權存取此檔案庫中的大部份資訊？

- 對於此檔案庫中的大部份資訊而言，人們應具備哪種存取權限？

請先專注於大多數人員以及大多數資訊的決策上。之後，您將學會如何處理異常狀況。規劃資源安全通常是一種循環處理。您會發現在考慮特定物件的需求後，您必須變更公用權限。在您選出最能滿足您的安全與效能需求的方式前，請對物件與檔案庫嘗試不同的公用與專用權限組合。

確保適當的權限

物件的 *CHANGE 權限加上檔案庫的 *USE 權限應足以因應大部份的應用程式功能。不過，您必須先詢問程式設計師或應用程式供應商，才可決定某些應用程式功能是否需要更多權限：

- 進行處理作業時，檔案庫中是否有任何檔案或其他物件會遭到刪除？是否有任何檔案被清除？是否有成員新增至任何檔案？刪除物件、清除檔案或新增檔案成員都需要物件的 *ALL 權限。
- 進行處理作業時，是否會在檔案庫中建立任何檔案或其他物件？建立物件需要檔案庫的 *CHANGE 權限。

在決定程式庫的公用權限之前，最好先參考範例瞭解 Sharon 在物件權限方面所作的選擇。

範例：JKL Toy Company 的檔案庫說明套表

Sharon Jones 複查了「客戶記錄」檔案庫的安全目標，以及使用客戶資訊之應用程式及部門的相關資訊。她寫下了她的結論：

- 各部門都需要變更客戶資訊，除了「倉儲部門」及「製造部門」。
- 「倉儲部門」及「製造部門」的使用者的使用者設定檔都有「限制功能」(是)，而且都限制在幾個功能表或程式上。他們的功能表只能檢視客戶資訊，但不能變更。
- 「客戶記錄」檔案庫中的物件公用權限，可以設定為 *CHANGE。限制功能表，可以防止未獲授權者變更客戶資訊。但日後若有其他部門加入系統，則應該重新評估。

這是寬鬆的資訊處理範例。它以使用者設定檔 (而非權限限制) 來處理異常。 Sharon 在「客戶記錄」檔案庫 (CUSTLIB) 的檔案庫說明套表中填寫了公用權限部份。

表 41. JKL Toy Company 的檔案庫說明套表--第 1 部份：客戶記錄範例

檔案庫名稱：CUSTLIB	描述性名稱 (文字)：客戶記錄
檔案庫的公用權限：	*USE
檔案庫物件的公用權限：	*CHANGE
新物件的公用權限 (CRTAUT)：	*CHANGE

Sharon Jones 發現「應收帳款」應用程式的月底處理程序，會清除「客戶記錄」檔案庫中的部份暫存檔。她選擇個別處理那些檔案的權限，以免不慎刪除檔案庫中的其他物件。至於其他處理活動，*CHANGE 權限應該足夠。

雖然只有少數人員執行月底處理程序，Sharon 並不認爲暫存檔有任何安全風險。她決定提供公用 *ALL 權限給那些檔案，而不是只將權限提供給執行月底處理程序的人員。下表顯示「客戶記錄」檔案庫的檔案庫說明套表的第 2 部份：

表 42. JKL Toy Company 的檔案庫說明套表--第 2 部份：客戶記錄範例

列出檔案庫物件的特定權限				
群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

現在您可以根據所需決定程式庫的公用權限。

決定程式庫的公用權限

應用程式有別於檔案與其他物件，多半是放在單獨的檔案庫中。雖然應用程式不一定要使用單獨的檔案庫，但許多程式設計師在設計應用程式時都是採用此技巧。如果您的應用程式具有專屬的程式庫，您必須決定這些程式庫的公用權限。雖然在檔案庫與其中的程式使用 *USE 權限即可有效執行程式，但程式庫中可能其他物件需要額外的權限。請向您的程式設計師提問一些問題：

- 應用程式是否會用資料區或訊息佇列來進行程式間的通信？它們是否放在程式庫中？要處理資料區與訊息佇列，須具有物件的 *CHANGE 權限。
- 進行處理作業時，是否會刪除程式庫中的任何物件 (例如資料區)？要刪除物件須具有物件的 *ALL 權限。
- 進行處理作業時，是否會在程式庫中建立任何物件 (例如資料區)？要在程式庫中建立任何新物件將需要檔案庫的 *CHANGE 權限。

將所有資源安全資訊填入檔案庫說明套表的兩大部份，但保留檔案庫擁有者與授權清單直欄。然後便可決定檔案庫與物件的所有權。

您最好先參閱下列兩個範例，瞭解 Sharon Jones 如何決定程式庫的權限。在第一個範例中，Sharon 決定對「客戶訂單」程式庫採用不限制的方法。第二個範例則是 Sharon 對「應收帳款」程式庫所採用的較具限制性的方式。

範例：JKL Toy Company 的檔案庫說明套表--無限制的作法

Sharon Jones 研究「客戶訂單」程式庫後，寫下這些附註：

- 程式間通信時，使用一個訊息佇列 COMSGQ01。
- 只清除訊息佇列，不刪除。*CHANGE 權限對訊息佇列而是足夠的。

Sharon 決定提供 *USE 權限給程式庫中的所有物件，並另外定義 COMSGQ01 訊息佇列。下列兩個表格顯示她爲 COPGMLIB 程式庫製作的檔案庫說明套表：

表 43. JKL Toy Company 的檔案庫說明套表：程式庫範例

檔案庫說明套表	**1 / 2**
檔案庫名稱：COPGMLIB	描述性名稱 (文字)：客戶訂單程式庫
檔案庫的公用權限：*USE 檔案庫物件的公用權限：*USE 新物件的公用權限 (CRTAUT) ：*USE 檔案庫擁有者：	

表 44. JKL Toy Company 的檔案庫說明套表：程式庫範例

檔案庫說明套表				**2 / 2**
列出檔案庫中個別物件的權限				
群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

使用程式權限來控制存取

雖然 JKL Toy Company 的多數人員可以變更客戶資訊，但只有少數人員可以設定客戶信用限制。信用限制儲存在客戶主檔案 (CUSTMAS) 中，但必須由 ARPGMLIB 中的個別程式 ARPGM12 來變更。Sharon 可以限制這個程式，防止未獲授權者變更信用限制。下列表格顯示 ARPGMLIB 的「檔案庫說明套表」：

表 45. JKL Toy Company 的檔案庫說明套表：個別權限範例

檔案庫說明套表	**1 / 2**
檔案庫名稱：ARPGMLIB	描述性名稱 (文字)：應收帳款程式庫
檔案庫的公用權限：*USE 檔案庫物件的公用權限：*USE 新物件的公用權限 (CRTAUT) ：*USE 檔案庫擁有者：	

表 46. JKL Toy Company 的檔案庫說明套表：個別權限範例

檔案庫說明套表				**2 / 2**
列出檔案庫中個別物件的權限				
群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

也許您想在決定檔案庫及物件的所有權之前，先複查使用採用權限的限制範例。

範例：JKL Toy Company 的檔案庫說明套表--限制的作法

目前爲止的範例皆顯示寬鬆的安全作法，大多數人可以存取檔案庫資訊。JKL Toy Company 的合約與計價資訊是機密資訊，需要限制性的作法。幸好這方面的資訊都放在個別的檔案庫中。合約與計價的更新程式，也放在特殊的檔案庫中。

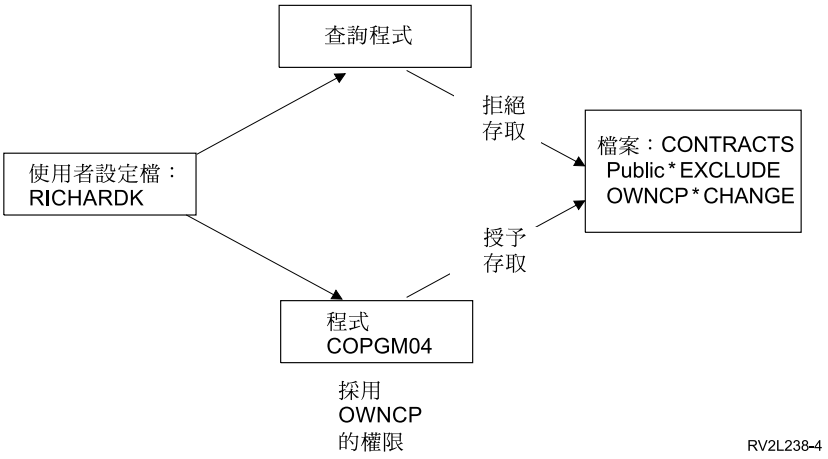
Sharon 複查了「合約與計價」應用程式的安全目標 (請參閱決定您的資源安全目標)。她也複查了「應用程式說明套表」及「檔案庫說明套表」。Sharon 認爲可能不容易達成應用程式的安全目標。她寫了一些附註，並且與應用程式供應商討論問題：

- 「市場行銷」人員及管理者需要建立及變更合約。他們需要使用檔案和程式。

- 「訂單處理」人員在輸入及訂單出貨時可以間接地變更合約及檢視價格，但不能以其他方式檢視合約與計價。不過，他們可以使用「查詢」來建立自己的客戶及訂單報告。如果他們有「合約與計價」檔案的權限，即可建立「查詢」程式來檢視或列印檔案。

JKL Toy Company 的應用程式供應商，建議使用安全採用權限特性來解決這個問題。**採用權限**能讓使用者在程式執行期間，採用程式擁有者的權限。使用者不需要物件的權限。

下圖顯示採用權限的運作範例。「訂單處理部門」的 Karen Richards (RICHARDK)，通常沒有「合約」檔案的使用權限。但她輸入訂單時，需要檢查及更新合約餘額。使用合約餘額 (COPGM04) 的訂單輸入程式，採用 OWNCP 設定檔權限。Karen 執行 COPGM04 程式時，具有合約檔案的使用權限：



有關物件所有權的詳細資訊，請參閱決定檔案庫及物件的所有權主題。應用程式供應商或程式設計師可以在建立 (編譯) 程式時指定程式採用擁有者權限，或者程式設計師可以使用「變更程式 (CHGPGM)」指令來指定程式的採用權限。使用這項技術之前，請務必瞭解程式的所有功能。

Sharon 決定使用採用權限功能，讓「業務及行銷部門」以外的人員也能存取「合約與計價」檔案。她也判定 *CHANGE 存取權對「合約與計價」應用程式使用的所有物件而言已經足夠。下表顯示「合約」檔案庫的「檔案庫說明套表」：

表 47. JKL Toy Company 的檔案庫說明套表：限制權限範例

檔案庫說明套表	**1 / 2**
檔案庫名稱：CONTRACTS	描述性名稱 (文字)：合約與計價檔案庫
檔案庫的公用權限：*EXCLUDE 檔案庫物件的公用權限：*CHANGE 新物件的公用權限 (CRTAUT)：*CHANGE 檔案庫擁有者：	

表 48. JKL Toy Company 的檔案庫說明套表：限制權限範例

檔案庫說明套表	**2 / 2**

表 48. JKL Toy Company 的檔案庫說明套表：限制權限範例 (繼續)

列出檔案庫中個別物件的權限				
群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

您不需要限制檔案庫物件的權限，因爲您已經限制存取檔案庫本身。此外，Sharon 也提供權限給管理者及「業務及行銷部門」。她使用群組權限，而不是提供權限給部門中的每一個人員。

註: 一個經驗豐富的程式設計師只要有檔案庫存取權，即使您撤回檔案庫權限，他仍能留有檔案庫物件的存取權。如果檔案庫物件的安全要求高，爲完全保護物件，請限制物件及檔案庫。

也許您想在決定檔案庫及物件的所有權之前，先複查使用公用權限的無限制範例。

決定檔案庫與物件的所有權

在您規劃應用程式檔案庫的安全後，便可決定檔案庫與物件的所有權。每個物件在建立時都會被指派一名擁有者。物件的擁有者會自動具有對該物件的所有權限，包括授權他人使用該物件、變更該物件以及刪除物件。安全主管可對系統上的任何物件執行這些功能。

系統會透過物件擁有者的設定檔來追蹤誰對物件具有權限。系統會在內部完成此功能。雖然這不會直接影響使用者設定檔。不過，如果您未正確規劃物件所有權，某些使用者設定檔將變得極爲龐大。

當系統儲存物件時，也會一併儲存其擁有者設定檔的名稱。日後需要復置物件時，系統便會使用此資訊。如果被復置物件的擁有者設定檔不存在系統上，系統會把所有權移轉給名爲 QDFTOWN 的設定檔，這是 IBM 隨附的設定檔。

建議

下列建議事項適用於許多 (但非全部) 狀況。參考建議事項後，請就物件所有權與程式設計師或應用程式供應商討論您的想法。如果您是外購應用程式，您可能無法控制哪個設定檔擁有檔案庫與物件。因爲應用程式在設計上可能會防止變更所有權。

- 避免將 IBM 隨附設定檔 (例如 QSECOFR 或 QPGMR) 作爲應用程式擁有者。此類設定檔擁有 IBM 隨附檔案庫中的許多物件，而且已非常龐大。
- 一般而言，群組設定檔不得擁有應用程式。除非您特別指派較低的權限，否則群組中的每個成員皆擁有與群組設定檔相同的權限。事實上，您會將完整的應用程式權限授予每位群組成員。
- 如果您想將控制應用程式的責任分派給各部門的經理，這些經理將是所有應用程式物件的擁有者。不過，應用程式的經理可能會變更職責。遇到此情形，您必須將所有應用程式物件的所有權，移轉給新的經理。

- 許多人常用的技巧是針對各個應用程式建立一個特殊的擁有者設定檔，將其密碼設成 *NONE 。系統會運用此擁有者設定檔來管理應用程式的權限。安全主管 (或具有同樣權限的人) 將實際負責執行應用程式的管理作業，或交由具備特定應用程式之 *ALL 權限的管理者來分擔責任。

決定哪些設定檔應擁有您的應用程式。將擁有者設定檔資訊輸入每一份檔案庫說明套表。

在您開始決定使用者檔案庫的所有權與存取權限之前，最好先參考範例以瞭解 JKL Toy Company 如何決定應用程式所有權。

範例：JKL Toy Company 的應用程式所有權

Sharon Jones 決定爲每一個應用程式建立一個特殊擁有者設定檔。她和 Ken Harrison (安全主管代理人) 負責管理應用程式的安全。日後如果公司的安全要求變得更複雜，Sharon 可以將管理權限的部份責任交給部門管理者。

Sharon 在她的「命名慣例套表」中新增一項登錄：

表 49. JKL Toy Company 的命名慣例套表：擁有者設定檔範例

物件類型	命名慣例
擁有者設定檔	每一個應用程式建立一個擁有者設定檔。它擁有所有應用程式檔案庫以及應用程式檔案庫中的物件。擁有者設定檔的名稱是 OWN 加上應用程式的縮寫。「庫存控制」擁有者設定檔的名稱是 OWNIC。

Sharon 決定讓擁有者設定檔的名稱以 OWN 開頭，這樣所有擁有者設定檔都會出現在顯示畫面及清單中。

Sharon 將擁有者指派到所有應用程式檔案庫，並在「命名慣例套表」中輸入這項資訊。唯一可能有多個應用程式擁有者的檔案庫是「客戶記錄」檔案庫。「應收帳款」應用程式要用來建立新客戶以及設定信用限制，因此 Sharon 認爲它應該擁有客戶檔案。這些是她指派的擁有者：

檔案庫名稱	擁有者名稱
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

現在您可以決定您的使用者檔案庫的所有權和存取權。

決定使用者檔案庫的所有權與存取權

如果您的系統上有安裝 IBM Query for iSeries 授權程式或其他決策支援程式，您的使用者將需要檔案庫來儲存他們所建立的查詢程式。一般而言，此檔案庫即爲使用者設定檔中的**現行檔案庫**。有關如何爲各個使用者建立現行檔案庫的詳情，請參閱《選擇會影響登入的值》。 Sharon Jones 打算將現行檔案庫用於「業務及行銷」部門，並將群組檔案庫用於其他部門：

- 「業務及行銷」人員將會大量使用「查詢」功能。因此每位使用者應具備專用的檔案庫。不然，他們將擔心如何為查詢作業命名，而且可能會意外刪除彼此的程式。
- 開始時，其他部門將使用群組檔案庫。如果他們會建立許多「查詢」程式，我們可考慮賦予個別的檔案庫。

若使用者隸屬某一群組，您可用使用者設定檔中的欄位來指定究竟是使用者或群組擁有使用者所建的任何物件。如果是使用者擁有物件，您可以指定群組成員對使用該物件所擁有的權限。您也可以指定群組的權限是否爲主群組權限或專用權限。主群組權限具有較佳的系統效能。Sharon 作了一些有關使用者檔案庫的附註：

- 「業務及行銷」人員應擁有其所建的物件，而非由群組擁有。他們不須變更彼此的查詢程式。
- 群組中的每個人應能執行彼此的「查詢」程式，亦即群組對其成員所建的任何物件皆具有 *USE 權限。
- 群組的權限須為主群組權限。
- 大眾不得存取這些檔案庫。因為「業務及行銷」人員可能會從查詢作業輸出檔案。而這些檔案中可能含有機密資料。
- 對其他部門而言，群組將擁有群組檔案庫以及檔案庫中所建立的任何事物。亦即任何群組成員皆可變更或刪除檔案庫內的所有事物。如果這會造成問題，我們可能須嘗試其他方法。

下表所示爲「業務及行銷」部門的「個別使用者設定檔套表」，該部門會用到使用者擁有的物件：

表 50. JKL Toy Company 的個別使用者設定檔套表：使用者擁有物件的範例

群組設定檔名稱：DPTSM	
所建物件的擁有者：*USRPRF	群組對所建物件的權限：*USE
群組權限類型：*PGP	

下表所示爲由群組擁有物件之部門的「個別使用者設定檔套表」：

表 51. JKL Toy Company 的個別使用者設定檔套表：群組擁有物件的範例

群組設定檔名稱：DPTxx	
所建物件的擁有者：*GRPPRF	群組對所建物件的權限：

如果所建物件的擁有者是群組，**群組對所建物件的權限**欄位即不會用到。群組成員會對任何已建物件自動擁有 *ALL 權限。

決定誰該擁有且得以存取使用者檔案庫。在個別使用者設定檔套表的**所建物件的擁有者** 與**群組對物件的權限**兩個欄位輸入您的選擇。現在您可開始將物件分組。

將物件分組

待已決定檔案庫與物件的所有權後，您即可開始將系統上的物件予以分組。爲簡化相關權限的管理，請使用授權清單把具有相同需求的物件納入同一群組。之後便可對整個授權清單而非個別的物件，來授予公用權限、群組設定檔權限及使用者設定檔權限。系統雖會將您透過授權清單來保護的每個物件一視同仁，不過您在整個清單中可爲不同使用者提供不同的權限。

當您復置物件時，授權清單可讓權限的重建作業較爲容易。如果您透過授權清單來保護物件，復置處理會自動將物件鏈結至授權清單。

您可以對群組或使用者授予管理授權清單的權限 (*AUTLMGT)。授權清單管理可讓使用者在清單中新增或移除其他使用者，以及變更這些使用者的權限。

建議

- 針對需要安全保護以及具有類似安全需求的物件來使用授權清單。使用授權清單可讓您專注於思考權限種類而非個別權限。授權清單還可簡化物件的復置作業，以及系統相關權限的審核。
- 避免採用結合了授權清單、群組權限和個別權限的複雜保護方式。選擇最符所需的方法，而非同時使用所有方法。

您還須將授權清單的命名慣例新增至您的命名慣例套表。

一旦備妥授權清單套表後，請回頭將其資訊新增至您的檔案庫說明套表。您的程式設計師或應用程式供應商可能已建立了授權清單。因此請務必要詢問他們。

在規劃印表機與印表機輸出的安全之前，若先參考範例瞭解 JKL Toy Company 的 Sharon Jones 如何規劃授權清單將十分有用。

範例：JKL Toy Company 的授權清單套表

Sharon 複查了「客戶記錄」檔案庫的「檔案庫說明」，並決定爲每月底清除的檔案建立一個授權清單。雖然只清除三個檔案，Sharon 仍然決定使用授權清單來簡化權限管理。如果日後月底處理程序要新增其他檔案，只需將這些檔案放入授權清單中即可完成安全保護。Sharon 決定排除檔案的公用權限，以防月底處理程序出現非預期的問題。她只提供 *ALL 權限給執行此處理程序的使用者。Rose Willis 是晚班系統操作員，她可能需要檢視檔案資訊來檢查月底處理程序。她需要 *USE 權限。

下表顯示 Sharon 使用的授權清單命名慣例：

表 52. JKL Toy Company 的命名慣例套表：授權清單範例

命名慣例套表	
準備人員：Sharon Jones	日期：9/5/99
物件類型	**命名慣例**
授權清單	保護檔案庫中物件安全的清單名稱，是部份檔案庫名稱加上 LST 和一個數字。CUSTLIB 中的物件清單名稱是 CUSTLST1。多個檔案庫中的物件清單名稱，則使用應用程式的縮寫 (如果可能)：ARLST1。如果清單套用於多個應用程式，請選取任何有意義的名稱。清單說明應該指出它的主要目的。

下表顯示 CUSTLIB 檔案庫的「授權清單套表」。Sharon 使用「檔案庫說明套表」資訊來準備這個套表：

表 53. JKL Toy Company 的授權清單規劃：範例

授權清單套表
授權清單名稱：CUSTLST1
說明：月底處理程序清除的檔案。
列出清單中的物件

表 53. JKL Toy Company 的授權清單規劃：範例 (繼續)

物件名稱	物件類型	物件檔案庫	物件名稱	物件類型	物件檔案庫
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
列出可以存取清單的群組及使用者					
群組或使用者	容許的存取類型	清單管理？	群組或使用者	容許的存取類型	清單管理？
PUBLIC	*EXCLUDE	否	ROSSG	*ALL	否
SMITHJ	*ALL	否	JONESS	*ALL	是
WILLISR	*USE	否			

Sharon 還將授權清單資訊新增到 CUSTLIB 檔案庫的「檔案庫說明套表」中：

檔案庫說明套表				2 / 2
準備人員：Sharon Jones			日期：9/9/99	
檔案庫名稱：CUSTLIB				
列出檔案庫物件的特定權限				
群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

請注意，每一個檔案的公用權限都必須變更爲 *AUTL，系統才能使用授權清單來決定公用權限。

請查看「檔案庫說明套表」中的群組及個別權限，判斷是否適合使用授權清單。如果適合，請準備「授權清單套表」，並使用授權清單資訊來更新「檔案庫說明套表」。接著，您可以規劃印表機及印表機輸出的安全。

規劃印表機與印表機輸出的安全

在將物件分組後，您必須規劃如何保護印表機輸出。先前您已擬妥保護系統資訊的計劃。下來還須規劃如何在進行列印與等待列印時保護機密資訊。請就貴公司用於列印機密輸出的印表機，檢查您的「實體安全計劃」。

當您執行用來列印報表的程式時，報表通常不會直接送往印表機。程式會先建立該報表的副本，稱作**排存檔**或**印表機輸出**。然後系統會將排存檔存入名爲**輸出佇列**的物件中，等候印表機可供使用。當輸出佇列含有印表機輸出時，您可在工作站上檢視報表。也可加以保留或轉送至特定的印表機。

排存作業可讓安排列印工作與共用印表機等作業更爲簡易。它還可協助您保護機密輸出。您可以建立一或多個特殊輸出佇列，用來保留機密輸出並限制誰可以檢視與管理這些輸出佇列。還可以控制何時將機密輸出由佇列送往印表機。

請在查看本主題的同時，填妥印表機輸出與工作站安全套表。

當您建立特殊輸出佇列時，可以指定數種與安全有關的參數：

- **顯示資料 (DSPDTA) 參數**：輸出佇列的 DSPDTA 參數可決定使用者是否可以檢視、傳送或複製另一使用者所擁有的排存檔。
- **檢查權限 (AUTCHK) 參數**：輸出佇列的 AUTCHK 參數可決定使用者是否可以變更或刪除另一使用者所擁有的排存檔。
- **操作員控制 (OPRCTL) 參數**：輸出佇列的 OPRCTL 參數可決定是否允許具有 *JOBCTL 特殊權限 (或 *SYSOPR 使用者類別) 的使用者控制輸出佇列。

輸出佇列參數、使用者對輸出佇列的權限以及使用者的特殊權限，三者將共同決定使用者可對輸出佇列中的排存檔執行的功能。下表所示爲不同組合下使用者可執行的各種功能：

列印功能	輸出佇列參數			輸出佇列權限	特殊權限
	DSPDTA	**AUTCHK**	**OPRCTL**		
新增排存檔至佇列 [1]	任意	任意	任意	*READ	無
	任意	任意	*Yes	任意	*JOBCTL
檢視排存檔的清單 (WRKOUTQ 指令)[2]	任意	任意	任意	*READ	無
	任意	任意	*Yes	任意	*JOBCTL
顯示、複製或傳送排存檔 (DSPSPLF、CPYSPFL、SNDNETSPLF、SNTCPSPLF)[2]	*YES	任意	任意	*READ	無
	*NO	*DTAAUT	任意	*CHANGE	無
	*NO	*OWNER	任意	擁有者[3]	無
	*YES	任意	*Yes	任意	*JOBCTL
	*NO	任意	*Yes	任意	*JOBCTL
	*OWNER[5]	任意	任意	任意	任意
變更、刪除、保留、釋放排存檔 (CHGSPLFA、DLTSPLF、HLDSPLF、RLSSPLF)[2]	任意	*DTAAUT	任意	*CHANGE	無
	任意	*OWNER	任意	擁有者[3]	無
變更、清除、保留及釋放輸出佇列 (CHGOUTQ、CLROUTO、HLDOUTQ、RLSOUT)[2]	任意	*DTAAUT	任意	*CHANGE	無
	任意	*OWNER	任意	擁有者[3]	無
	任意	任意	*YES	任意	*JOBCTL
啓動佇列寫出器 (STRPRTWTR、STRRMTWTR)[2]	任意	*DTAAUT	*任意	*CHANGE[4]	無
	任意	任意	*YES	任意[4]	*JOBCTL

1 這是將您的輸出轉送至輸出佇列時所需的權限。

2 請從顯示器使用這些指令或對等選項。

3 您必須是輸出佇列的擁有者。

4 還需要印表機裝置說明的 *USE 權限。

5 您必須是排存檔的擁有者，或具有使用指令 *SPLCTL 的特殊權限。

複查「實體安全計劃」的印表機部份。在查看本主題的同時，請填寫印表機輸出與工作站安全套表的輸出佇列區段。

在您規劃工作站的資源安全之前，若能複查範例將十分有用，其間可參考 JKL Toy Company 的 Sharon Jones 是如何決定這些輸出佇列參數。

範例：JKL Toy Company 的輸出佇列及工作站安全套表--輸出佇列部份

JKL Toy Company 的「業務及行銷部門」對機密列印有兩個基本要求：

- 規劃變更價格時，列印初步價格清單。「業務及行銷部門」以外的人員 (公司主管除外) 看不到這項資訊。
- 在協商的過程中，合約是機密。只有負責協商合約的人員看得到合約初稿，「業務及行銷部門」的其他人員看不到。

Sharon 決定建立兩種特殊輸出佇列：

PRICEQ

用於初步價格清單。「業務及行銷部門」人員都能執行這個輸出佇列的所有功能。部門外的人員不能使用這個輸出佇列，包括系統操作員。PRICEQ 在 CONTRACTS 檔案庫中。

NEWCP

用來列印協商的合約。「業務及行銷部門」人員可以共用輸出佇列，但只有在輸出佇列中建立排存檔的人員可以控制這個檔案。 NEWCP 在 CONTRACTS 檔案庫中。

下表顯示 Sharon 爲這些輸出佇列準備的「輸出佇列及工作站安全套表」：

表 54. JKL Toy Company 的輸出佇列及工作站安全套表：印表機輸出佇列範例

列出限制輸出佇列的參數：				
輸出佇列名稱	輸出佇列檔案庫	顯示任何檔案 (DSPDTA)	檢查權限 (AUTCHK)	操作員控制 (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

決定程式庫的公用權限主題中有 JKL Toy Company 的 CONTRACTS 檔案庫權限範例。只有「業務及行銷部門」管理者和成員可以存取檔案庫。檔案庫物件的公用權限 (包括這些輸出佇列) 爲 *CHANGE。

NEWCP 輸出佇列的 AUTCHK 參數爲 *OWNER，因此只有排存檔擁有者可以使用這個檔案 (請參閱上述「執行列印功能時所需的權限」表格)。這可防止「業務及行銷部門」人員列印彼此的新合約或在輸出佇列中檢視合約。

規劃印表機輸出佇列安全之後，您可以規劃工作站安全。

規劃工作站的安全

在規劃印表機與印表機輸出的資源安全後，您即可開始規劃工作站安全。先前在「實體安全計畫」中，您已列出了所在位置有安全風險的工作站。請用此資訊來決定哪些工作站須加以限制。

您可以鼓勵這些工作站的使用者特別注意安全。每當他們離開工作站時即應執行登出。您最好將您對這些易遭入侵之工作站的登出決策記錄在安全原則中。您也可限制此類工作站上所能執行的功能以降低風險。

限制工作站功能的最簡單方法，就是只限具備限制功能的使用者設定檔加以使用。Sharon Jones 即對 JKL Toy Company 的「倉儲部門」採行此技巧。 Sharon 允許在裝載處工作的 Ray Wagner 與 Janice Ames 只能執行收貨程式。她另外還規定只有他們可登入裝載處的工作站。

您可以選擇不准安全主管或具有服務權限的人員登入任意工作站。若以 QLMTSECOFR 系統值作此限制，具有安全主管權限的人員將只能在經過特別授權的工作站上登入。

準備輸出佇列與工作站安全套表的工作站部份。

準備「輸出佇列與工作站安全」套表的工作站部份時，您最好參考範例瞭解 Sharon 如何規劃工作站安全。同時還應參閱資源安全建議事項清單，以確保您的資源安全計劃既簡單又完整。查閱範例與建議事項後，您便可開始規劃您的應用程式安裝。

範例：JKL Toy Company 的輸出佇列及工作站安全套表--工作站部份

Sharon Jones 複查了她的「實體安全規劃」，判斷哪些工作站有安全危機。例如，JKL Toy Company 以外的人員，容易就能在公司裝載處及遠端行銷辦事處存取工作站。Sharon 在「實體安全規劃」中指出，這些工作站有潛伏的安全危機。

限制工作站功能的最簡單方法是使用限制功能來限制使用者設定檔。 Sharon Jones 對 JKL Toy Company 的「倉儲部門」使用這項技術。 Sharon 只容許在裝載處工作的 Ray Wagner 及 Janice Ames 執行庫存接收程式。同時，Sharon 在裝載處也只容許他們登入工作站。

Sharon 重新評估了她選擇的 QLMTSECOFR 系統值。她決定將其設定爲 1 (是) 來加強保護裝載處及遠端行銷辦事處的脆弱工作站。

下表顯示 Sharon 準備的「輸出佇列及工作站安全套表」中的工作站部份。

表 55. JKL Toy Company 的輸出佇列及工作站安全套表：工作站範例

安全主管工作站： 如果您將安全主管限制在特定工作站 (系統值 QLMTSECOFR 爲是)，以下列出安全主管獲得授權的工作站，以及任何有 *ALLOBJ 權限者：以下列出的工作站除外。	
以下列出限制工作站的權限：	
工作站名稱	獲得授權的群組或使用者 (*CHANGE 權限)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

也許您想在規劃您的應用程式安裝之前，先複查資源安全建議摘要。

資源安全建議摘要

完成規劃工作站安全後，您可以複查下列資源安全建議事項。 iSeries 系統提供許多選項，可用來保護系統上的資訊。因此您有很大的彈性來設計最符所需的資源安全計劃。但大量的選項也容易使人混淆。

以 JKL Toy Company 爲例，本主題將示範如何以基本方式來規劃資源安全並且採用下列準則：

- 從一般到特殊：
  - 規劃檔案庫的安全。僅在必要時處理個別物件。
  - 先規劃公用權限，然後是群組權限，最後是個別權限。
- 爲提高效能並簡化備份及回復作業，僅對公用權限仍無法滿足其安全需求的物件定義特定安全機能。
- 使檔案庫中各新物件 (CRTAUT) 的公用權限，和您爲該檔案庫大多數現存物件所定義的公用權限相同。
- 授予群組或個人的權限應儘量高於公用權限。否則會降低效能，進而可能導致錯誤，並使審核作業益加困難。如果您知道每個人至少對公用物件擁有相同權限，您在規劃與審核安全時將較爲容易。
- 透過授權清單，將安全需求相同的物件劃分在一起。授權清單比起個別權限來得容易管理，而且可協助回復安全資訊。
- 建立特殊的使用者設定檔來作爲應用程式擁有者。將擁有者密碼設成 *NONE。
- 避免讓 IBM 隨附設定檔 (例如，QSECOFR 或 QPGMR) 擁有應用程式。
- 對機密報表使用特殊的輸出佇列。將輸出佇列放入和機密資訊所在的相同檔案庫。
- 限制具有安全主管權限的人員數。
- 謹慎處理物件或檔案庫之 *ALL 權限的授予。具有 *ALL 權限的人員往往會意外刪除某些事物。

爲確保順利完成有關設定資源安全方面的規劃作業，您應蒐集下列資訊：

- 針對所有的應用程式檔案庫，填寫檔案庫說明套表的第 1 部份與第 2 部份。
- 在個別使用者設定檔套表上，填寫**所建物件的擁有者**與**群組對所建物件的權限**等欄位。
- 在命名慣例套表上，說明如何爲授權清單命名。
- 準備授權清單套表。
- 將授權清單資訊新增至您的檔案庫說明套表中。
- 準備輸出佇列與工作站安全套表。

現在您已可開始規劃您的應用程式安裝。

規劃您的應用程式安裝

要完成規劃資源安全，您必須準備應用程式安裝作業。下面的主題將協助您在安裝應用程式後，規劃其所有權與權限。此處所說明的方法可能無法適用於所有應用程式。請洽商您的程式設計師或應用程式供應商，協助擬定良好的安裝計劃。

如果您打算向應用程式供應商購置應用程式，請用此資訊來規劃載入應用程式檔案庫之前與之後須執行的安全活動。

如果您打算安裝程式設計師所開發的應用程式，請用此資訊來規劃相關安全活動，使應用程式能從測試階段進入正式作業狀態。

先針對某一應用程式完成所有相關步驟。然後再針對其他應用程式重頭準備「應用程式安裝」套表。

需要哪些套表？

在您查看本主題的同時，請複製下列套表並加以填寫：

表 56. 規劃應用程式安裝作業時所需的規劃套表

套表名稱	所需份數
「應用程式安裝」套表	每支應用程式一份

利用這些您先前準備的套表，來蒐集用於規劃應用程式安裝作業的資訊：

套表名稱	準備階段：
「檔案庫說明」套表	說明檔案庫資訊
「授權清單」套表	將物件分組

在載入您的應用程式主題中，您已學會如何執行安裝應用程式時所需的步驟。

若要規劃您的應用程式安裝，請參閱下列主題：

- 決定應用程式的使用者設定檔與安裝值。
- 變更安裝值。

決定應用程式的使用者設定檔與安裝值

在規劃您的應用程式安裝後，您必須先決定各應用程式的使用者設定檔與安裝值。若要安裝在其他系統上建立的應用程式，您可能須先建立一或多個使用者設定檔。擁有該應用程式檔案庫與物件的使用者設定檔須已存在於系統上，您才可將檔案庫載入至您的系統。請在「應用程式安裝」套表上，記錄下您須爲各檔案庫建立的設定檔以及設定檔所需的參數。

要決定所需的安裝值時，請向您的程式設計師或應用程式供應商詢問下列問題，並在「應用程式安裝」套表上記錄其回答：

- 哪個設定檔擁有應用程式檔案庫？
- 哪個設定檔擁有檔案庫中的物件？
- 檔案庫的公用權限 (AUT) 爲何？
- 新物件的公用權限 (CRTAUT) 爲何？
- 檔案庫中之物件的公用權限爲何？
- 哪些程式 (如果有) 採用了擁有者的權限？

查明您的程式設計師或應用程式供應商是否已爲應用程式建立任何授權清單。針對已建立的每一個授權清單準備「授權清單」套表，或向程式設計師詢問該清單的相關資訊。

您可以自行決定是否應變更任何安裝值。

變更應用程式的安裝值

請將「應用程式安裝」套表上的資訊，與「檔案庫說明」套表的檔案庫資源安全計劃作一比較。如果兩者不同，您必須決定在安裝好應用程式後應該作哪些變更。

變更應用程式所有權

如果您的程式設計師或應用程式供應商已建立特殊設定檔來擁有應用程式檔案庫與物件，請考慮採用該設定檔，即使其不符您的命名慣例。移轉物件的所有權可能極耗時間，應加以避免。

如果 IBM 隨附的群組設定檔之一 (例如 QSECOFR 或 QPGMR) 擁有此應用程式，您應在安裝好應用程式後，將所有權移轉給另一設定檔。

程式設計師有時會將應用程式設計成不准變更物件所有權。在滿足您本身安全管理需求的同時，請儘量遵循此限制。不過，如果 IBM 隨附的設定檔 (例如 QSECOFR) 擁有該應用程式，您以及您的程式設計師或應用程式供應商即必須擬訂計劃來變更所有權。您最好是事先變更所有權，然後才安裝應用程式。

變更公用權限

當儲存物件時，您也會一併儲存其公用權限。當您將應用程式檔案庫復置到系統上時，檔案庫及其所有物件將具有和儲存時相同的公用權限。即使您在其他系統上儲存檔案庫，情況仍然一樣。

檔案庫的 CRTAUT 值 (新物件的公用權限) 並不影響所復置的物件。物件將回復其儲存時的公用權限，不論檔案庫的 CRTAUT 值爲何。

您應變更檔案庫與物件的公用權限，以符合您在「檔案庫說明」套表上所列的計劃。

規劃您的應用程式安裝時，您最好先參考範例，瞭解 JKL Toy Company 的 Sharon Jones 如何規劃應用程式安裝作業。

爲確保您完整規劃了您的應用程式安裝作業，您應該：

- 填妥您的第一份應用程式安裝套表。然後回頭爲其餘每支應用程式準備相關套表。
- 複查所有套表，並確定套表的完整。製作套表副本，並將其存放在安全之處，直到安裝好您的系統以及授權程式。

完成這些規劃作業後，您即可設定您的使用者安全。

範例：JKL Toy Company 應用程式安裝套表

JKL Toy Company 向應用程式供應商採購「客戶訂單」及「應收帳款」應用程式。他們外聘一位程式設計師來開發「合約與計價」應用程式，並將它鏈結至「客戶訂單」應用程式。

Sharon Jones 使用「檔案庫說明套表」中的資訊來準備「應用程式安裝套表」。下表顯示 Sharon 的 CUSTLIB「檔案庫說明」套表複本：(請參閱說明檔案庫資訊主題)

表 57. JKL Toy Company 的檔案庫說明套表：範例

檔案庫說明套表	**1 / 2**
準備人員：Sharon Jones	日期：9/9/99
檔案庫名稱：CUSTLIB	描述性名稱 (文字)：客戶記錄檔案庫
簡短說明這個檔案庫的功能：保存全部客戶檔案，包括訂單和帳戶。	
定義檔案庫的安全目標，如：是否有機密資訊： 如今，我們容許公司所有人員查看客戶訂單。 為保護資訊的精確度，我們應該限制人員變更資訊。	

表 57. JKL Toy Company 的檔案庫說明套表：範例 (繼續)

檔案庫的公用權限：*USE
檔案庫物件的公用權限：*CHANGE
新物件的公用權限 (CRTAUT)：*CHANGE
檔案庫擁有者：OWNAR

下表顯示 Sharon 爲「客戶訂單」應用程式準備的「應用程式安裝套表」。請注意，Sharon 決定使用應用程式供應商建立的擁有者設定檔。設定檔 COWNER 同時擁有檔案庫及程式庫。

安裝應用程式之後，Sharon 應該執行下列作業：

- 變更檔案庫的公用權限，以符合「檔案庫說明套表」中的資源安全規劃。
- 將 COWNER 設定檔的使用者類別變更爲 *USER，並移除所有特殊權限。
- 將 COWNER 設定檔的密碼變更爲 *NONE。

表 58. JKL Toy Company 的應用程式安裝套表：範例

應用程式名稱：客戶訂單 (CO)		說明：訂單的輸入、追蹤及出貨。
列出及解釋爲了安裝應用程式而必須建立的設定檔：檔案所屬的程式庫，屬於 COWNER 設定檔。程式庫屬於 QPGMR。		
程式庫名稱：CUSTLIB		
	安裝之前	**安裝之後**
程式庫擁有者	COWNER	COWNER
物件擁有者	COWNER	COWNER
程式庫公用權限	*EXCLUDE	*USE
物件公用權限	*ALL	*CHANGE
新物件的公用權限	*CHANGE	*CHANGE
程式庫名稱：COPGMLIB		
	安裝之前	**安裝之後**
程式庫擁有者	QPGMR	COWNER
物件擁有者	QPGMR	COWNER
程式庫公用權限	*EXCLUDE	*USE
物件公用權限	*ALL	*CHANGE
新物件的公用權限	*CHANGE	*CHANGE

現在您已經完成了規劃作業，接下來可以設定使用者安全。

第 6 章 設定使用者安全

本主題將引導您完成相關作業，利用指令行介面爲您的系統設定使用者安全。如果您是在設定新的系統，您必須依序完成這些步驟。當您逐一進行各步驟時，系統將會使用其間的相關資訊。要設定基本系統安全，您需要完成兩組作業。首先是定義您的使用者安全，其次則是保護系統資源。下方的兩個表格將指明您在設定使用者與資源安全時所需執行的各項步驟。

註: 您**必須**先完成設定使用者安全的所有步驟，才可開始設定資源安全。

表 59. 設定使用者安全時的相關步驟

步驟	此步驟中應執行的作業	應使用的套表
設定您的整體環境	設定起始系統值與網路屬性。建立安全主管使用者設定檔。	「系統值選項」套表
設定安全系統值	設定額外的系統值。	「系統值選項」套表
準備載入應用程式的基本安全步驟	建立擁有者設定檔。載入您的應用程式。應用程式檔案庫與物件須已存在於系統上，您才可執行其餘步驟。	「應用程式安裝」套表
設定使用者群組	建立工作說明、群組檔案庫和群組設定檔。	「使用者群組說明」套表
設定個別使用者	建立個別檔案庫與使用者設定檔。	「個別使用者設定檔」套表

表 60. 設定資源安全時的相關步驟

步驟	此步驟中應執行的作業	應使用的套表
設定所有權及公用權限	建立檔案庫與物件的所有權和公用權限。	「應用程式安裝」套表
建立授權清單	建立授權清單。	「授權清單」套表
設定特定權限	設定檔案庫與個別物件的存取權限。	「檔案庫說明」套表
保護印表機輸出	藉由建立輸出佇列和指派輸出來保護印表機輸出。	「輸出佇列與工作站安全」套表
保護工作站	保護工作站。	「輸出佇列與工作站安全」套表

除了上表所列的主題外，亦請參閱下列主題來協助您管理系統安全：

- 測試安全。
- 變更安全資訊。
- 保存安全資訊。
- 監督安全。

開始之前

如果您是在安裝新的系統，請先執行下列事項後才開始設定安全機能：

- 確定您的主機與相關裝置已安裝妥當並能正確運作。如果不想使用 iSeries 的裝置命名，請在變更了可決定裝置名稱的系統值 (QDEVNAMING) 後，才接裝工作站與印表機。套用新的系統值會說明何時應接上這些裝置。
- 載入任何您想要使用的授權程式。

設定您的整體環境

要開始設定使用者安全，您必須先爲您的使用者設定整體環境。在本主題中，請使用 SETUP 功能表來設定系統值，並建立您自己的使用者設定檔。其間，您還要變更「專用服務工具 (DST)」設定檔的使用者 ID 和密碼。

在下列程序中，您將可找到範例指令行螢幕，螢幕中會列出這些相關步驟。不過，它們都不是完整的螢幕。所顯示的部份僅是完成相關作業所需的資訊。

需要哪些套表？

輸入您在《規劃您的整體安全策略》中所準備的「系統值選項」套表資訊。

若要設定整體環境，您必須完成下列作業：

1. 登入系統。
2. 選取正確的輔助層次。
3. 防止他人登入。
4. 輸入安全系統值。
5. 套用新的系統值。
6. 建立安全主管設定檔。

完成上述步驟後，您必須變更「服務工具」密碼，以防有人誤用。相關詳情請參閱服務工具。

登入系統

要開始設定您的系統環境，您必須先登入系統。

1. 在主控台，以安全主管 (QSECOFR) 身份登入。如果您是初次登入，請使用密碼 QSECOFR。由於系統會將此密碼視爲已過期，因此會提示您加以變更。您必須變更此密碼才能順利登入。
2. 在「登入」顯示器的「*功能表*」欄位中輸入 SETUP。

註: SETUP 功能表稱爲 「自訂您的系統、使用者及裝置」功能表。本文將其通稱爲 SETUP 功能表。

```
                    登入
                                    系統  . . . . . .
                                    子系統  . . . . .
                                    顯示  . . . . . .

使用者  . . . . . . . . . . . . .   QSECOFR
密碼  . . . . . . . . . . . . . .   _________
程式/程序 . . . . . . . . . . . .   _________
功能表  . . . . . . . . . . . . .   SETUP
現行檔案庫  . . . . . . . . . . .   _________
```

登入系統後，您必須選取適當的輔助層次。

選取正確的輔助層次

於登入系統後，您便可爲使用者選擇適當的輔助層次。**輔助層次**會決定您所能見到的顯示器版本。許多系統顯示器皆具有兩種不同的版本：

- 一是基本輔助層次版本，其中含有較少的資訊，而且不使用技術術語。
- 另一是中階輔助層次版本，會顯示較多資訊，而且採用技術術語。

某些欄位或功能只會出現在特定版本的顯示器上。相關指示會告訴您所要使用的版本爲何。若要從某一輔助層次變更爲另一輔助層次，請使用 **F21** (選取輔助層次)。 **F21** 不在所有的顯示器上。

選妥輔助層次後，您必須在設定安全時防止他人登入系統。

防止他人登入

當您選取正確的輔助層次後，您必須防止他人登入系統。如果您擔心系統在尚未受到保護前即遭人侵害，可在另一工作站防止其他人登入。此作業屬選用性質。請僅在您需要暫時安全時才執行此作業：

1. 從 SETUP 功能表，按下 **F9** 來顯示指令行。
2. 在此指令行上，鍵入 GO DEVICESTS。
3. 螢幕即會顯示「裝置狀態作業」功能表。如果您看到「使用配置狀態」功能表，請用 **F21** (選取輔助層次) 來變更爲基本輔助層次。
4. 選取選項 **1** (使用顯示裝置)。
5. 在「使用顯示裝置」顯示器上，讓所有工作站 (除了您正在使用者) 無法使用。其作法是在各工作站名稱前鍵入 **2**，然後按下 **Enter** 鍵。
6. 藉著按兩次 **F3** (跳出)，返回 SETUP 功能表。
7. 按下 **F12** (取消)來移除指令行。

```
                          使用顯示器裝置

請鍵入下列選項，然後按 Enter 鍵。
  1=可使用     2=不可使用    5=顯示
  7=顯示訊息   8=使用控制器與線路
  13=變更說明

選項  裝置         類型     狀態
__    DSP01        3196     QSECOFR
2_    DSP02        3196     可供使用
2_    DSP03        3196     可供使用
2_    DSP04        3196     可供使用
```

當您讓某一裝置無法使用時，即使已開啓電源，它也不會出現「登入」顯示器。工作站會一直保持無法使用，直到您關閉並重新啓動系統。您可能會需要重複此步驟。

在您防止他人登入系統後，即可輸入安全系統值。

輸入安全系統值

當您已防止他人登入後，您必須輸入系統值給系統。

請使用下列程序來輸入「系統值選項」套表之第 1 部份的資訊：

1. 在 SETUP 功能表中，選取選項 **1** (變更系統選項)。
2. 在「變更系統選項」顯示器上，輸入來自「系統值選項」套表的資訊。如果不想變更顯示器上的某些選項，可用 Tab 鍵加以跳過。
3. 如果啓動系統時未設定日期與時間，請在此顯示器上輸入正確者。

4. 鍵入此頁面的資訊後，請換到下一頁。顯示器右下角的*尚有...* 表示至少還有另一頁。

```
                              變更系統選項
系統：
請鍵入下列選項，然後按 Enter 鍵。

系統名稱  . . . . . .  JKLTOY     名稱

日期與時間選項：
  系統日期  . . . . . .  09/21/99     MM/DD/YY
  系統時間  . . . . . .  10:52:57     HH:MM:SS
  日期分隔字元  . . . . . .  1          1=/
                                       2=-
                                       3=.
                                       4=,
                                       5=空白
  日期格式  . . . . . .  MDY          YMD, MDY, DMY, JUL
  時間分隔字元  . . . . . .  1          1=:
                                       2=.
                                       3=,
                                       4=空白


                                                          尚有...
F1=說明   F3=跳出   F5=重整   F12=取消
```

5. 在第二頁鍵入您的選項，然後換到下一頁。

```
                              變更系統選項

請鍵入下列選項，然後按 Enter 鍵。

安全選項：
  安全層次  . . . . . .  40
    :
  允許安全主管
    登入至任何
    顯示站  . . . . . .  N
```

6. 在第三頁鍵入您的選項，然後按 **Enter** 鍵。

```
                              變更系統選項

請鍵入下列選項，然後按 Enter 鍵。

裝置選項：
  新裝置的裝置命名
  格式  . . . . . .  1


  預設系統印表機  . . . . . .  PRT01

額外選項：
  登入時將使用者置於
    S/36 環境中 . . . . . .  N
  儲存關於已完成
    印表機輸出的
    工作帳戶資訊  . . . . . .  Y
```

7. SETUP 功能表應該會再次出現。請注意位於顯示器底端的訊息：**系統選項已順利變更。需要 IPL。**

註: 系統唯有在您變更了安全層次時才需要 IPL。

在大部份的系統作業主題末尾，您都會看到一份表格，說明可能的錯誤情況與回復步驟。如果您的作業結果與所述的不同，請利用這些表格來協助您更正。雖然這些表格可能無法涵蓋所有問題，但其目的旨在引導您解決問題，並讓您在使用系統時更加上手。

可能的錯誤	回復方式
出現 MAIN 功能表。	您按到 **F3** (跳出) 或 **F12** (取消)。請鍵入 GO SETUP，並重試一次。
出現另一個顯示器，例如「變更清除選項」顯示器。	您從 SETUP 功能表 選取了錯誤的選項。請按 **F3** (跳出) 返回功能表，並重試一次。
按下 **Enter** 鍵後，「變更系統選項」顯示器再次出現。	查看顯示器底端的錯誤訊息。您可能鍵入了不被允許的值。如果需要進一步資訊，請記得使用 **F1** (說明)。若要系統將所有的值復置成您開始鍵入前的原貌，請使用 **F5** (重整)。然後重試一次。
在未鍵入所有顯示器上的選項前便按下 **Enter** 鍵。	您可以視需要多次使用此顯示器來變更系統值。請從 SETUP 功能表選取選項 **1**，然後輸入您上次遺漏的值。**注意：一旦系統開始運作，請務必先洽詢程式設計師後再變更安全層次。另外，如果您正在使用 iSeries Access 或正與另一部電腦通信，請勿變更系統名稱。**
按到 **Enter** 鍵，而非向下換頁。	再次從 SETUP 功能表選取選項 **1**，然後切換至第二頁。鍵入您的選項，然後按 **Enter** 鍵。

輸入了系統值後，您必須接著套用新的系統值。

套用新的系統值

當您輸入系統值後，便須套用部份的系統值。對系統值所作的變更多數會立即生效。不過，當您變更系統的安全層次時，變更內容須等到您關閉系統並再次啓動後才會生效。當您確認已在「變更系統選項」顯示器上正確鍵入所有的值後，即可開始套用新的值。

註: 如果您尚未將工作站附加至系統，請先執行此動作。當您啓動系統時，它會用您在「變更系統選項」顯示器上所選擇的命名格式，自動配置這些裝置。

請使用下列程序來關閉系統並重新加以啓動。當您再度啓動系統時，您在「變更系統選項」顯示器所輸入的值即會生效。

1. 請確定您已登入主控台，而且沒有登入其他工作站。
2. 請確定處理器裝置上的按鍵鎖定開關位於「正常」位置。
3. 在 SETUP 功能表中，選取「電源開啓及關閉作業」的選項。
4. 選取立即關閉系統電源，然後開啓電源的選項。按下 **Enter** 鍵。
5. 系統將會帶出顯示器，要求您確認是否要執行電源關閉程序。按下 **F16** (確認)。

如此即會自動關閉系統，然後再次加以啓動。您的顯示器將空白數分鐘。然後「登入」顯示器便會再次出現。

套用新的系統值後，您必須在系統上爲您自己建立安全主管設定檔。

建立安全主管設定檔

系統上的**安全主管**是指具備 *SECOFR 使用者類別或 *ALLOBJ 與 *SECADM 特殊權限的任何使用者。

從「變更系統選項」顯示器套用系統值後，請爲您自己和代理安全主管建立使用者設定檔。日後，當您執行安全主管功能時，請使用您的設定檔而非 QSECOFR 設定檔。

1. 以 QSECOFR 身份登入系統並要求 SETUP 功能表。

   請注意您所選擇的系統名稱是否出現在「登入」顯示器的右上角。

```
                    登入
                                   系統  . . . . . .
                                   子系統  . . . . .
                                   顯示  . . . . . .

使用者  . . . . . . . . . . . . .  QSECOFR
密碼  . . . . . . . . . . . . . .  _________
程式/程序 . . . . . . . . . . . .  _________
功能表  . . . . . . . . . . . . .  SETUP
現行檔案庫  . . . . . . . . . . .  _________
```

2. 在 SETUP 功能表中，選取*查看使用者列名*選項。「查看使用者列名」顯示器將會列出目前在您系統上的設定檔。

   註: 如果出現「查看使用者設定檔」顯示器，請按 **F21** (選取輔助層次)，並變更爲基本輔助層次。

3. 若要建立新的設定檔，請在*選項*直欄中鍵入 **1** (新增)，並在*使用者*直欄中鍵入您的設定檔名稱。按下 **Enter** 鍵。

```
                          查看使用者列名

請鍵入下列選項，然後按 Enter 鍵。
  1=新增    2=變更    3=複製    4=移除    5=顯示

選項 使用者      說明
1       JONESS
QDOC                              文件使用者設定檔
QSECOFR                           安全主管使用者設定檔
```

4. 在「新增使用者」顯示器上，爲自己指派一個密碼。
5. 以您自己的適當資訊，填寫範例顯示器上的欄位。
6. 切換至下一頁。

```
                              新增使用者

請鍵入下列選項，然後按 Enter 鍵。

使用者  . . . . . .   JONESS
使用者說明  . . . . . .   Jones, Sharon
密碼  . . . . . .   密鑰
使用者類型  . . . . . .   *SECOFR
使用者群組  . . . . . .   *NONE

限制指令行使用              _____
預設檔案庫  . . . . . .
預設印表機  . . . . . .   *WRKSTN
登入程式  . . . . . .   *NONE
檔案庫  . . . . . .

第一個功能表  . . . . . .
檔案庫  . . . . . .
```

7. 填寫顯示器第二頁，然後按 **Enter** 鍵。
8. 檢查位於「查看使用者列名」顯示器底端的確認訊息。
9. 按 **F3** (跳出) 回到 SETUP 功能表。

```
                              新增使用者

請鍵入下列選項，然後按 Enter 鍵。

岔斷鍵程式  . . . . . .   *SYSVAL
  檔案庫  . . . . . .
```

可能的錯誤	回復方式
未鍵入所有欄位的資訊前便按下 **Enter** 鍵。	使用「查看使用者列名」顯示器的變更選項，來變更您剛剛建立的設定檔。如果此設定檔未出現在清單中，請按下 **F5** (重整)，然後換下頁尋找。

當您爲自己建立好安全主管設定檔後，即必須變更「服務工具」使用者 ID 和密碼。請參閱「資訊中心」下的服務工具主題。

設定安全系統值

在本主題中，我們要使用「查看系統值 (WRKSYSVAL)」指令來變更及顯示系統值。

需要哪些套表？

輸入您在《規劃您的整體安全策略》中所準備的「系統值選項」套表資訊。

若要設定您的系統值，請完成下列作業：

1. 變更安全系統值。
2. 變更個別的系統值。

登入指令行介面

使用下列資訊來登入系統：

設定檔 您自己的 (需要 *SECADM 與 *ALLOBJ 權限)

功能表 MAIN

當您登入後，即可開始變更安全系統值。

變更安全系統值

登入系統後，使用此程序來輸入出現在「系統值選項」套表第 2 部份的安全系統值。

1. 在此指令行上，鍵入 WRKSYSVAL *SEC，然後按 **Enter** 鍵。指令名稱之後的 *SEC 是表示您只想看到與安全有關的系統值。
2. 在「查看系統值」顯示器上，於想要變更之系統值其前方的*選項*直欄中鍵入 **2** (變更)。如果要變更的系統值不在顯示器上，請換下頁加以尋找。

```
                          查看系統值

定位於 . . . . . .                    開始字元
依類型區分子集 . . . . .   *SEC         F4 以列示

請鍵入選項，然後按 Enter 鍵。
  2=變更   5=顯示

        系統
選項    值            類型        說明
        QINACTMSGQ    *SEC        非作用中工作訊息佇列
2       QLMTDEVSSN    *SEC        限制裝置階段作業
        QLMTSECOFR    *SEC        限制安全主管裝置
        QMAXSGNACN    *SEC        失敗時擬採取的動作
  ⋮
```

3. 鍵入您的系統值選項，然後按 **Enter** 鍵。螢幕即會再次出現「查看系統值」顯示器。

```
                          變更系統值
系統值 . . . . . :    QLMTDEVSSN
說明 . . . . . :     限制裝置階段作業

請鍵入選項，然後按 Enter 鍵。

  限制裝置階段作業 . . . . . .   0          0=不限制
                                           1=限制
```

4. 檢查位於顯示器底端的確認訊息。

可能的錯誤	回復方式
出現不同於範例「查看系統值」顯示器中的系統值。	您忘了鍵入 *SEC。比較顯示器頂端的以及範例顯示器的*依類型區分子集*欄位。將游標移至*依類型區分子集*欄位。鍵入 *SEC，然後按 **Enter** 鍵。
系統並未處理您的指令。您仍然看到功能表。	檢查顯示器底端的錯誤訊息。您可能鍵入了錯誤的指令名稱。請重試一次。如果訊息指出您未獲授權，請先登出後，再以具備安全主管權限的設定檔重新登入。
您按下 **Enter** 鍵後，「變更系統值」顯示器再次出現。	檢查顯示器底端的錯誤訊息。您可能鍵入了錯誤的選項，或撿選超過許可範圍的值。請用 **F1** (說明) 來查看其餘資訊。
出現的是功能表，而非「查看系統值」顯示器。	您可能按了兩次 **Enter** 鍵。請鍵入 WRKSYSVAL *SEC。
選到不想變更的系統值。	按下 **F12** (取消) 即可返回「查看系統值」顯示器。

*** (星號) 代表什麼意義**？

您可能已經注意到某些值的前面帶有一個星號 (*)。系統就是以星號來區別特殊值與一般文字。例如，當您指定使用者設定檔的密碼是 *NONE 時，即表示系統將不許任何人以此設定檔來登入。如果將密碼指定爲 NONE，使用者即必須鍵入字元 NONE 作爲密碼。

當您設定系統安全時，請務必注意星號在指示與套表中的使用方式。

變更好安全系統值後，您即可變更個別的系統值。

變更個別的系統值

當您變更安全系統值後，即可變更個別的系統值。

例如，「斷線工作逾時間隔 (QDSCJOBITV)」系統值即未併入爲安全系統值。它不會出現在「查看系統值」顯示器的 *SEC 子集中。請用此程序來變更 QDSCJOBITV 系統值或任何個別系統值：

1. 鍵入 WRKSYSVAL QDSCJOBITV，並按下 **Enter** 鍵。
2. 在「查看系統值」顯示器上，於 QDSCJOBITV 前方的*選項*直欄中鍵入 **2** (變更)。
3. 鍵入您對 QDSCJOBITV 的選項。
4. 檢查確認訊息。

```
                              變更系統值
系統值 . . . . . :   QDSCJOBITV
說明 . . . . . :   斷線工作逾時間隔

請鍵入選項，然後按 Enter 鍵。

  斷線工作逾時間隔 ..................... 300
```

列出您的安全值

輸入「系統值選項」套表的所有資訊後，您即可列印所有安全系統值的清單。請鍵入 WRKSYSVAL *SEC OUTPUT(*PRINT)。以您的「系統值選項」套表將此清單存檔。每當您變更安全系統值時，重新列印此清單。

當您針對「系統值選項」套表的系統值輸入了所有選項後，即可準備載入您的應用程式。

執行載入應用程式時的安全步驟

在您設定系統值後，即可準備載入您的應用程式。本主題會列出所需的安全步驟，供您在載入應用程式檔案庫至系統時使用。待您建立了設定檔與其他安全物件後，《設定所有權及公用權限》和《設定資源安全》將會告訴您如何爲應用程式建立所有權與權限。

儘可能在設定使用者群組與個別設定檔之前，將應用程式載入至您的系統上。因爲在您建立工作說明與設定檔時，必須參考應用程式物件。

如果無法在建立群組與個別設定檔之前載入應用程式，您可能會收到如下所示的警告訊息：

- 當您建立工作說明時，系統找不到起始檔案庫。
- 當您建立設定檔時，系統找不到起始程式或功能表。

除非載入您的應用程式檔案庫，否則您無法順利測試工作說明與設定檔。

請使用您在《規劃您的應用程式安裝》中所準備的「應用程式安裝」套表。

若要載入您的各種應用程式，請完成下列作業：

1. 建立擁有者設定檔。
2. 載入應用程式。

登入系統

- 若要建立擁有者設定檔：

  設定檔 您自己的 (需要 *SECADM 權限)

  功能表 MAIN

- 若要載入應用程式檔案庫：

  洽詢您的應用程式供應商，查明在您載入應用程式檔案庫時，是否須以安全主管或應用程式擁有者身份登入。

當您登入後，即可爲您的應用程式建立擁有者設定檔。

建立擁有者設定檔

登入系統後，請檢查您的應用程式安裝規劃，以瞭解在載入應用程式前是否還需建立任何設定檔。若要建立設定檔：

1. 鍵入 CRTUSRPRF (建立使用者設定檔)，並按下 **F4** (提示)。
2. 在「建立使用者設定檔」顯示器上，依照程式設計師或應用程式供應商的指示，填寫相關欄位。
3. 使用 **F10** (尚有欄位) 與 Page Down 鍵來顯示其餘欄位。

```
                        建立使用者設定檔 (CRTUSRPRF)

請鍵入選項，然後按 Enter 鍵。

使用者設定檔 . . . . . . . . . . >
使用者密碼 . . . . . . . . . .   *USRPRF
將密碼設定成過期 . . . . . . . .   *NO
狀態 . . . . . . . . . . . . .   *ENABLED
使用者類別 . . . . . . . . . .   *USER
輔助層次 . . . . . . . . . . .   *SYSVAL
現行檔案庫 . . . . . . . . . .   *CRTDFT
擬呼叫的起始程式 . . . . . . .   *NONE
  檔案庫 . . . . . . . . . . .
起始功能表 . . . . . . . . . .   MAIN
  檔案庫 . . . . . . . . . . .     *LIBL
限制功能 . . . . . . . . . . .   *NO
文字說明 . . . . . . . . . . .   xxxxxx 的擁有者
```

4. 檢查顯示器底端的訊息。

註: 建立群組設定檔會進一步詳述如何建立設定檔。

爲應用程式建立擁有者後，即可開始載入您的應用程式。

載入應用程式

請遵照應用程式供應商的指示，來載入您的應用程式檔案庫。在《設定所有權及公用權限》中，您將學到如何設定應用程式的所有權與公用權限。

待您載入所有的應用程式後，便可設定使用者群組。

設定使用者群組

當您執行載入應用程式的安全步驟後，便可設定使用者群組。您需要建立群組檔案庫、工作說明和群組設定檔。請先針對您的使用者群組之一來完成整個主題，然後再就任何其他群組重複相關步驟。範例顯示器所示爲 JKL Toy Company 之「業務及行銷部門」與「倉儲部門」的「使用者群組說明」套表資訊。

請使用您在「規劃使用者群組」階段所準備的「使用者群組說明」套表。

完成以下作業來設定使用者群組：

1. 建立使用者群組的檔案庫。
2. 建立工作說明。
3. 建立群組設定檔。

登入系統

設定檔 您自己的 (需要具有 *SECADM 權限)

功能表 MAIN

當您登入後，即可建立使用者群組的檔案庫。

建立群組的檔案庫

當您登入系統後，您必須爲使用者群組建立檔案庫。如果希望使該群組共用檔案庫來存放所建立的物件，例如「查詢」程式，請在建立群組設定檔之前先建立檔案庫：

1. 鍵入 CRTLIB (建立檔案庫)，再按 **F4** (提示)。
2. 填寫顯示器畫面。檔案庫名稱須爲群組設定檔名稱。
3. 按 **F10** (其它參數)。
4. 填入檔案庫以及在檔案庫中所建立的新物件的公用權限。
5. 按 **Enter** 鍵。檢查確認訊息。

```
                              建立檔案庫

請鍵入選項，然後按 Enter 鍵。

檔案庫 . . . . . . . . . . . . . .   DPTWH
檔案庫類型 . . . . . . . . . . . .   *PROD
文字說明 . . . . . . . . . . . . .   倉儲檔案庫

                            其它參數

權限 . . . . . . . . . . . . . . .   *USE
輔助儲存體儲存區 ID  . . . . . . . 1
建立權限 . . . . . . . . . . . . .   *CHANGE
建立物件審核 . . . . . . . . . . .   *SYSVAL
```

可能的錯誤	回復方式
在鍵入檔案庫說明之前，便已按下 **Enter** 鍵。	鍵入 **CHGLIB** 再按下 **F4** (提示)。在提示畫面上鍵入檔案庫名稱，然後按 **Enter** 鍵。於「變更檔案庫」顯示器上鍵入說明。
提供錯誤的檔案庫名稱。	使用「更名物件 (RNMOBJ)」指令。

建立好群組檔案庫後，您便可建立工作說明。

建立工作說明

當您建立群組的檔案庫後，就可開始爲每一個群組建立工作說明。

如果起始檔案庫清單所需的檔案庫尚不存在於系統上，您在建立工作說明時將會收到警告訊息。

1. 鍵入 **CRTJOBD** (建立工作說明)，並按下 **F4** (提示)。
2. 填寫以下欄位：

   工作說明：
   和群組設定檔名稱相同。

   程式庫名稱：
   QGPL

   本文： 群組說明
3. 按下 **F10** (其它參數)。
4. 切換至下頁的*起始檔案庫清單*欄位。

```
                    建立工作說明

請鍵入選項，然後按 Enter 鍵。

工作說明  . . . . . . . . . . . .  DPTSM
  檔案庫  . . . . . . . . . . . .  QGPL
工作佇列  . . . . . . . . . . . .  QBATCH
  檔案庫  . . . . . . . . . . . .    *LIBL
工作優先順序 (於 JOBQ)  . . . . .  5
輸出優先順序 (於 OUTQ)  . . . . .  5
列印裝置 . . . . . . . . . . . .  *USRPRF
輸出佇列 . . . . . . . . . . . .  *USRPRF
  檔案庫  . . . . . . . . . . . .
文字說明 . . . . . . . . . . . .   業務及行銷
```

5. 在*起始檔案庫清單*欄位中，於 *SYSVAL 上鍵入 **+** (加號)，指明您想要輸入一串的值。按 **Enter** 鍵。

```
帳戶碼  . . . . . . . . . . . .   *USRPRF
   :
CL 語法檢查 . . . . . . . . . .   *NOCHK
起始檔案庫清單  . . . . . . . .   +
             + 尚有其餘值
```

6. 在*起始檔案庫清單*欄位中，鍵入從「使用者群組說明」套表所標示 (✓) 之檔案庫的名稱：
   - 每一行輸入一個檔案庫名稱。
   - 包括 QGPL 與 QTEMP。每個工作都是使用名叫 QTEMP 的檔案庫來儲存暫時物件。**所有的起始檔案庫清單都須具有 QTEMP 檔案庫**。對大部份的應用程式而言，QGPL 檔案庫也應該列入起始檔案庫清單中。
   - 您不需將現行 (預設) 檔案庫納入到檔案庫清單中。系統會在登入時自動新增該檔案庫。
7. 按 **Enter** 鍵。檢查訊息。(換下頁以查看所有訊息)。

```
指定更多值

請鍵入選項，然後按 Enter 鍵。

起始檔案庫清單 . . . . . . . . .   CUSTLIB
                                    ITEMLIB
                                    COPGMLIB
                                    ICPGMLIB
                                    QGPL
                                    QTEMP
```

可能的錯誤	回復方式
您按的是 **Enter** 鍵，而非 **F10**。	要將正確的檔案庫放入起始檔案庫清單，請鍵入 **CHGJOBD** (變更工作說明) 並按 **F4**。

可能的錯誤	回復方式
嘗試建立工作說明時，收到錯誤訊息。	最常見的錯誤訊息，多半是因爲您嘗試併入不存在系統上的檔案庫所致。這都屬於警告訊息。此時工作說明依然會被建立，檔案庫也會併入起始檔案庫清單。不過，除非該檔案庫已存在於系統上，否則您將無法透過指定此工作說明的設定檔來登入。 如果您的檔案庫已在系統上，可能是您鍵入了錯誤的名稱。請驗證檔案庫名稱，再重試一次。

建立了工作說明後，您就可建立群組設定檔。

建立群組設定檔

當您建立工作說明後，便可建立群組設定檔。要進行此作業，請使用「使用者群組說明」套表的第 2 部份資訊。

1. 使用「查看使用者設定檔」指令。鍵入 WRKUSRPRF *ALL。開始時，顯示器會列出 IBM 所提供的設定檔。

   註: 如果出現「查看使用者列名」顯示器，請按 **F21** 來變更爲中階輔助層次。

2. 若要建立新的設定檔，請在*選項*直欄中鍵入 **1**，並在*使用者設定檔*直欄中鍵入設定檔名稱。按 **Enter** 鍵。

```
                          查看使用者設定檔

請鍵入選項，然後按 Enter 鍵。
  1=建立    2=變更    3=複製    4=刪除    5=顯示
  12=依擁有者使用物件

     使用者
選項  設定檔       本文
1    DPTSM
     QDOC         文件使用者設定檔
     QSECOFR      安全主管使用者設定檔
```

3. 將「使用者群組說明」套表的資訊分別鍵入到適當的欄位中。
4. 若想在任何欄位使用其預設值，可用 **Tab** 鍵加以跳過。
5. 按下 **F10** (其它參數)。
6. 換下頁。

```
                        建立使用者設定檔 (CRTUSRPRF)

請鍵入選項，然後按 Enter 鍵。

使用者設定檔 . . . . . > DPTSM
使用者密碼 . . . . . .   *none
將密碼設定成過期 . . . . .   *NO
狀態 . . . . . .   *ENABLED
使用者類別 . . . . . .   *USER
輔助層次 . . . . . .   *SYSVAL
現行檔案庫 . . . . . .   *CRTDFT
擬呼叫的起始程式 . . . . . .   cpsetup
  檔案庫 . . . . . .   cppgmlib
起始功能表 . . . . . .   cpmain
  檔案庫 . . . . . .   cppgmlib
限制功能 . . . . . .   *yes
文字說明 . . . . . .   業務及行銷
```

7. 將「使用者群組說明」套表上的其餘資訊輸入顯示器的其餘頁面，然後按 **Enter** 鍵。

```
                        建立使用者設定檔

                          其它參數

特殊權限 . . . . . .   *USRCLS

   ⋮
工作說明 . . . . . .   DPTSM
  檔案庫 . . . . . .   QGPL
```

```
                        建立使用者設定檔

群組權限 . . . . . .   *NONE

   ⋮
列印裝置 . . . . . .   PRT03
```

8. 檢查訊息。

請記得

群組設定檔只是一種特殊的使用者設定檔。許多訊息與顯示器會將群組設定檔視爲使用者或使用者設定檔。如果您在其中新增了成員或爲其指定群組識別碼 (gid)，系統才會曉得您建立了群組設定檔。

可能的錯誤	回復方式
在鍵入群組設定檔的所有相關值之前，便已按下 **Enter** 鍵。 以錯誤的名稱建立設定檔。	按下 **F5** (重整)，將所建立的設定檔新增至「查看使用者設定檔」顯示器。使用選項 **2** (變更)，來更正設定檔。 您無法變更設定檔的名稱。因此，請使用複製選項 (**3**) 來建立具有正確名稱的新設定檔。然後再刪除 (選項 **4**) 名稱錯誤的設定檔。

可能的錯誤	回復方式
「使用者群組說明」套表的某些欄位並未出現在顯示器上。	請確定您是使用中階輔助層次。「建立使用者設定檔」的基本輔助層次版稱爲「新增使用者」顯示器。若要變更輔助層次，請按 **F12** (取消)，回到「查看使用者列名」顯示器。使用 **F21** 來變更輔助層次。請參閱《選取正確的輔助層次》。
不小心消除了「建立使用者設定檔」顯示器上的部份預設資訊。	如果將欄位留白，系統建立使用者設定檔時會使用預設值。若要查看預設值，可按 **F5** (重整) 來復置整個顯示器。然後再重新鍵入您的資訊。

列出結果

您可以用「顯示授權使用者 (DSPAUTUSR)」指令，來列出系統上所有設定檔的名稱與說明。請鍵入 `DSPAUTUSR OUTPUT(*PRINT)`。檢查以確定所有的群組設定檔密碼皆爲 *NONE。

在您設定個別使用者之前，請先完成下列作業：

- 爲每一個使用者群組建立工作說明。
- 選用性地，爲每一個群組建立檔案庫。
- 爲每一個使用者群組建立群組設定檔。

設定個別使用者

當您設定使用者群組時，即已完成建立群組設定檔的步驟。現在，請您爲群組成員建立個別的設定檔。

請先以某個使用者群組的成員完成整個主題，然後再回頭對其他群組重複這些步驟。範例畫面中顯示的個別使用者設定檔套表中的使用者，是 Sharon Jones 爲 JKL Toy Company 的「業務及行銷部門」及「倉儲部門」所準備的。您可以在規劃個別使用者設定檔中找到這些套表的複本。

請使用您在規劃個別使用者設定檔中準備的「個別使用者設定檔」套表。

若要建立群組成員的個別設定檔，請完成這些作業：

1. 建立個人檔案庫。(可選用)
2. 複製群組設定檔。
3. 將密碼設爲到期。
4. 建立其他使用者。(可選用)

   註: 重複建立個人檔案庫及建立其他使用者，直到各群組成員都有使用者設定檔。
5. 必要時，可以變更使用者資訊。
6. 顯示您的結果。

登入系統

設定檔 您自己的 (需要 *SECADM 權限)

功能表 SETUP

建立個人檔案庫

設定個別使用者之前，您可能需要爲物件的每一個成員建立個人檔案庫，如：「查詢」程式。建立個別使用者設定檔之前，請先建立個人檔案庫。

1. 鍵入 **CRTLIB**，然後按一下 **F4** (提示)。
2. 提供與使用者設定檔同名的檔案庫名稱。
3. 按 **F10** (其它參數)。
4. 填寫檔案庫及它的新建物件的公用權限。
5. 按 **Enter** 鍵。檢查確認訊息。

```
                          建立檔案庫

請鍵入選項，然後按 Enter 鍵。

檔案庫 . . . . . .  DPTSM
檔案庫類型 . . . . . .  *PROD
文字「說明」 . . . . . .  倉儲檔案庫

                        其它參數

權限 . . . . . .  *EXCLUDE
輔助儲存體儲存區 ID . . . . . .  1
建立權限 . . . . . .  *CHANGE
建立物件審核 . . . . . .  *SYSVAL
```

建立個人檔案庫之後，您可以用複製群組設定檔的方式來建立個別設定檔。

複製群組設定檔

群組設定檔有兩個角色：

1. 系統用它來決定是否授權群組成員使用物件。
2. 您可以用它作爲型樣來建立個別群組成員的使用者設定檔。

當您設定使用者群組的同時，其實也建立了群組設定檔。現在，您可以複製群組設定檔來建立個別設定檔，複製個別設定檔來建立群組中的其他設定檔。

1. 選取 SETUP 功能表中的「查看使用者列名」選項。

   註: 如果您看到「查看使用者設定檔」顯示畫面，使用 **F21** (選取輔助層次) 即可變更爲基本輔助層次。

2. 在使用者群組之前的*選項*直欄中，鍵入 **3** (複製)。螢幕會顯示「複製使用者」顯示畫面 (如果顯示畫面中沒有您想要複製的使用者群組，請向下翻頁尋找)。系統會讓您複製的群組設定檔中的使用者名稱欄位空白，但會填寫其餘欄位。

```
                        查看使用者列名

請鍵入下列選項，然後按 Enter 鍵。
  1=新增    2=變更    3=複製    4=移除    5=顯示

選項     使用者          說明

         DPTSM           業務及行銷部門
3        DPTWH           倉儲部門
```

3. 鍵入您正在建立的使用者設定檔的名稱和說明。

4. 讓密碼保持空白。系統會自動建立與新使用者設定檔名稱相同的密碼。
5. 在*使用者群組*欄位中填入群組設定檔名稱。
6. 檢查「個別使用者設定檔」套表，查看使用者的其他值是否不同於群組值。請輸入這些值。
7. 向下翻頁。

```
                                複製使用者

複製來源使用者  . . . . :   DPTWH

請鍵入下列選項，然後按 Enter 鍵。

使用者. . . . . . . . . .   WILLISR
使用者說明. . . . . . . .   Willis, Rose
密碼. . . . . . . . . . .
使用者類型. . . . . . . .   *SYSOPR
使用者群組. . . . . . . .   DPTWH

限制指令行使用              N

預設檔案庫  . . . . . . .   DPTWH
預設印表機  . . . . . . .   PRT04
登入程式  . . . . . . . .   *NONE
  檔案庫  . . . . . . . .

第一個功能表  . . . . . .   ICMAIN
  檔案庫  . . . . . . . .     ICPGMLIB
```

8. 在下一頁的顯示畫面中進行必要的變更，然後按 **Enter** 鍵。
9. 檢查「查看使用者列名」顯示器底端的確認訊息。

```
                                複製使用者

複製來源使用者  . . . . :   DPTWH

請鍵入下列選項，然後按 Enter 鍵。

忽斷鍵程式. . . . . . . .   *SYSVAL
  檔案庫  . . . . . . . .
```

可能的錯誤	回復方式
您看到的是「建立使用者設定檔」顯示畫面，而非「複製使用者」顯示畫面。	使用 **F12** (取消)，返回「查看使用者設定檔」顯示畫面。使用 **F21**，變更爲基本輔助層次。重新複製。
您選取的使用者設定檔名稱無法放入使用者提示中。	雖然使用者設定檔名稱的上限爲 10 個字元，但「複製使用者」及「新增使用者」顯示畫面最多只支援 8 個字元的名稱。請選擇較短的使用者名稱，或使用中階輔助層次來建立個別使用者設定檔。

測試使用者設定檔

當您在群組中建立了第一個個別設定檔時，應該用它來登入測試。請驗證您看到的第一個功能表是否正確，以及登入程式是否在執行。

如果使用這個設定檔無法順利登入，可能是系統找不到設定檔中的指定項目。這個項目可能是登入程式、工作說明或是起始檔案庫清單中的某個檔案庫。請使用「使用印表機輸出」顯示畫面，尋找您嘗試登入時撰寫的工作日誌。工作日誌會告訴您發生哪些錯誤。

有關變更安全時的測試及診斷問題的詳細資訊，請參閱測試安全。

測試使用者設定檔之後，您可以將密碼設爲到期。

將密碼設為到期

設定個別設定檔，要求使用者初次登入後立即變更密碼。基本輔助層次版的「複製使用者」顯示畫面中沒有*將密碼設爲到期*欄位。當您使用複製功能建立使用者設定檔之後，您必須個別變更。若要變更*將密碼設爲到期*欄位，請鍵入 CHGUSRPRF *設定檔名稱* PWDEXP(*YES)。

註: 如果您想以使用者設定檔測試登入，請在將密碼設爲到期*之前*，先進行測試。

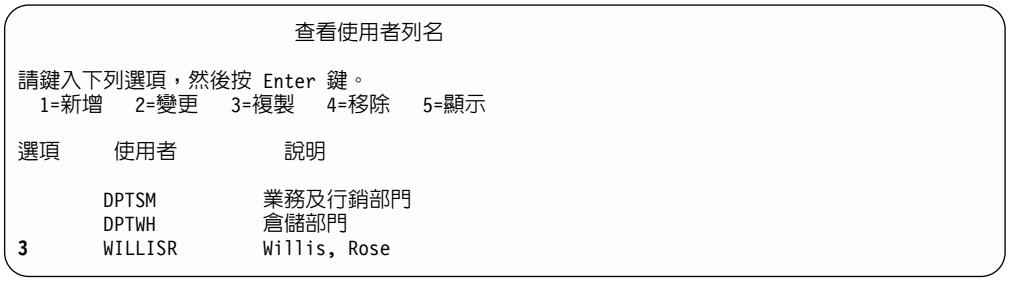
可能的錯誤	回復方式
您已經測試設定檔，並且被強制變更密碼。	請鍵入 **CHGUSRPRF** *設定檔名稱*，然後按 **F4** (提示)。請將密碼設回到使用者設定檔名稱 (在密碼欄位中鍵入使用者設定檔名稱)。在*將密碼設爲到期*欄位中，鍵入 ***YES**。您需要在中階輔助層次中執行這個動作。

建立第一個個別使用者設定檔之後，您可以建立其他使用者。

建立其他使用者

當您以複製群組設定檔的方式建立第一個個別設定檔之後，即可建立其他使用者。請複製第一個個別使用者設定檔，用它來建立群組的其他成員。當您以複製方法建立個別設定檔時，請仔細查看每一個個別設定檔。請檢查「個別使用者設定檔」套表，確定新使用者設定檔的唯一欄位都有變更。

1. 在「查看使用者列名」顯示畫面中您想複製的使用者設定檔前面，鍵入 **3** (複製)。
2. 在「複製使用者」顯示畫面中，鍵入設定檔名稱及說明。
3. 在新使用者的唯一欄位中輸入資訊。



可能的錯誤	回復
「查看使用者列名」顯示畫面中沒有您要複製的設定檔。	按 **F5** (重新整理)。向上及向下翻頁。清單按設定檔名稱的字母順序排列。

如果您想改變使用者的相關資訊，請參閱變更使用者的相關資訊。

變更使用者的相關資訊

您可能需要爲某些使用者設定「複製使用者」顯示畫面中沒有的值。例如，某些使用者可能屬於多個群組設定檔。當您以複製方法建立使用者設定檔之後，即可進行變更。

1. 在「查看使用者列名」顯示畫面中按 **F21**，即可變更爲中階輔助層次。
2. 在「查看使用者設定檔」顯示畫面中您想變更的設定檔旁邊的*選項* 直欄中，鍵入 **2** (變更)。按 **Enter** 鍵。

```
                          查看使用者設定檔

請鍵入選項，然後按 Enter 鍵。
  1=建立    2=變更    3=複製    4=刪除    5=顯示
  12=依擁有者使用物件

     使用者
選項 設定檔       文字
2    AMESJ        Ames, Janice
     DPTSM        業務及行銷部門
     QDOC         文件使用者設定檔
     QSECOFR      安全主管使用者設定檔
     WAGNERR      Wagner, Ray
     WILLISR      Willis, Rose
```

3. 在「變更使用者設定檔」顯示畫面中，按 **F10** (其它參數)。
4. 向下翻頁尋找您要變更的欄位。例如，如果您要讓某個使用者成爲其他群組設定檔的成員，請向下翻頁尋找*增補群組*欄位。
5. 鍵入所需值，然後按 **Enter** 鍵。您會收到確認訊息，並再次看到「查看使用者設定檔」顯示畫面。

```
                    變更使用者設定檔 (CHGUSRPRF)

請鍵入選項，然後按 Enter 鍵。

容許儲存體的上限  . . . . . .    *NOMAX
排程最高優先順序. . . . . .    3
工作說明  . . . . . . . . . .    DPTWH
  檔案庫  . . . . . . . . . .      QGPL
群組設定檔  . . . . . . . . .    DPTWH
擁有者  . . . . . . . . . . .    *GRPPRF
群組權限  . . . . . . . . . .    *USEE
群組權限類型  . . . . . . . .    *PGP
增補群組  . . . . . . . . . .    DPTIC
              + 尚有其餘值
```

變更使用者資訊後，您可以顯示您的結果來檢查設定檔。

顯示使用者設定檔

顯示您建立的設定檔，有許多種方法。

顯示一個設定檔

在「查看使用者列名」顯示畫面或「查看使用者設定檔」顯示畫面中，使用選項 **5** (顯示)。

列出一個設定檔

使用「顯示使用者設定檔」指令：DSPUSRPRF *設定檔名稱* DETAIL(*BASIC) OUTPUT(*PRINT)。

顯示群組成員

鍵入 DSPUSRPRF *群組設定檔名稱* *GRPMBR。您可以使用 OUTPUT(*PRINT) 來列印清單。

列出所有設定檔

若要按群組排序列出所有設定檔的名稱及說明，請使用「顯示授權使用者」指令：DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT)。

設定所有權及公用權限之前，請先確定完成這些作業：

- 完成建立所有個別使用者設定檔。
- 將每一個設定檔的密碼設爲到期。
- 按群組排序列印所有設定檔清單，並和「使用者群組說明」套表一起保存。新增使用者時，還要再列印此清單。

第 7 章 設定資源安全

您將在這個主題中建立物件的所有權及公用權限，以及應用程式的特定權限。您還會設定工作站及印表機的資源安全。請先用一個檔案庫完成整個主題，然後再回頭用應用程式的其他檔案庫重複這些步驟。當您完成這個應用程式的資源安全設定之後，再對其他應用程式重複這些步驟。

每次系統安裝新應用程式或設定現有應用程式的資源安全時，即可使用這些程序。

這個主題範例中顯示的是 JKL Toy Company 的「授權清單套表」、「檔案庫說明套表」及「輸出佇列及工作站安全套表」。您可以在設定所有權及公用權限中找到這些套表範例。

需要哪些套表？

- 您在規劃您的應用程式安裝中準備的「應用程式安裝套表」。
- 您在物件分組中準備的「授權清單套表」。
- 您在決定檔案庫及物件的所有權中準備的「檔案庫說明套表」。
- 您在保護印表機輸出及保護工作站中準備的「輸出佇列及工作站安全套表」。
- 您在規劃您的整體安全策略中準備的「系統責任套表」。

您可以用幾種方法來設定資源安全。這個主題的步驟順序與「應用程式安裝套表」、「授權清單套表」及「檔案庫說明套表」中的資訊排序相同：

1. 設定所有權及公用權限。
2. 建立授權清單。
3. 使用授權清單保護物件安全。
4. 將使用者新增至授權清單。
5. 設定任何特定權限。
6. 保護印表機輸出安全。
7. 保護工作站安全。
8. 限制存取系統操作員訊息佇列。

設定所有權及公用權限

您將在這個主題中建立應用程式檔案庫、群組檔案庫及個人檔案庫的所有權及公用權限。請先用一個應用程式完成整個主題，然後再回頭用其他應用程式重複這些步驟。這個範例顯示 Sharon Jones 在規劃您的應用程式安裝中爲「客戶訂單」應用程式準備的「應用程式安裝套表」 。

每次系統安裝新應用程式或設定現有應用程式安全時，即可使用這個主題中的程序。

請使用您在規劃您的應用程式安裝中準備的「應用程式安裝套表」。

若要設定所有權及公用權限，請完成這些作業：

1. 建立擁有者設定檔。

2. 變更檔案庫所有權。
3. 設定應用程式物件的所有權。
4. 設定檔案庫的公用存取權限。
5. 設定檔案庫中所有物件的公用權限。
6. 設定新物件的公用權限。
7. 使用群組及個人檔案庫。

登入系統

設定檔 您自己的 (需要 *ALLOBJ 權限)

功能表 MAIN

建立擁有者設定檔

如果還沒有擁有者設定檔，請執行下列作業：

- 使用 CRTUSRPRF (建立使用者設定檔) 指令建立它。密碼設定爲 *NONE。

如果已有擁有者設定檔，請執行下列作業：

- 使用 CHGUSRPRF (變更使用者設定檔) 指令，將密碼設定爲 *NONE。

建立擁有者設定檔之後，您可以變更檔案庫所有權。

變更檔案庫所有權

這個步驟是變更檔案庫的所有權，而非檔案庫中物件的所有權。

注意：變更任何應用程式物件的所有權之前，請先聯繫應用程式供應商。有些應用程式使用的功能，仰賴特定的物件所有權。

1. 鍵入 CHGOBJOWN (變更物件擁有者)，然後按 **F4** (提示)。
2. 填寫檔案庫名稱、物件類型 (*LIB) 及新的擁有者。
3. 檢查確認訊息。

```
                    變更物件擁有者 (CHGOBJOWN)

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . > COPGMLIB
  檔案庫 . . . . . >   *LIBL       名稱,
物件類型 . . . . . > *LIB
新的擁有者 . . . . .   COWNER
現行擁有者權限 . . . .   *REVOKE
```

可能的錯誤	回復方式
接收到錯誤訊息。	最常見的訊息是找不到檔案庫，或是找不到新的擁有者設定檔。請檢查鍵入值是否有錯，然後重試。

變更檔案庫所有權之後，您可以設定應用程式物件的所有權。

設定應用程式物件的所有權

變更應用程式物件所有權是一件非常麻煩的作業，因爲您必須個別變更每一個物件。如果可能，請程式設計師或應用程式供應商爲您建立所有權。

列出檔案庫中的物件

變更所有權之前，請先使用「顯示檔案庫」指令，列印檔案庫中所有物件的清單。您可以把它當作核對清單。請鍵入 DSPLIB *檔案庫名稱* *PRINT。

選擇最佳方法

請選擇下列一種方法，變更應用程式檔案庫中的物件所有權：

表 61. 變更物件所有權的方法

方法	作用	何時使用
依擁有者使用物件指令	顯示一個顯示畫面，裡面列出設定檔擁有的所有物件。您可以使用顯示畫面中的選項來變更物件擁有者。	這個方法比較容易使用。但若是 QPGMR 或 QSECOFR 擁有物件，則 IBM 不建議您使用這個方法。因爲這些設定檔擁有許多物件，清單顯示畫面可能會很大。
變更物件所有權指令	每一個物件需要使用個別的指令。但是您可以使用*擷取* (**F9**) 來重複上一個指令，減少鍵入次數。	如果 QPGMR 或 QSECOFR 擁有物件，這個方法比較快。

使用依擁有者使用物件 (WRKOBJOWN) 指令

如果 IBM 提供的設定檔 (如：QPGMR 或 QSECOFR) 不擁有物件，則可以使用這個方法來變更檔案庫中的物件所有權：

1. 請鍵入 WRKOBJOWN *擁有者設定檔名稱*。螢幕中列出使用者設定檔擁有的所有物件。
2. 請在您使用的檔案庫的每一個物件前面鍵入 **9** (變更擁有者)。
3. 在顯示畫面底端的*參數或指令*行中，鍵入 NEWOWN(*擁有者設定檔名稱*)，然後按 **Enter** 鍵。
4. 系統將您指出的每一個物件的擁有者，變更爲您在底端鍵入的新擁有者。您會在顯示畫面底端收到確認訊息。顯示畫面中不再出現這些物件，因爲設定檔已不再擁有這些物件。
5. 請重複步驟 2 及 4，變更檔案庫中所有物件的所有權。

```
                              依擁有者使用物件

使用者設定檔 . . . . . :   OLDOWNER

請鍵入選項，然後按 Enter 鍵。
  2=編輯權限          4=刪除    5=顯示權限
  8=顯示說明          9=變更擁有者

選項 物件           檔案庫         類型       屬性
     COPGMMSG       COPGMLIB       *MSGQ
9    CUSTMAS        CUSTLIB        *FILE
9    CUSTMSGQ       CUSTLIB        *MSGQ
     ITEMMSGQ       ITEMLIB        *MSGQ


   ⋮

參數或指令
===> NEWOWN(COWNER)
F3=跳出    F4=提示    F5=重整    F9=擷取
F18=底端
```

可能的錯誤	回復方式
您看到「變更物件擁有者」顯示畫面。	如果您指定選項 **9** (變更擁有者)，卻沒有在「依擁有者使用物件」顯示畫面的底端鍵入任何參數，就會看到這個顯示畫面。如果您鍵入的參數不正確，也會看到這個顯示畫面。請按 **F12** (取消)，返回「依擁有者使用物件」顯示畫面。請重試。請確定您鍵入的是範例中所示的參數。

您可以使用變更物件擁有者指令，變更 QPGMR 或 QSECOFR 擁有的物件的所有權。

使用變更物件擁有者指令

如果 QPGMR 或 QSECOFR *確實*擁有物件，您可以使用這個方法來變更檔案庫中物件的擁有者。

1. 鍵入 CHGOBJOWN，然後按 **F4** (提示)。
2. 在顯示畫面中填入清單中第一個物件的資訊，然後按 **Enter** 鍵。

```
                        變更物件擁有者 (CHGOBJOWN)

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . . . . . . . . . . > CUSTMAS
  檔案庫   . . . . . . . . . . . >   CUSTLIB
物件類型 . . . . . . . . . . . . > *FILE
新的擁有者 . . . . . . . . . . .   COWNER
現行擁有者權限 . . . . . . . . .   *REVOKE
```

3. 您會收到一個確認訊息，指出已經變更物件所有權。請取消勾選清單中的這個項目。
4. 按 **F9** (擷取)，擷取您鍵入的指令。
5. 按 **F4** (提示)。請在「變更物件擁有者」顯示畫面中輸入檔案庫中下一個物件的資訊，然後按 **Enter** 鍵。
6. 對檔案庫中的每一個物件，重複執行步驟 4 及 5。

檢查您的工作

若要確定您已經變更檔案庫中所有物件的所有權，請使用「依擁有者使用物件」指令。請鍵入 WRKOBJOWN *新的擁有者設定檔*。比較這個顯示畫面與檔案庫中的物件清單。

變更檔案庫中物件的所有權之後，您可以設定檔案庫的公用存取權限。

設定檔案庫的公用存取權限

設定應用程式物件的所有權之後，您可以使用「編輯物件權限 (EDTOBJAUT)」指令來變更檔案庫的公用權限：

1. 請鍵入 EDTOBJAUT *檔案庫名稱* *LIB。
2. 將游標移到下面的 **PUBLIC* 行。
3. 請鍵入您希望檔案庫具有的公用權限，然後按 **Enter** 鍵。

```
                              編輯物件權限

物件 . . . . . :   CUSTLIB         擁有者 . . . . . :   COWNER
  檔案庫 . . . . . :   QSYS          主群組 . . . . . :   *NONE
物件類型 . . . . . :   *LIB

變更現行權限，然後按 Enter 鍵。

  由授權清單保護安全的物件. . . . . .   *NONE

                         物件
使用者       群組        權限
COWNER                   *ALL
*PUBLIC                  *CHANGE
```

4. 顯示畫面顯示新的權限。

現在您可以設定檔案庫中所有物件的公用權限。

設定檔案庫中所有物件的公用權限

您可以使用「取消物件權限 (RVKOBJAUT)」指令，移除檔案庫中物件的現行公用權限。您可以使用「授予物件權限 (GRTOBJAUT)」指令，設定檔案庫中所有物件的公用權限：

1. 請鍵入 RVKOBJAUT，然後按 **F4** (提示)。
2. 依顯示畫面所示填寫，更改應用程式檔案庫名稱，然後按 **Enter** 鍵。

```
                      取消物件權限 (RVKOBJAUT)

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . .   *all
  檔案庫 . . . . . .     custlib
物件類型 . . . . . .   *all
使用者 . . . . . .   *public
             + 尚有其餘值
權限 . . . . . .   *all
```

註: 如果檔案庫有大量物件，系統可能要花幾分鐘來處理您的要求。

3. 鍵入 GRTOBJAUT，然後按 **F4** (提示)。
4. 依顯示畫面所示填寫，更改應用程式檔案庫名稱以及您想要的權限，然後按 **Enter** 鍵。

```
                    授予物件權限 (GRTOBJAUT)

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . .  *all
  檔案庫 . . . . . .  custlib
物件類型 . . . . . .  *all
使用者 . . . . . .  *public
            + 尚有其餘值
權限 . . . . . .  *use
```

註: 如果檔案庫有大量物件，系統可能要花幾分鐘來處理您的要求。

完成檔案庫中所有物件的公用權限設定之後，接著您可以使用工作日誌來檢查您的工作。

使用工作日誌來檢查您的工作

當您使用 GRTOBJAUT 指令多方變更權限時，請檢視工作日誌來驗證所作的變更。

1. 請鍵入 DSPJOBLOG (顯示工作日誌)。
2. 按 **F10** (顯示詳細訊息)。
3. 您應該會收到有關檔案庫中每一個物件的權限變更訊息。請一邊複查這些訊息，一邊取消勾選清單中的物件。

```
                          顯示所有訊息
   系統:   RCHASxxx
工作 . .:  QPADEV0010    使用者 . :  JCHEIDEL      號碼 . . . . :  025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  針對 CUSTLIB 物件類型 *FILE 的物件 CUSTMAS，授予使用者 *PUBLIC 權限。
  針對 CUSTLIB 物件類型 *MSGQ 的物件 CUSTMSGQ，授予使用者 *PUBLIC 權限。
  授予 2 個物件權限。0 個物件無權限。0 個物件有部份權限。
  授予物件權限。
7>> dspjoblog
```

可能的錯誤	回復方式
工作日誌指出檔案庫中部份物件的權限並未變更。	使用「說明」(**F1**)，取得訊息的詳細資訊。使用 EDTOBJAUT，個別設定這些物件的權限。

現在您可以設定新物件的公用權限。

設定新物件的公用權限

檔案庫說明有一個「建立權限 (CRTAUT)」參數，它可以決定檔案庫中新建物件的公用權限。指令建立物件時，使用物件檔案庫的 CRTAUT 權限作爲預設值。您應該讓檔案庫的 CRTAUT 等於檔案庫中多數現有物件的公用權限。

1. 請鍵入 CHGLIB *檔案庫名稱*，然後按 **F4** (提示)。
2. 按 **F10** (其它參數)。
3. 在*建立權限*欄位中，輸入您的選擇。

```
                    變更檔案庫 (CHGLIB)

請鍵入選項，然後按 Enter 鍵。

檔案庫 . . . . . > CUSTLIB
檔案庫類型 . . . . . *PROD
文字「說明」 . . . . . 「客戶記錄」


                    其它參數

建立權限 . . . . . *CHANGE
建立物件審核 . . . . . *SYSVAL
```

如果您將 CRTAUT 設定爲 *SYSVAL，檔案庫新建物件時，系統是以現行設定值作爲 QCRTAUT 系統值。爲每一個檔案庫設定特定的 CRTAUT 權限，可以防止未來 QCRTAUT 系統值變更。

現在您可以使用群組及個人檔案庫。

使用群組及個人檔案庫

設定檔擁有您設定使用者群組及個別使用者時建立的群組及個人檔案庫。

您可以使用前述程序，將群組檔案庫所有權變更到群組設定檔，並將個人檔案庫所有權變更到個別使用者設定檔。請使用 EDTOBJAUT 指令。

您可以爲每一個群組及個人檔案庫設定「建立權限」參數，決定檔案庫中任何新物件的公用權限。請使用 CHGLIB 指令。

建立授權清單之前，請先完成這些作業：

- 使用「應用程式安裝套表」及您的「檔案庫說明套表」，確定您已經爲所有應用程式檔案庫建立所有權及公用權限。
- 爲您建立的所有群組及個人檔案庫設定所有權並建立權限。

  註: 鍵入 DSPOBJD *ALL *LIB *PRINT，即可獲得系統上所有檔案庫的清單。

建立授權清單

設定所有權及公用權限之後，接著您可以設定授權清單。您可以使用「授權清單套表」中的資訊來建立授權清單，用來保護檔案庫安全。請使用「建立授權清單 (CRTAUTL)」指令：

1. 請鍵入 CRTAUTL，然後按 **F4** (提示)。
2. 填寫「授權清單套表」中的資訊。
3. 按 **F10** (其它參數)。
4. 使用權限參數，指定由清單保護安全的物件的公用權限。
5. 檢查確認訊息。

```
                    建立授權清單 (CRTAUTL)

請鍵入選項，然後按 Enter 鍵。

授權清單 . . . . . .  custlst1
文字「說明」 . . . . . .  檔案清除於

                      其它參數

權限 . . . . . .  *ALL
```

可能的錯誤	回復方式
您鍵入的清單名稱不正確。	您不能變更系統建立的清單名稱。刪除清單 (DLTAUTL)，然後重試。
您忘記指定清單的公用權限。	使用「編輯授權清單 (EDTAUTL)」指令。

現在您可以使用授權清單保護物件安全。

使用授權清單保護物件安全

建立授權清單之後，您可以使用「編輯物件權限 (EDTOBJAUT)」指令來保護「授權清單套表」中項目的安全：

1. 鍵入 EDTOBJAUT，然後按 **F4** (提示)。
2. 填寫提示顯示畫面，然後按 **Enter** 鍵。
3. 在「編輯物件權限」顯示畫面中，輸入授權清單名稱。
4. 如果物件的公用權限來自授權清單，請將公用權限變更爲 *AUTL。
5. 對「授權清單套表」中的每一個物件重複這些步驟。

```
                        編輯物件權限

物件 . . . . . :   ARFILE01        擁有者 . . . . . :   OWNAR
  檔案庫 . . . . . :     CUSTLIB      主群組 . . . . . :   *NONE
物件類型 . . . . . :   *FILE

變更現行權限，然後按 Enter 鍵。

  由授權清單保護安全的物件     . . . . . .  CUSTLST1

                          物件
使用者       群組         權限
OWNER                     *ALL
*PUBLIC                   *AUTL
```

現在您可以將使用者新增至授權清單。

將使用者新增至授權清單

使用授權清單保護物件安全之後，您可以使用「編輯授權清單 (EDTAUTL)」指令來新增「授權清單套表」中列出的使用者：

1. 鍵入 EDTAUTL *授權清單名稱*。
2. 在「編輯授權清單」顯示畫面中，按 **F6** (新增使用者)。
3. 在清單中的項目上輸入使用者或群組名稱以及它們應該具備的權限，然後按 **Enter** 鍵。
4. 清單中會出現新的使用者。

```
                              新增使用者

物件 . . . . . :   WSLST1          擁有者   . .
  檔案庫 . . . . . :     QSYS

請鍵入新使用者，然後按 Enter 鍵。

               物件       清單
使用者         權限       管理
QSECOFR      *CHANGE
```

可能的錯誤	回復方式
您在清單中提供了錯誤的使用者或群組權限。	您可以在「編輯授權清單」顯示畫面中變更權限。
您在清單中新增了錯誤的使用者或群組。	您可以使用「移除授權清單項目 (RMVAUTLE)」指令來移除使用者或群組，或者，您也可以在「編輯授權清單」顯示畫面中的使用者權限上鍵入空白。

檢查您的工作

您可以使用「顯示授權清單 (DSPAUTL)」指令，將所有使用者權限列在授權清單中。在顯示畫面中按 **F15**，即可列出由授權清單保護安全的所有物件。

設定特定權限之前，請先完成這些作業：

- 使用 CRTAUTL 指令，建立應用程式所需的任何授權清單。
- 使用 EDTOBJAUT 指令，使用授權清單保護物件安全。
- 使用 EDTAUTL 指令，將使用者新增至授權清單。

設定特定權限

您在設定所有權及公用權限中學習了如何根據「檔案庫說明套表」第 1 部份的資訊，使用 GRTOBJAUT 指令來設定檔案庫中所有物件的公用權限。現在，您可以根據「檔案庫說明套表」第 2 部份的資訊，使用「編輯物件權限 (EDTOBJAUT)」指令來設定檔案庫及檔案庫中物件的特定權限。

設定特定權限時，請參閱這些主題：

- 設定檔案庫特定權限。
- 設定物件特定權限。
- 同時設定多個物件的權限。

設定檔案庫特定權限

檔案庫實際上是一種特殊類型的物件。爲檔案庫設定權限就像爲其他物件設定權限一樣，請使用 EDTOBJAUT 指令。所有檔案庫都常駐在 IBM 提供的 QSYS 檔案庫中。下列範例的顯示畫面，在 JKL Toy Company 的 CONTRACTS 檔案庫上使用「檔案庫說明套表」的第 2 部份：

列出檔案庫物件的特定權限				
群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. 鍵入 EDTOBJAUT，然後按 **F4** (提示)。
2. 填寫提示顯示畫面，然後按 **Enter** 鍵。

```
                    編輯物件權限 (EDTOBJAUT)

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . .  CONTRACTS
  檔案庫 . . . . .  QSYS
物件類型 . . . . .  *LIB
```

3. 在「編輯物件權限」顯示畫面中按 **F6** (新增使用者)，爲顯示畫面未列出的使用者提供權限。
4. 按 **Enter** 鍵。

```
                          新增使用者

物件 . . . . . :  CONTRACTS      擁有者 . . . . . :  OWNCP
  檔案庫 . . . . :  QSYS         主群組 . . . . . :  *NONE
物件類型 . . . . :  *LIB


請鍵入新使用者，然後按 Enter 鍵。

              物件
使用者        權限
DPTSM         *USE
DPTMG         *USE
```

5. 「編輯物件權限」顯示畫面應該符合「檔案庫說明套表」第 1 及第 2 部份的資訊。

```
                              編輯物件權限

物件 . . . . . :   CONTRACTS       擁有者 . . . . . :   OWNCP
  檔案庫 . . . . . :     QSYS        主群組 . . . . . :   *NONE
物件類型 . . . . . :   *LIB

變更現行權限，然後按 Enter 鍵。

  由授權清單保護物件安全  . . . . . . . . . . . . . . . . . . .   *NONE

                         物件
使用者       群組        權限
OWNCP                    *ALL
DPTSM                    *USE
DPTMG                    *USE
*PUBLIC                  *EXCLUDE
```

新物件 (CRTAUT) 權限的公用權限，未出現在檔案庫的「編輯物件權限」顯示畫面中。請使用「顯示檔案庫 (DSPLIB)」指令來查看檔案庫的 CRTAUT。

您也可以使用這個程序來設定系統上物件的特定權限。

現在您可以設定物件特定權限。

設定物件特定權限

設定應用程式檔案庫物件之特定權限的程序，與設定檔案庫的特定權限相同。範例在 JKL Toy Company 的 COPGMLIB 檔案庫上使用「檔案庫說明套表」的第 2 部份：

表 62. JKL Toy Company 的檔案庫說明套表

群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. 鍵入 EDTOBJAUT，然後按 **F4** (提示)。
2. 填寫提示顯示畫面中的資訊，然後按 **Enter** 鍵。
3. 填寫「編輯物件權限」顯示畫面中的權限資訊，然後按 **Enter** 鍵。

```
                              編輯物件權限

物件 . . . . . :   COMSGQ01        擁有者 . . . . . :   OWNCO
  檔案庫 . . . . . :     COPGMLIB    主群組 . . . . . :   *NONE
物件類型 . . . . . :   *MSGQ

變更現行權限，然後按 Enter 鍵。

  由授權清單保護物件安全  . . . . . . . . . . . . . . . . . . .   *NONE

                         物件
使用者       群組        權限
OWNCO                   *ALL
*PUBLIC                  *CHANGE
```

現在您可以同時設定多個物件的權限。

同時設定多個物件的權限

到目前爲止，這些範例使用 EDTOBJAUT 指令來設定單一物件的特定權限。您可以使用「授予權限 (GRTOBJAUT)」指令，設定多個物件的安全。請鍵入 GRTOBJAUT，然後按 **F4** (提示)。下列是多方變更權限的範例。

- 下列顯示畫面中輸入的欄位，將 CUSTLIB 檔案庫中所有訊息佇列的公用權限設定爲 *CHANGE。

```
                    授予物件權限 (GRTOBJAUT)

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . . . . . . . . . .   *all
  檔案庫 . . . . . . . . . . . .     custlib
物件類型 . . . . . . . . . . . .   *msgq
使用者 . . . . . . . . . . . . .   *public
             + 尚有其餘值
權限 . . . . . . . . . . . . . .   *change
```

- 下列顯示畫面中輸入的欄位，爲使用者 AMES 的 CUSTLIB 檔案庫中以 WRK 開頭的所有檔案名稱，提供 *ALL 權限。

```
                    授予物件權限

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . . . . . . . . . .   WRK*
  檔案庫 . . . . . . . . . . . .     custlib
物件類型 . . . . . . . . . . . .   *file
使用者 . . . . . . . . . . . . .   AMES
             + 尚有其餘值
權限 . . . . . . . . . . . . . .   *all
```

這個範例使用一種**同屬**命名技術來指定參數。許多指令可讓您指定第一個字元加上星號 (*) 的參數。系統會在名稱以這些字元開頭的各物件上執行作業。指令的線上資訊會指出哪些參數容許同屬名稱。

- 您需要執行兩個步驟，用授權清單 ARLST1 來保護名稱以 AR 開頭的所有檔案的安全，並從清單中取得檔案的公用權限。這些顯示畫面顯示所需步驟。

```
                    授予物件權限

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . . . . . . . . . .   AR*
  檔案庫 . . . . . . . . . . . .     CUSTLIB
物件類型 . . . . . . . . . . . .   *FILE

   ⋮
授權清單 . . . . . . . . . . . .   ARLST1
```

```
                        授予物件權限

請鍵入選項，然後按 Enter 鍵。

物件 . . . . . . . . . . . . . .   AR*
  檔案庫 . . . . . . . . . . . .     CUSTLIB
物件類型 . . . . . . . . . . . .   *FILE
使用者 . . . . . . . . . . . . .   *PUBLIC
             + 尚有其餘值
權限 . . . . . . . . . . . . . .   *AUTL
             + 尚有其餘值
```

您可以使用使用工作日誌檢查您的工作中描述的 DSPJOBLOG 指令，來驗證系統執行了要求的權限變更。

保護印表機輸出安全之前，請先使用 EDTOBJAUT 或 GRTOBJAUT 指令來設定「檔案庫說明套表」第 2 部份的特定權限。

保護印表機輸出安全

設定特定權限之後，您可以使用這些主題資訊來保護機密的印表機輸出：

- 建立輸出佇列及控制管理人員。
- 指派特殊印表機輸出至佇列。

建立輸出佇列

1. 鍵入 CRTOUTQ (建立輸出佇列)，然後按 **F4** (提示)。
2. 填寫輸出佇列名稱及檔案庫。
3. 按 **F10** (其它參數)。
4. 向下翻頁尋找輸出佇列的安全資訊。

```
                    建立輸出佇列 (CRTOUTQ)

請鍵入選項，然後按 Enter 鍵。

輸出佇列 . . . . . . . . . . . .>   NEWCP
  檔案庫 . . . . . . . . . . . .     CONTRACTS
排存檔大小上限：
  頁數 . . . . . . . . . . . . .   *NONE          數字, *NONE
  開始時間 . . . . . . . . . . .                  時間
  結束時間 . . . . . . . . . . .                  時間
             + 尚有其餘值
檔案佇列次序 . . . . . . . . . .   *FIFO
遠端系統 . . . . . . . . . . . .   *NONE

   ⋮
文字「說明」 . . . . . . . . . .   新的合約佇列
```

5. 填寫「輸出佇列及工作站安全套表」資訊，控制輸出佇列的使用和管理人員。
6. 按 **Enter** 鍵，然後檢查確認訊息。

```
                        建立輸出佇列 (CRTOUTQ)

請鍵入選項，然後按 Enter 鍵。


其它參數

顯示任何檔案 . . . . . .  *NO
工作分隔頁 . . . . . .  0
操作員控制 . . . . . .  *NO
資料佇列 . . . . . .  *NONE
  檔案庫 . . . . . .
檢查權限 . . . . . .  *OWNER
權限 . . . . . .  *LIBCRTAUT
```

可能的錯誤	回復方式
您按的是 **Enter** 鍵，而非 **F10**。	使用「變更輸出佇列 (CHGOUTQ)」指令來輸入其他資訊。
您的輸出佇列建立在錯誤的檔案庫中。	使用「移動物件 (MOVOBJ)」指令，將它移至正確的檔案庫中。

現在您可以指派印表機輸出至輸出佇列。

將印表機輸出指派至輸出佇列

建立輸出佇列之後，您可以將印表機輸出指派至輸出佇列中。印表機檔案通常會控制印表機的輸出目的地。請聯繫應用程式供應商，找出機密報告的印表機檔案名稱及檔案庫。

如果您無法存取這個資訊，請列印報告並將它保存在輸出佇列中。您可以使用「使用排存檔」顯示畫面中的屬性選項來找出印表機檔案名稱。印表機檔案會出現在「使用排存檔屬性」顯示畫面的*裝置檔案*欄位中。

若要變更印表機檔案目的地 (輸出佇列)，請使用「變更印表機檔案 (CHGPRTF)」指令：

```
CHGPRTF FILE(檔案庫名稱/印表機檔案名稱)
        OUTQ(檔案庫名稱/輸出佇列名稱)
```

有人再度要求報告時，報告會前往新的目的地。若要變更輸出佇列中的排存檔目的地，請使用「使用排存檔」顯示畫面中的變更選項。

例如，JKL Toy Company 的 Sharon Jones 想將價格清單印表機檔案 PRCLST1 指派至 PRICEQ 輸出佇列。她鍵入：

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

若要將所有價格清單報告指派至 PRICEQ 輸出佇列，Sharon 可以使用同屬印表機檔名：

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

若要將所有新合約導引到 NEWCP 輸出佇列，Sharon 可以變更在建立合約時使用的範例文件的相關輸出佇列。

檢查您的工作

檢查印表機機密輸出保護策略的最佳方法是將它列印出來。看看它是否輸出至正確的輸出佇列。另外再以系統操作員身份登入，看看能否看到或操作佇列中的檔案。

保護工作站安全之前，請確定您：

- 使用 CRTOUTQ 指令，建立「輸出佇列及工作站安全套表」中列出的輸出佇列。
- 使用 CHGPRTF 指令，將印表機輸出指派至新的輸出佇列中。

保護工作站安全

保護印表機輸出安全之後，接著應該保護工作站安全。授權工作站與授權系統其他物件相同。請使用 EDTOBJAUT 指令來提供工作站的使用者權限。

使用者必須有 *CHANGE 權限才能登入工作站。如果 QLMTSECOFR 系統值爲「否」(0)，則安全主管或任何有 *ALLOBJ 權限的人，可以登入任何工作站。

如果 QLMTSECOFR 系統值爲「是」 (1)，請使用這些引導說明來設定工作站權限：

可以登入工作站的使用者	公用權限	QSECOFR 權限	個別使用者權限
所有使用者	*CHANGE	*CHANGE	不需要
選定的使用者	*EXCLUDE	無權限	*CHANGE
選定的使用者以及有所有物件權限的使用者	*EXCLUDE	*CHANGE	*CHANGE
有所有物件權限的使用者之外的全部使用者	*CHANGE	無權限	不需要

限制存取系統操作員訊息佇列之前，請先根據「輸出佇列及工作站安全套表」中的資訊，使用 EDTOBJAUT 指令來保護工作站的安全。

限制存取系統操作員訊息佇列

您可以藉由保護印表機輸出安全、 保護工作站安全以及限制存取系統操作員訊息佇列，來改進安全性。

處理 ASSIST 功能表上訊息的選項，可讓使用者使用功能鍵來顯示系統操作員 (QSYSOPR) 訊息佇列。回應系統操作員訊息錯誤，會導致系統發生問題。使用者必須有 *CHANGE 權限，才能回應及刪除訊息佇列中的訊息。應該只有系統操作員有這個權限。請查閱「系統責任套表」，看看誰有系統操作員訊息佇列的 *CHANGE 權限。

請使用 EDTOBJAUT 指令：

1. 鍵入 `EDTOBJAUT QSYSOPR *MSGQ`，然後按 **Enter** 鍵。
2. 按 **F11**，即可顯示詳細的物件權限資訊。
3. 如範例顯示畫面所示，提供公用 *OBJOPR 權限，然後按 **Enter** 鍵。

```
                              編輯物件權限

物件 . . . . . :   QSYSOPR         擁有者 . . . . . :   QSYS
  檔案庫 . . . . . :     QSYS         主群組 . . . . . :   *NONE
物件類型 . . . . . :  *MSGQ

變更現行權限，然後按 Enter 鍵。

  由授權清單保護物件安全  . . . . . .   *NONE

                         物件       ----------物件---------------
使用者       群組        權限     操作員 管理 存在    變更   重整
*PUBLIC                 USER DEF     X
```

4. 系統將*物件權限*直欄變更爲 USER DEF (使用者定義)。
5. 再按 **F11**，即可顯示資料權限資訊明細。
6. 如範例顯示畫面所示，提供公用 *ADD 權限，然後按 **Enter** 鍵。

```
                              編輯物件權限

物件 . . . . . :   QSYSOPR         擁有者 . . . . . :   QSYS
  檔案庫 . . . . . :     QSYS         主群組 . . . . . :   *NONE
物件類型 . . . . . :  *MSGQ

變更現行權限，然後按 Enter 鍵。

  由授權清單保護物件安全  . . . . . .   *NONE

                         物件       ---------------資料---------------
使用者       群組        權限       讀取  新增 更新     刪除   執行
*PUBLIC                 USER DEF           X
```

7. 使用 **F6** (新增使用者)，新增必須回應 QSYSOPR 訊息的使用者。提供他們 *CHANGE 權限。

注意：請勿提供公用權限 *EXCLUDE。所有工作 (及使用者) 必須能將訊息新增至 QSYSOPR 訊息佇列中。

若要確定已完成資源安全設定，您應該：

- 使用「授權清單套表」及「檔案庫說明套表」，確定您已經爲所有應用程式檔案庫建立安全。
- 檢查「輸出佇列及工作站安全套表」，確定您已經保護了工作站並且建立了特殊的輸出佇列。
- 限制存取系統操作員 (QSYSOPR) 訊息佇列。
- 根據應用程式提供的指示，儲存應用程式檔案庫。系統會儲存應用程式及所有權和公用權限資訊。
- 使用「儲存安全資料 (SAVSECDTA)」指令，儲存您建立的安全資訊。有關如何儲存安全資訊的詳細資訊，請參閱儲存安全資訊。

現在您可以測試您的安全設定。

第 8 章 測試安全

這個主題說明一些測試系統上安全設定的技術。這個環境變數中的測試，是指確定您設定的安全皆以您預期的方式運作。監督安全主題是在討論如何評估系統安全效力。

系統做重大變更時，就應該測試安全。例如，新增應用程式、設定現有應用程式的資源安全、新增使用者群組，或是變更安全層次。

有關變更安全後要測試及診斷問題的相關方法，請複查這些主題：

- 測試使用者設定檔。
- 測試資源安全。

測試使用者設定檔

若要測試您的安全，也許您想在系統設定新群組時，測試使用者設定檔。您可以測試從群組設定檔複製來的一個個別設定檔。

- 使用這個使用者設定檔，能夠順利登入嗎？如果無法登入，請檢查未順利登入時撰寫的工作日誌。您可以使用 ASSIST 功能表的「使用印表機輸出」選項，尋找工作日誌中的詳細資訊。

  這些是常見的問題：

  – 缺少一個必要物件，如：起始功能表、現行檔案庫或起始程式。
  – 工作說明中指定的檔案庫清單，導致發生錯誤。可能是檔案庫不存在，或者是您忘記在檔案庫清單中併入 QGPL 及 QTEMP。
  – 使用者沒有工作站的授權。
- 登入後，螢幕是否顯示正確的起始功能表或程式？
- 在「登入」顯示畫面中輸入一個起始功能表或現行檔案庫時，發生什麼狀況？如果使用者設定檔是「限制功能」(YES)，您應該會收到一個錯誤訊息。
- 按「注意」鍵時，是否出現正確的顯示畫面？
- 是否輸出至正確的印表機？如果不是，請使用 ASSIST 功能表中的「使用印表機輸出」選項，尋找它輸出至何處。檢查使用者設定檔及工作說明，瞭解它爲何輸出至不同的印表機。
- 可以取得指令行嗎？
- 能否執行所需應用程式功能而不發生安全錯誤？詳細資訊，請參閱測試資源安全。
- 能否執行必要的系統作業，如：管理印表機或儲存檔案庫？

使用設定檔登入時，如果系統要求您指派新密碼，請在完成測試之後，將密碼設回使用者設定檔名稱：

1. 使用您自己的設定檔登入 (使用安全主管權限)。
2. 鍵入 CHGUSRPRF *設定檔名稱* PASSWORD(*設定檔名稱*) PWDEXP(*YES)。

現在您已經測試了使用者設定檔，接著要測試資源安全。

測試資源安全

測試使用者設定檔之後，您也應該測試資源安全。測試資源安全時，請尋找：

- 沒有足夠權限執行工作的使用者。
- 權限超過您預期的使用者。

測試權限不足

測試交談式功能及批次功能，看看使用者設定檔的權限是否足夠。

交談式測試

測試應用程式的資源安全時，您可能需要用幾種不同的使用者設定檔登入。您的目標是測試範例使用者，確定您指派給他足夠的權限。

- 測試功能，需要不同層次的權限：檢視、變更及刪除。
- 測試程式，不只是測試功能表。選取一個功能表選項，可能不足以測試權限。有時您必須實際執行某個作業，如：刪除記錄，系統才會存取檔案。系統開啓檔案時，會檢查權限。應用程式設計決定系統何時開啓檔案。
- 記錄安全錯誤，並且解決問題。發生權限錯誤時，顯示畫面上應該會出現一則訊息，告訴您作業權限不足以及您想使用的物件。

批次測試

- 使用提出工作的使用者的設定檔，執行應用程式的範例批次作業。
- 測試需要不同權限層次的批次作業，如：列印資訊、變更資訊或月底清除檔案。
- 檢查 QSYSOPR 訊息佇列及 QHST 日誌中的安全錯誤。使用 DSPLOG 指令來檢視 QHST 日誌。安全訊息的範圍如下：
  CPF2200、CPI2200、CPC2200、CPD2200、CPF4A00、CPI4A00 、CPC4A00 及 CPD4A00。

  您也可以使用安全審核功能來記錄權限失效和其他安全相關事件。

測試過多權限

如果您設定資源安全來保護機密資訊，請測試範例使用者設定檔，確定您的安全可以運作。請使用無法存取機密檔案的使者設定檔來登入。

- 您可以得到容許存取檔案的功能表嗎？
- 如果您選取的功能表選項需要使用檔案，會發生什麼狀況呢？
- 您可以得到指令行嗎？
- 您可以執行指令以列出檔案嗎？ (如：`CPYF FROMFILE(`*檔名*`) TOFILE(QSYSPRT)`)
- 您可以使用查詢工具來查看檔案嗎？

測試結果可能指出您需要變更安全資訊。

第 9 章 變更安全資訊

現在您已經規劃了系統安全，您還必須確定企業需要變更時，您的規劃仍然有效。

這個主題強調「簡易」是安全設計上的基本目標。您已經設計使用者群組，作爲個別使用者的型樣。您還嘗試使用公用權限、授權清單及檔案庫權限，而非使用特定的個別權限。您可以運用這個方法的優點來管理安全：

- 新增使用者群組或應用程式時，請使用您規劃安全時使用的技術。
- 需要變更安全時，請用一般方式，而非建立特例來解決特定問題。

安全指令主題說明一些用來顯示、變更及刪除安全資訊的指令。

如需不同變更類型的相關建議，請參閱這些主題：

- 將使用者新增至系統。
- 建立新使用者群組。
- 變更使用者群組。
- 新增應用程式。
- 新增工作站。
- 變更使用者的責任。
- 移除系統中的使用者。

安全指令

下表顯示您可以使用哪些指令來使用系統上的安全物件。您可以使用這些指令，執行這些作業：

- 檢視及列出安全資訊。
- 變更安全資訊。
- 刪除安全資訊。

表 63. 安全指令

安全物件	如何檢視	如何變更	如何刪除
系統值	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	無法刪除
工作說明	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
群組設定檔	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
使用者設定檔	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]

表 63. 安全指令 (繼續)

安全物件	如何檢視	如何變更	如何刪除
物件權限	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
物件所有權	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN 能讓您撤回前一個擁有者的權利。
主群組	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP 可將主群組設定爲 *NONE
物件審核	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (設定爲 *NONE) CHGAUD
授權清單	DSPAUTL DSPAUTLOBJ	EDTAUTL (清單的使用者權限) EDTOBJAUT (由清單保護安全的物件) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (整個清單)[3] RMVAUTLE (移除清單的使用者權限) EDTOBJAUT (由清單保護安全的物件) RVKOBJAUT

1. IBM 建議您使用「查看使用者列名」顯示畫面中的移除選項來刪除設定檔。這個選項可讓您刪除設定檔擁有的任何物件，或是將物件重新分派給新的擁有者。有些 DLTUSRPRF 指令參數可讓您刪除使用者擁有的所有物件，或是將物件指派給新的擁有者。刪除或重新分派擁有的物件後，才能刪除設定檔。您不能刪除任何物件的主群組設定檔。
2. 您不能刪除有成員的群組設定檔。請使用 DSPUSRPRF 指令的 *GRPMBR 選項，列出群組成員。刪除群組設定檔之前，請先變更每一個個別群組設定檔的*群組設定檔*欄位。
3. 您不能刪除用來保護物件安全的授權清單。請使用 DSPAUTLOBJ 指令，列出由清單保護安全的物件。您可以使用 EDTOBJAUT 指令，變更由清單保護安全的物件權限。

檢視及列出安全資訊

您可以使用顯示 (DSP) 指令與列印 (*PRINT) 選項，列出安全資訊。例如，若要顯示 MYLIST 授權清單，請鍵入 `DSPAUTL MYLIST *PRINT`。

有些顯示指令提供不同清單類型的選項。例如，建立個別使用者設定檔之後，您會使用 DSPUSRPRF 指令的 *GRPMBR 選項，列出群組設定檔的所有成員。您可以使用提示 (**F4**) 和線上資訊，尋找安全物件可用的清單。

您可以使用「顯示」指令來檢視顯示站上的安全資訊。您也可以使用「使用... (WRK)」指令，它提供更多的功能。「使用...」指令可以提供清單顯示畫面。您可以使用這個顯示畫面來變更、刪除及檢視資訊。

您也可以使用安全指令及同屬名稱來列出或檢視資訊。如果您鍵入 `WRKUSRPRF DPT*`，「查看使用者列名」顯示畫面或「查看使用者設定檔」顯示畫面只顯示以 *DPT* 開頭的設定檔。您可以使用指令的線上資訊，尋找容許同屬名稱的參數。

變更安全資訊

您可以使用「使用...(WRK)」或「編輯... (EDT)」指令，以交談方式變更安全資訊。您可以檢視資訊、變更資訊，並於變更之後再次檢視資訊。

您也可以使用「變更... (CHG)」或「授予... (GRT)」指令來變更安全資訊，而不需在變更前後檢視它。這個方法在同時變更多個物件時，特別有用。例如，使用 GRTOBJAUT 指令來設定檔案庫中所有物件的公用權限 (請參閱第 103 頁的『設定檔案庫中所有物件的公用權限』)。

刪除安全資訊

您可以使用「使用... (WRK)」和「編輯... (EDT)」指令，以交談方式刪除或移除某些類型的安全資訊。您也可以使用「刪除... (DLT)」、「移除... (RMV)」及「取消... (RVK)」指令來刪除安全資訊。通常您必須符合某些條件，系統才容許您刪除安全資訊。 安全指令中的附註，說明部份的條件。

將使用者新增至系統

如果您需要將使用者新增至系統，請使用下列程序：

1. 將人員指派至使用者群組。請參照使用者群組說明套表。
2. 決定新使用者是否需要執行系統功能。如果需要，請將資訊新增至系統責任套表。
3. 將人員新增至個別使用者設定檔套表。
4. 複查「系統責任套表」及「使用者群組說明套表」，判斷新使用者是否需要不同於群組的值。
5. 複製群組設定檔或群組成員的設定檔，來建立使用者設定檔。請確定將密碼設爲到期 (請參閱複製群組設定檔)。
6. 提供新使用者一個安全備忘錄複本。

若要學習如何建立新使用者群組，請參閱建立新使用者群組。

建立新使用者群組

您可能因爲幾個理由，而需要建立新使用者群組：

- 其他部門需要使用系統。
- 您必須有更特定的使用者群組，以符合資源安全需要。
- 公司重組部份部門。

若要建立新使用者群組，請執行下列作業：

1. 遵循規劃使用者群組中的指示，填寫使用者群組說明套表。
2. 新增使用者群組至應用程式、檔案庫及使用者群組的圖解中。
3. 評估是否有任何群組成員需要執行系統功能。更新「系統責任套表」 (請參閱決定負責系統功能的人員)。
4. 使用「使用者群組說明套表」及「系統責任套表」中的資訊，填寫「個別使用者設定檔套表」。
5. 建立群組檔案庫。
6. 建立群組工作說明。

7. 建立群組設定檔。

   註: 有關執行步驟 5、6 和 7 的相關指示，請參閱設定使用者群組。
8. 建立群組成員的個別使用者設定檔 (請參閱設定個別使用者)。
9. 評估群組所需的所有應用程式的「檔案庫說明套表」。使用設定資源安全中說明的技術，採用任何必要的步驟，提供群組存取權給應用程式物件。
10. 提供安全備忘錄複本給群組的所有成員。

若要學習如何變更使用者群組，請參閱變更使用者群組。

變更使用者群組

您必須用不同方法來處理不同類型的群組性質變更。下列是一些變更及處理範例：

變更群組的權限

您可能會發現群組需要起始規劃中沒有包含的物件權限。請執行下列作業：

1. 請使用「編輯物件權限 (EDTOBJAUT)」指令，讓群組存取正確的物件或適當的授權清單。 第 107 頁的『設定特定權限』中有處理範例。當您提供群組權限時，群組中的每個成員都得到物件權限。
2. 如果您提供機密資源的群組權限，可能要驗證群組的現行成員。請使用「顯示使用者設定檔」指令 (DSPUSRPRF *群組設定檔名稱* *GRPMBR)，列出群組成員。

變更群組自訂

您可能需要變更群組成員的使用者環境設定。例如，如果部門有了自己的印表機，您希望新印表機成爲部門使用者群組成員的預設印表機。或者，如果系統安裝新應用程式，使用者群組成員可能希望登入時有不同的起始功能表。

群組設定檔提供一個型樣，您可以複製它來建立群組成員的個別設定檔。您建立的群組設定檔自訂值，不影響個別使用者設定檔。例如，變更群組設定檔的*印表機裝置*欄位，不影響群組成員。您必須變更每一個個別使用者設定檔的*印表機裝置*欄位。

若要同時變更多個使用者的參數，請使用「查看使用者設定檔」顯示畫面。這個範例是變更群組所有成員的輸出佇列：

1. 鍵入 WRKUSRPRF *ALL，然後按 **Enter** 鍵。
2. 如果您看到「查看使用者列名」顯示畫面，請使用 **F21** (選取輔助層次) 變更至「查看使用者設定檔」顯示畫面。

```
                          查看使用者設定檔

請鍵入選項，然後按 Enter 鍵。
  1=建立    2=變更    3=複製    4=刪除    5=顯示
  12=依擁有者使用物件

      使用者
選項  設定檔        本文

                  HARRISOK          Harrison, Keith
2                 HOGANR            Hogan, Richard
                  JONESS            Jones, Sharon
2                 WILLISR           Willis, Rose

   ⋮
                                                              尚有資訊...
選項 1、2、3、4 及 5 的參數或指令
===> PRTDEV(PRT02)
F3=跳出    F5=重整    F12=取消    F16=重複定位於    F17=定位於
F21=選取輔助層次     F24=其餘鍵
```

3. 在您要變更的每一個設定檔旁鍵入 **2** (變更)。
4. 在顯示畫面底端的參數行中，鍵入參數名稱及新的值。如果您不知道參數名稱，請按 **F4** (提示)。
5. 按 **Enter** 鍵。您會收到每一個變更設定檔的確認訊息。

   雖然變更群組設定檔中的自訂欄位並不影響群組成員，但日後可能會有幫助。當您日後想要新增群組成員時，群組設定檔會提供一個型樣。它也是群組標準欄位值的一項記錄。

提供新應用程式的群組存取權限

使用者群組需要存取新應用程式時，您必須分析群組及應用程式的相關資訊。下列是建議的方法：

1. 查看新應用程式的「應用程式說明套表」以及您的應用程式、檔案庫及使用者群組的圖解，看看應用程式使用哪些檔案庫。將這些檔案庫新增至「使用者群組說明套表」中。
2. 更新應用程式、檔案庫及使用者群組的圖解，顯示使用者群組及應用程式間新的關係。
3. 如果群組的起始檔案庫清單應包括這些檔案庫，請使用「變更工作說明 (CHGJOBD)」指令來變更群組的工作說明。如果您需要使用工作說明上的協助，請參閱第 88 頁的『建立工作說明』。

   註: 當您新增檔案庫至工作說明的起始檔案庫清單時，並不需要變更這些使用工作說明的使用者設定檔。使用者下次登入時，起始檔案庫清單會自動新增這些檔案庫。
4. 評估您提供新應用程式的存取權限時，是否需要變更群組的起始程式或起始功能表。您必須使用 CHGUSRPRF 指令，個別變更每一個使用者設定檔的起始功能表或程式。
5. 複查應用程式使用的所有檔案庫的「檔案庫說明套表」。判斷檔案庫的公用存取權限，是否足夠群組的需要。如果不夠，您可能需要提供檔案庫、特定物件或授權清單的群組權限。請使用「編輯物件權限 (EDTOBJAUT)」和「編輯授權清單 (EDTAUTL)」指令來執行 (詳細資訊，請參閱設定資源安全)。

系統若要新增應用程式，請參閱新增應用程式。

新增應用程式

您應像規劃原始應用程式般，仔細規劃新應用程式的安全。請遵循相同程序：

1. 請準備應用程式的「應用程式說明套表」及「檔案庫說明套表」。
2. 更新應用程式、檔案庫及使用者群組的圖解。
3. 遵循規劃資源安全中的程序，決定如何保護新應用程式的安全。
4. 使用規劃您的應用程式安裝中說明的方法，準備「應用程式安裝套表」。
5. 評估應用程式的印表機輸出是否是機密，以及是否需要保護。必要時，請更新「輸出佇列及工作站安全套表」。
6. 遵循設定所有權及公用權限及設定資源安全中說明的步驟，來安裝及保護應用程式安全。

系統若要新增工作站，請參閱新增工作站。

新增工作站

系統新增工作站時，請考慮安全基本要求：

1. 新工作站的實體位置是否有安全危機 (如果您不太記得，請參閱規劃實體安全)？
2. 如果工作站確實有危機，請更新「輸出佇列及工作站安全套表」。
3. 您建立新工作站時通常應該使用公用權限 *CHANGE。如果它不符合工作站的安全基本要求，請使用 EDTOBJAUT 指令來指定不同的權限。

若要變更系統使用者的責任，請參閱變更使用者的責任。

變更使用者的責任

系統使用者在公司中接受新的工作或是新的責任時，您必須評估對使用者設定檔有何影響。

1. 使用者是否屬於不同的使用者群組？您可以使用 CHGUSRPRF 指令來變更使用者群組。
2. 需要變更設定檔中的任何自訂值嗎？如：印表機或起始功能表。您同樣也可以使用 CHGUSRPRF 指令來變更。
3. 新使用者群組的應用程式權限對該人員來說足夠嗎？
   - 請使用「顯示使用者設定檔 (DSPUSRPRF)」指令來查看舊的及新的群組設定檔的權限。
   - 也查看個別使用者設定檔的權限。
   - 使用 EDTOBJAUT 指令來執行必要的變更。
4. 使用者擁有任何物件嗎？您應該變更這些物件的所有權嗎？請使用「依擁有者使用物件 (WRKOBJOWN)」指令。
5. 使用者執行系統功能嗎？使用者需要執行新工作的系統功能嗎？如果必要的話，請更新「系統責任套表」並變更使用者設定檔。

若要學習如何從系統中移除使用者，請參閱移除系統中的使用者。

移除系統中的使用者

有人離開公司時，您應該立即從系統中移除此人的使用者設定檔。刪除使用者設定檔之前，您必須先刪除或轉送設定檔擁有的物件所有權。您可以使用 WRKOBJOWN 指令來執行，或是使用「查看使用者列名」顯示畫面中的選項 **4** (移除)。

在「查看使用者列名」顯示畫面中對設定檔選取選項 **4** (移除) 時，您會看到其他顯示畫面，可用來處理使用者擁有的任何物件。您可以選擇將所有物件提供給新擁有者，或是個別處理物件：

```
                              移除使用者

使用者 . . . . . :   HOGANR
使用者說明 . . . . . :   業務及行銷部門

若要移除這個使用者，請鍵入下列選項，然後按 Enter 鍵。

    1. 將這個使用者擁有的所有物件提供給新的擁有者。
    2. 刪除或變更這個使用者擁有的特定物件的擁有者。
```

如果您選擇個別處理物件 (選項 **2**)，螢幕上會列出這個使用者擁有的所有物件：

```
                              移除使用者

使用者 . . . . . :   HOGANR
使用者說明 . . . . . :   業務及行銷部門

新擁有者 . . . . . .                    名稱，按 F4 列出

若要移除這個使用者，請刪除或變更所有物件的擁有者。
請鍵入下列選項，然後按 Enter 鍵。
  2=變更為新擁有者    4=刪除    5=顯示明細

選項  物件         檔案庫        說明
 4   HOGANR       QUSRSYS       Hogan、Richard 訊息佇列
 4   QUERY1       DPTWH         庫存查詢
```

如果您選擇刪除物件，則會看到「確認刪除」顯示畫面。系統刪除物件後，您就可以移除使用者設定檔。您又會看到「查看使用者列名」顯示畫面，裡面有一則訊息告訴您系統已移除這個使用者。

第 10 章 儲存安全資訊

這個主題介紹安全資訊的儲存及復置概觀。規劃系統的備份及回復時，您必須考慮資訊的安全性以及資訊本身。請參閱「資訊中心」的備份、回復及可用性主題，它可以協助您設計完整的備份及回復規劃。

下列主題說明如何備份及復置您在設定安全時建立的安全資訊：

- 儲存系統值。
- 儲存群組及使用者設定檔。
- 儲存工作說明。
- 儲存資源安全資訊。
- 使用預設擁有者設定檔 (QDFTOWN)。
- 自損壞的授權清單回復。

儲存系統值

系統值儲存在系統檔案庫 QSYS 中。執行下列作業時，即會儲存 QSYS 檔案庫：

- 使用「儲存系統 (SAVSYS)」指令。
- 使用「儲存」功能表中的選項來儲存整個系統。
- 使用「儲存」功能表中的選項來儲存系統資訊。
- 使用「執行備份 (RUNBCKUP)」功能表中的選項來備份整個系統。

如果您需要回復整個系統，當您復置作業系統時，就會自動復置系統值。

請參閱接下來的儲存群組及使用者設定檔。

儲存群組及使用者設定檔

群組及使用者設定檔儲存在 QSYS 檔案庫中。當您使用「儲存系統 (SAVSYS)」指令或選取功能表選項來儲存整個系統時，就會儲存它們。

您也可以使用「儲存安全資料 (SAVSECDTA)」指令來儲存群組及使用者設定檔。

您可以使用「復置使用者設定檔 (RSTUSRPRF)」指令來復置使用者設定檔。正常順序如下：

1. 復置作業系統，它會復置檔案庫 QSYS。
2. 復置使用者設定檔。
3. 復置其餘的檔案庫。
4. 使用「復置權限 (RSTAUT)」指令，復置物件權限。

請參閱接下來的儲存工作說明。

儲存工作說明

建立工作說明時，您需要指定檔案庫所在的位置。 IBM 建議您在 QGPL 檔案庫中建立工作說明。

您可以將檔案庫儲存在工作說明所在的位置，以儲存工作說明。請使用「儲存檔案庫 (SAVLIB)」指令來執行。您也可以使用「儲存物件 (SAVOBJ)」指令來儲存工作說明。

您可以使用「復置檔案庫 (RSTLIB)」指令來復置檔案庫內容。您可以使用「復置物件 (RSTOBJ)」指令來復置個別工作說明。

請參閱接下來的儲存資源安全資訊。

儲存資源安全資訊

資源安全可用來定義使用者使用物件的方式，它是由幾個儲存在不同地方的不同類型資訊所組成：

表 64. 儲存及復置資源安全資訊

資訊類型	儲存位置	儲存方式	復置方式
公用權限	與物件一起	SAVxxx 指令 [1]	RSTxxx 指令 [2]
物件審核值	與物件一起	SAVxxx 指令 [1]	RSTxxx 指令 [2]
物件所有權	與物件一起	SAVxxx 指令 [1]	RSTxxx 指令 [2]
主群組	與物件一起	SAVxxx 指令 [1]	RSTxxx 指令 [2]
授權清單	QSYS 檔案庫	SAVSYS 或 SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
物件與授權清單間的鏈結	與物件一起	SAVxxx 指令 [1]	RSTxxx 指令 [2]
專用權限	與使用者設定檔一起	SAVSYS 或 SAVSECDTA	RSTAUT

1. 您可以使用 SAVOBJ 或 SAVLIB 指令，儲存大部份的物件類型。有些物件類型，如：配置，有特殊的儲存指令。
2. 您可以使用 RSTOBJ 或 RSTLIB 指令，復置大部份的物件類型。有些物件類型，如：配置，有特殊的復置指令。

需要回復應用程式或整個系統時，您必須仔細地規劃步驟，包括回復物件權限。下列是回復應用程式資源安全資訊時的基本步驟：

1. 如果必要，復置使用者設定檔，包括擁有應用程式的設定檔。您可以使用 RSTUSRPRF 指令，復置特定的設定檔或所有設定檔。
2. 復置應用程式使用的任何授權清單。當您使用 RSTUSRPRF USRPRF(*ALL) 時，就會復置授權清單。

   註: 它會從備份媒體復置所有使用者設定檔值，包括密碼。
3. 使用 RSTLIB 或 RSTOBJ 指令，復置應用程式檔案庫。它會回復物件所有權、公用權限，以及物件和授權清單間的鏈結。
4. 使用 RSTAUT 指令，復置物件的專用權限。RSTAUT 指令也會復置授權清單的使用者權限。您可以復置特定使用者或所有使用者的權限。

有關復置系統之外之物件及擁有者設定檔的相關資訊，請參閱使用預設擁有者設定檔 (QDFTOWN)。

使用預設擁有者設定檔 (QDFTOWN)

復置物件時，如果擁有者設定檔不在系統中，系統會將物件所有權轉換爲預設設定檔 QDFTOWN。回復擁有者設定檔或重新建立之後，您可以使用「依擁有者使用物件 (WRKOBJOWN)」指令將所有權轉換回來。

有關授權清單回復的詳細資訊，請參閱自損壞的授權清單回復。

自損壞的授權清單回復

保護物件安全的授權清單損壞時，有所有物件 (*ALLOBJ) 特殊權限的使用者才能存取物件。

自損壞的授權清單回復，需要兩個步驟：

1. 回復授權清單上的使用者及其權限。
2. 回復授權清單與物件的連結。

有 *ALLOBJ 特殊權限的使用者，可以完成這些步驟。

步驟 1：回復授權清單

如果您知道授權清單的使用者權限，請刪除授權清單後再重新建立，然後再爲它新增使用者。

如果您不知道授權清單的所有使用者權限，請使用這些步驟，從最後的 SAVSYS 或 SAVSECDTA 磁帶復置它：

1. 刪除損壞的授權清單：

   ```
   DLTAUTL AUTL(授權清單名稱)
   ```

2. 復置授權清單：

   ```
   RSTUSRPRF USRPRF(*ALL)
   ```

3. 使用「復置權限 (RSTAUT)」指令，將使用者新增至清單中。

步驟 2：回復授權清單的物件連結

復置授權清單或是重新建立之後，您還需要建立清單和由它保護安全的物件之間的鏈結：

1. 使用「收回儲存體 (RCLSTG)」指令。RCLSTG 會將由損壞或遺失之授權清單保護安全的物件，指派至 QRCLAUTL 預設清單中。
2. 列出由 QRCLAUTL 授權清單保護安全的物件：

   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```

3. 使用 GRTOBJAUT 指令，以正確的授權清單來保護物件安全。例如，若要使用授權清單 ARLST01 來保護 CUSTLIB 檔案庫中的 ARWRK01 檔案，請鍵入

   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

第 11 章 監督安全

這個主題提供監督系統安全防護效率的基本建議。

定期監督安全，有兩個基本目標：

- 確定適當地保護公司資源。
- 偵測未獲授權存取系統及公司資訊。

當您決定要定期監督作業時，請複查安全原則陳述式及使用者安全備忘錄。

有關監督安全的詳細資訊，請參閱下列主題：

- 監督安全核對清單。
- 安全審核。

監督安全核對清單

下列是複查系統中不同安全觀點的核對清單。可用來開發您的規劃。

監督實體安全

- 防止備份媒體損壞與遭竊。
- 限制存取公用區域中的工作站。您可以使用 DSPOBJAUT 指令來查看誰有工作站的 *CHANGE 權限。

監督系統值

- 驗證設定值確實符合「系統值選項套表」。請使用「列印系統安全屬性 (PRTSYSSECA)」指令。
- 複查系統值決策，尤其是安裝新應用程式時。

監督群組設定檔

- 驗證群組設定檔確實沒有密碼。請使用 DSPAUTUSR 指令，驗證所有群組設定檔的密碼都是 *NONE。
- 驗證群組成員的人員正確無誤。請使用 DSPUSRPRF 指令和 *GRPMBR 選項，列出群組成員清單。
- 檢查每一個群組設定檔的特殊權限。請使用 DSPUSRPRF 指令。如果正於安全層次 30、40 或 50 上執行，群組設定檔應該沒有 *ALLOBJ 權限。

監督使用者設定檔

- 驗證系統上的使用者設定檔，屬於下列一個種類：
  - 現行員工的使用者設定檔
  - 群組設定檔
  - 應用程式擁有者設定檔
  - IBM 提供的設定檔 (以 Q 開頭)
- 使用者調職或離開公司時，移除他的使用者設定檔。使用者一旦離開，請使用「變更有效期限排程項目 (CHGEXPSCDE)」指令，自動刪除或停用設定檔。

- 尋找非作用中設定檔並且移除它。設定檔的非作用中狀態達指定時間時，請使用「分析設定檔活動 (ANZPRFACT)」指令，自動停用設定檔。
- 判斷哪些使用者的密碼與使用者設定檔同名。請使用「分析預設密碼 (ANZDFTPWD)」指令。請使用這個指令選項，強制使用者在下次登入系統時變更密碼。

  注意：請勿從系統中移除 IBM 提供的任何設定檔。IBM 提供的設定檔以 Q 開頭。
- 請注意誰的使用者類別不是 *USER 與原因。請使用「列印使用者設定檔 (PRTUSRPRF)」指令，列出所有使用者以及使用者類別和特殊權限。拿這項資訊與「系統責任套表」比對。
- 控制哪些使用者設定檔的*限制功能*欄位設定爲 *NO。

監督關鍵物件

- 複查可以存取關鍵物件的人員。請使用「列印專用權限 (PRTPVTAUT)」指令及「列印公開授權物件 (PRTPUBAUT)」指令，監督物件。如果群組有存取權限，請使用 DSPUSRPRF 指令的 *GRPMBR 選項來驗證群組成員。
- 驗證誰可以使用應用程式以另一個安全方法 (如：採用權限) 來存取物件。請使用「列印採用物件 (PRTADPOBJ)」指令。

監督未授權的存取

- 指示系統操作員注意 QSYSOPR 訊息佇列中的安全訊息。尤其要系統操作員在有人重複嘗試登入失敗時通知安全主管。安全訊息的有效範圍是 2200 至 22FF 以及 4A00 至 4AFF。安全訊息的字首是 CPF、CPI、CPC 及 CPD。
- 設定安全審核，記載嘗試未授權存取物件。

請參閱接下來的安全審核。

安全審核

作業系統在監督安全時，會記錄系統上所發生的安全事件。這些事件會記錄在名爲**異動日誌接收器**的特殊系統物件中。您可以根據需求來設定異動日誌接收器，使其記錄不同類型的安全事件，例如變更系統值或使用者設定檔，或記錄不成功的物件存取嘗試。以下各值可用來控制所記錄的事件：

- 審核控制 (QAUDCTL) 系統值
- 審核等級 (QAUDLVL) 系統值
- 使用者設定檔中的審核等級 (AUDLVL) 值
- 使用者設定檔中的物件審核 (OBJAUD) 值
- 物件中的物件審核 (OBJAUD) 值。

審核日誌內的資訊是用來：

- 偵測安全違規試圖。
- 規劃移轉至更高的安全層次。
- 監督敏感物件的使用情形，例如機密檔案。

本系統提供有相關指令，供您以不同方式來檢視審核日誌中的資訊。

第 12 章 基本系統安全規劃套表

您可以透過瀏覽器來複製或列印這些套表。

若要列印整個安全基本資訊，請選取右窗格，然後按一下「資訊中心」旗標中的 PDF 圖示。

若要列印單一規劃套表，請按一下所要列印之規則套表的對應鏈結。按一下右窗格，然後按一下瀏覽器中的「列印」圖示。如此就會列印所選取的套表。

以下是各類規劃套表的完整清單，這些套表可讓您順利規劃及使用基本系統安全：

- 實體安全規劃套表
- 應用程式說明套表
- 命名慣例套表
- 檔案庫說明套表
- 系統值選項套表
- 系統責任套表
- 使用者群組識別套表
- 使用者群組說明套表
- 個別使用者設定檔套表
- 授權清單套表
- 輸出佇列與工作站安全套表
- 應用程式安裝套表

實體安全規劃套表

表 65. 實體安全規劃套表

實體安全規劃套表	
準備人員：	日期：
說明 • 有關這個套表，請參閱規劃資源安全。 • 您可以使用這個套表來說明有關主機實際位置及附屬裝置的安全議題。 • 您不需要將套表資訊輸入系統中。	
主機：	
說明保護主機的安全措施 (如：房間上鎖)：	
一般使用的按鍵鎖定位置爲何？	
鑰匙的存放位置？	
有關主機的其他說明：	
備份媒體及文件：	
企業存放備份磁帶的位置？	
工作區外存放備份磁帶的位置？	

表 65. 實體安全規劃套表 (繼續)

安全主管、服務程式及 DST 密碼的保存位置？	
重要系統文件 (如：序號及配置資料) 的保存位置？	

實體安全規劃套表			2 / 2
第 2 部份的其他說明 • 以下列出可能因位置而暴露安全的工作站或印表機。指出您採取的保護措施。印表機會在安全暴露直欄下列出列印機密報告的範例。 • 如果您讓系統自動配置區域裝置，則您必須等到系統安裝完成後，才會知道工作站和印表機的名稱。準備此套表時，如果您不知道這些名稱，請先填寫說明 (如：位置)，稍後再加入名稱。			
工作站及印表機的實體安全			
工作站或印表機名稱	它的位置或說明	安全暴露	採取的保護措施

應用程式說明套表

表 66. 應用程式說明套表

應用程式說明套表	
準備人員：	日期：
說明 • 有關這個套表，請參閱說明您的應用程式及規劃資源安全。 • 每一個應用程式準備一個套表。 • 您不需要將此套表資訊輸入到系統中。	
應用程式名稱：	縮寫：
應用程式的簡短說明：	
主功能表名稱：	檔案庫：
起始程式名稱：	檔案庫：
列出應用程式使用的檔案庫及程式庫：	
定義應用程式的安全目標，如：是否有機密資訊：	

命名慣例套表

表 67. 命名慣例套表

命名慣例套表	
準備人員：	日期：

表 67. 命名慣例套表 (繼續)

說明	
• 有關這個套表，請參閱說明您的應用程式。 • 您不需要直接將套表資訊輸入系統中。 • 您可以使用這個套表來說明您如何指派系統物件名稱。每個物件不妨提供一些範例。	
物件類型	**命名慣例**
群組設定檔	
使用者設定檔	
授權清單	
檔案庫	
檔案	
行事曆	
裝置	
磁帶	

檔案庫說明套表

表 68. 檔案庫說明套表

檔案庫說明套表	1 / 2
準備人員：	日期：
說明： • 有關這個套表，請參閱規劃使用者安全及規劃資源安全。 • 您可以使用這個套表來說明主要檔案庫，並定義它的資源安全基本要求。 • 爲系統中每個主要應用程式檔案庫填寫一個套表。 • 有關如何輸入套表資訊，請參閱設定資源安全。	
檔案庫名稱：	描述性名稱 (文字)：
簡單說明檔案庫的功能：	
定義檔案庫的安全目標，如：是否有機密資訊：	
檔案庫的公用權限：	
檔案庫物件的公用權限：	
新物件的公用權限 (CRTAUT)：	
檔案庫擁有者：	

檔案庫說明套表				2 / 2
準備人員：			日期：	
檔案庫名稱：				
第 2 部份的其他說明： • 下列圖表中列出需要特定權限的所有個人或物件。 • 指定所需權限類型： *ALL、*CHANGE、*USE 或 *EXCLUDE。				
列出檔案庫物件的特定權限				
群組設定檔或使用者設定檔	物件名稱	物件類型	所需權限	授權清單

系統值選項套表

表 69. 系統值選項套表

系統值選項套表		1 / 2
準備人員：		日期：
說明 • 有關這個套表的詳細資訊，請參閱規劃您的整體對策。 • 您可以使用這個套表來記錄您選擇的會影響安全及自訂的系統值。 • 請使用 SETUP 功能表中的選項 **1** 來輸入這個套表的第 1 部份。		
「變更系統選項」顯示畫面中的值		
系統值/網路屬性	**建議選項**	**您的選擇**
系統名稱		
日期分隔字元 (QDATSEP)		
日期格式 (QDATFMT)		
時間分隔符號 (QTIMSEP)		
新裝置的裝置命名格式 (QDEVNAMING)	1 (iSeries 系統)	
系統印表機 (QPRTDEV)		
安全層次 (QSECURITY)	40	
允許安全主管登入任何顯示站 (QLMTSECOFR)	N	
儲存有關已完成印表機輸出的工作帳戶資訊 (QACGLVL)	N (*NONE)	

系統值選項套表		2 / 2
第 2 部份的其他說明 • 有關這個套表的第 2 部份的詳細資訊，請參閱設定系統值。 • 您可以使用「使用系統值 (WRKSYSVAL)」指令來輸入第 2 部份。		
安全系統值		
系統值	**建議選項**	**您的選擇**
非作用中工作逾時間隔 (QINACTITV)	30 到 60	
非作用中工作訊息佇列 (QINACTMSGQ)	*DSCJOB	
限制裝置階段作業 (QLMTDEVSSN)	1 (YES)	

嘗試登入失敗後採取的動作 (QMAXSGNACN)	3 (兩者皆停用)	
嘗試登入次數上限 (QMAXSIGN)	3 到 5	
密碼過期間隔 (QPWDEXPITV)	30 到 60	
密碼長度上限 (QPWDMAXLEN)	8	
密碼長度下限 (QPWDMINLEN)	6	
需要不同的密碼 (QPWDRQDDIF)	7 (6 個單一密碼)	
其他系統值		
系統值	**建議選項**	**您的選擇**
切斷工作逾時間隔 (QDSCJOBITV)	300	
註: 有時您可能需要設定有關安全的其他系統值。如需有關安全的系統值完整清單以及建議的系統值，請參閱 *Security-Reference* (SC41-5302-04) 的第三章。		

系統責任套表

表 70. 系統責任套表

系統責任套表			
準備人員：		日期：	
說明： • 有關這個套表，請參閱規劃個別使用者設定檔。 • 您可以使用這個套表來列出使用者類別不爲 *USER 的使用者。 • 將這個套表資訊傳送到「個別使用者設定檔」套表中的*使用者類別*直欄。			
誰是您的主要安全主管？ 誰是您的代理安全主管？			
設定檔名稱	使用者名稱	類別	說明

使用者群組識別套表

表 71. 使用者群組識別套表

使用者群組識別套表	
準備人員：	日期：
說明： • 有關這個套表，請參閱規劃使用者群組。 • 這個套表可以協助您識別出需要類似應用程式的使用者群組。 1. 在此套表頂端列出您的主要應用程式。 2. 在左側直欄列出您的使用者。 3. 標示每位使用者所需的應用程式。 • 您不需要將套表資訊輸入系統中。	

表 71. 使用者群組識別套表 (繼續)

		應用程式需要的存取權						
使用者名稱	部門	應用程式：	應用程式：	應用程式：	應用程式：	應用程式：	應用程式：	應用程式：

註:

- 如果您的安全保護環境爲*寬鬆*，請使用 **X** 來標示使用者所需的應用程式。
- 如果您的安全保護環境爲*嚴密*，您可能需要使用 **C** (變更) 及 **V** (檢視) 來指定*如何*使用應用程式。

使用者群組說明套表

表 72. 使用者群組說明套表

使用者群組說明套表	1 / 2
準備人員：	日期：
第 1 部份的說明 • 有關如何準備這個套表，請參閱規劃使用者群組。 • 有關如何輸入這個套表，請參閱設定使用者安全。 • 爲每個要使用系統的群組準備一個套表。 • 您可以使用「建立工作說明 (CRTJOBD)」指令來建立群組的工作說明。工作說明具有群組的起始檔案庫清單。	
群組設定檔名稱： 群組說明：	
群組的主要應用程式： 列出群組需要的其他應用程式：	
列出群組需要的每一個檔案庫。請標示出 (✓) 應該放在群組起始檔案庫清單中的每一個檔案庫：	
註: 請查看上一節列出的各應用程式的「應用程式說明套表」，找出應用程式使用的檔案庫。	

使用者群組說明套表	2 / 2
第 2 部份的其他說明 • 下表列出「建立使用者設定檔」顯示畫面中呈現的所有欄位。這些欄位分成兩個群組：需要您選擇的欄位以及 IBM 建議預設值的欄位。 • 您可以使用「查看使用者設定檔」顯示畫面或「建立使用者設定檔 (CRTUSRPRF)」指令，將這個部分的套表資訊輸入到您的系統中。	

選擇群組設定檔中的這些欄位值：		
欄位名稱	**建議選項**	**您的選擇**
群組設定檔名稱 (使用者)		
密碼	*NONE	
使用者類別 (使用者類型)	*USER	
現行檔案庫 (預設檔案庫)	*與群組設定檔同名*	
呼叫的起始程式 (登入程式)		
起始程式庫		
起始功能表 (第一個功能表)		
起始功能表檔案庫		
限制功能 (限制指令行使用)	*YES	
文字 (使用者說明)		
工作說明	*與群組設定檔同名*	
工作說明檔案庫		
群組設定檔名稱 (使用者群組)	*NONE	
列印裝置 (預設印表機)		
輸出佇列	*DEV	
註: 這些欄位依「建立使用者設定檔」顯示畫面 (使用 F4) 中的次序排列。		
下列欄位使用系統提供值 (預設值)：		
帳戶碼	鍵盤緩衝法	公用權限
輔助層次	語言 ID	將密碼設爲到期
岔斷程式	限制裝置階段作業	排序順序
編碼字集 ID	儲存體上限	特殊權限
國家或地區 ID	訊息佇列	特殊環境
顯示登入資訊	密碼過期間隔	狀態
文件密碼	優先順序限制	使用者選項
註: 這個清單中的欄位按字母順序排列。		

個別使用者設定檔套表

表 73. 個別使用者設定檔套表

個別使用者設定檔套表	
準備人員：	日期：
說明： • 有關如何準備這個套表，請參閱規劃個別使用者設定檔。 • 這個套表可用來記錄個別系統使用者的相關資訊。爲系統中每一個使用者群組 (群組設定檔) 填寫一個套表。 • 右邊空白欄可作爲個別使用者的附加欄位。 • 有關如何輸入這個套表，請參閱設定個別使用者。	
群組設定檔名稱：	
建立的物件擁有者：	建立的物件群組權限：

表 73. 個別使用者設定檔套表 (繼續)

群組權限類型：						
爲每個群組成員製作一個登錄：						
使用者設定檔	文字 (說明)	使用者類別	限制功能			

授權清單套表

表 74. 授權清單套表

授權清單套表					
準備人員：			日期：		
說明 • 有關這個套表，請參閱規劃資源安全。 • 爲每個授權清單準備一個套表。 • 您可以使用此套表，列出具有存取此清單安全權限的清單物件、群組物件及個別物件。 • 有關如何輸入這個套表，請參閱設定資源安全。					
授權清單名稱：					
說明：					
列出清單保護安全的物件					
物件名稱	物件類型	物件檔案庫	物件名稱	物件類型	物件檔案庫
列出可以存取清單的群組及使用者					
群組或使用者	容許的存取類型	清單管理？	群組或使用者	容許的存取類型	清單管理？

表 74. 授權清單套表 (繼續)

印表機輸出佇列與工作站安全套表

表 75. 印表機輸出佇列與工作站安全套表

印表機輸出佇列與工作站安全套表				
準備人員：		日期：		
說明 • 有關這個套表，請參閱保護印表機輸出。 • 您可以在這個套表中爲需要特殊保護的工作站或輸出佇列製作一個登錄。 • 有關如何輸入這個套表，請參閱保護工作站。				
列出限制輸出佇列的參數：				
輸出佇列名稱	輸出佇列檔案庫	顯示所有檔案 (DSPDTA)	檢查權限 (AUTCHK)	操作員控制 (OPRCTL)
安全主管工作站： 如果您有限制的安全主管只能存取特定工作站 (系統值 QLMTSECOFR 爲是)，請在下面列出授權給安全主管以及任何有 *ALLOBJ 權限的人員的工作站：				
請在下面列出限制工作站的權限：				
工作站名稱	獲得授權的群組或使用者 (*CHANGE 權限)			
註: 限制工作站的公用權限應該設定爲 *EXCLUDE。				

應用程式安裝套表

表 76. 應用程式安裝套表

應用程式安裝套表	1 / 2
準備人員：	日期：

表 76. 應用程式安裝套表 (繼續)

說明 • 有關這個套表，請參閱規劃您的應用程式安裝。 • 爲每個要安裝的應用程式準備一個套表。 • 您可以使用這個套表來規劃如何在載入應用程式後，建立它的所有權及公用權限。 • 有關如何輸入這個套表，請參閱設定資源安全。		
應用程式名稱：		
說明：		
列出及解釋安裝應用程式時必須建立的設定檔：		
檔案庫名稱：		
	安裝之前	安裝之後
檔案庫擁有者		
物件擁有者		
檔案庫公用權限		
物件公用權限		
新物件的公用權限		
檔案庫名稱：		
	安裝之前	安裝之後
檔案庫擁有者		
物件擁有者		
檔案庫公用權限		
物件公用權限		
新物件的公用權限		

應用程式安裝套表		2 / 2
檔案庫名稱：		
	安裝之前	安裝之後
檔案庫擁有者		
物件擁有者		
檔案庫公用權限		
物件公用權限		
新物件的公用權限		
檔案庫名稱：		
	安裝之前	安裝之後
檔案庫擁有者		
物件擁有者		
檔案庫公用權限		
物件公用權限		
新物件的公用權限		
檔案庫名稱：		

	安裝之前	安裝之後
檔案庫擁有者		
物件擁有者		
檔案庫公用權限		
物件公用權限		
新物件的公用權限