

內控制度

電腦化資訊處理循環

	頁	次
電子計算機循環控制程序		
一、電子計算機循環流程圖	1	- 1
二、作業內容及控制重點		
CC-101 資訊部門與使用部門權責之劃分作業	1	- 2
CC-102 資訊部門之功能及職責劃分作業	1	- 3
CC-103 系統開發及程式修改控制作業	1	- 4
CC-104 編制系統文書控制作業	1	- 5
CC-105 程式及資料存取控制作業	1	- 6
CC-106 資料輸出入控制作業	1	- 7
CC-107 資料處理之控制作業	1	- 9
CC-108 檔案及設備安全控制作業	1	- 10
CC-109 硬體及系統軟體之購置、使用及維護控制作業	1	- 12
CC-110 系統復原計劃制度及測試程序控制作業	1	- 13
CC-111 資通安全檢查作業	1	- 14
CC-112 公開資訊申報作業	1	- 17

附則

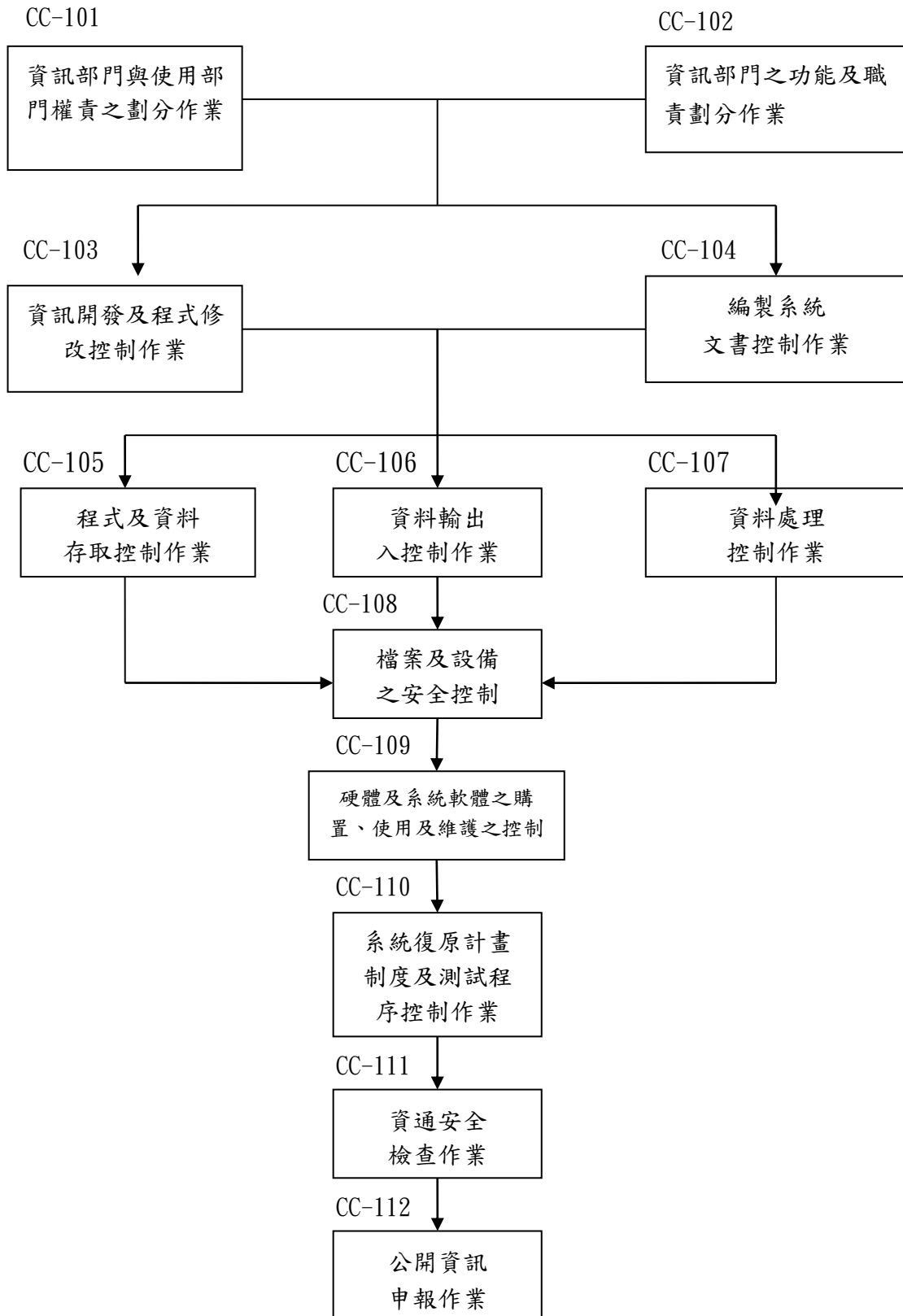
1. 制修廢：

本制度屬於管理規章，經由總經理核准，呈董事會審議承認後頒布實施；修訂或廢止時亦同。

2. 公告實施：

本制度自民國 109 年 11 月 10 日起施行。

一、流程圖



CC-101

資訊部門與使用部門權責之劃分作業

一、作業程序：

(一) 資訊部職責劃分如下：

1. 資訊單位內部人員編制及所負責職務由資訊單位主管擬定，報請核准後聘僱人員執行相關業務。
2. 資訊單位主管負責各部門溝通、協調及評估，定期與各部門檢討業務需求；擬定公司中、長期資訊系統發展方向。
3. 硬體工程師負責硬體維護、網路架設及對外網路之安全維護、維持作業系統與各應用軟體之正常運作。
4. 系統開發/應用系統工程師負責應用程式系統分析、系統架構、程式設計、測試除錯及編製應用程式之書面文件。

(二) 資訊部職責劃分如下：

1. 資訊作業制度之訂定與維護。
2. 統籌作業系統及應用系統之規劃、開發事宜。
3. 使用者帳號密碼管理作業。
4. 使用者權限設定作業。
5. 資料輸出/輸入管制作業。
6. 系統恢復之規劃與執行。
7. 電腦軟硬體設備之管理作業。
8. 委外廠商評估、聯繫及監控作業。
9. 資訊系統安全性測試。

(三) 使用單位規範：

1. 負責提出資訊系統軟硬體需求。
2. 確保業務作業流程與電腦處理流程一致。
3. 應對實際作業環境之資料負全責，即正確操作電腦系統以確保資料之正確性、完整性。
4. 提出電腦資訊系統需求、進一步需求資料及詳細需求說明。
5. 準備相關測試個案及測試資料。
6. 進行系統測試及提供系統測試紀錄及文件。
7. 配合修改與電腦化後之相關作業控制制度、控管重點。
8. 協助評估各項電腦系統作業之績效。
9. 監控委外廠商所提供之服務。

二、控制重點：

- (一) 明確定義職掌內容。
- (二) 除代理人外，權責有無重疊現象。
- (三) 使用單位依相關作業規範，執行資料處理。
- (四) 程式管理人員不得兼代資料輸入之操作。
- (五) 資訊部門人員僅止建置及維護電子計算機之運作，其他各單部門單位之工作事項均由各部門自行處理。

三、參考資料：使用權限表。

四、使用表單：維護需求單。

CC-102 資訊部門之功能及職權劃分作業

一、作業程序：

(一)資訊部門功能：

1. 統籌全公司資訊管理有關事項，負責公司資訊系統之規劃、推動、維護、管理及支援作業。
2. 資訊系統之資訊來源及使用則為各使用單位，資訊單位人員不負責資訊系統之資料來源、核准及使用。
3. 電腦資訊軟硬體之規劃、評估與維護。
4. 視部門需要統籌規畫及調配公司之電腦資訊軟硬體。
5. 資訊單位之電腦資訊軟硬體設備之採購建議與維護。
6. 電腦資訊網路規劃、架設與維護。
7. 各類套裝軟體導入。
8. 應用系統開發與維護。
9. 資訊單位與各相關部門應有明確權責之劃分，避免資訊權限管轄不當；並且定期更新使用者權限表。

(二)資訊管理之職能：

1. 資訊系統之規劃，資訊系統之評估、購置、推行、維護、管理及支持。
2. 電腦軟硬體採購規格審核，設備及機房之管理。
3. 各部門資訊需求之整合及使用者有關資訊系統之教育訓練。

(三)職責劃分：

1. 資訊單位內部人員編制及所負責職務由資訊單位主管擬定，報請核准後聘僱人員執行相關業務。
2. 資訊單位主管負責各部門溝通、協調及評估，定期與各部門檢討業務需求；擬定公司中、長期資訊系統發展方向。
3. 硬體工程師負責硬體維護、網路架設及對外網路之安全維護、資訊系統維護、檢校、測試資訊系統，維持系統程式與各應用軟體之正常運作。
4. 系統開發/應用系統工程師負責應用程式系統分析、系統架構、程式設計、測試除錯及編製應用程式之書面文件。

二、控制重點：

- (一)系統開發/應用系統人員是否與系統安全管理/使用者明確劃分。
- (二)資訊部是否獨立於其他使用單位。

三、參考資料：使用權限表。

四、使用表單：無。

一、作業程序：

◆ 系統開發控制

1. 系統開發申請由使用單位填寫「資訊需求申請單」，填寫需求項目及要點，並告知詳細作業流程與所需之報表格式，並經由相關權責主管核准。
2. 經資訊單位評估使用單位實際作業需求，確認可行且有開發新系統必要時，由資訊單位以簽呈方式提出，於簽呈中說明系統開發之初步評估結果，檢附「系統規格說明書」，確認規劃功能符合申請單位需求。
3. 系統開發人員於開發環境系統進行測試，確定程式邏輯性之合理及其運用，驗證系統功能是否符合申請單位之需求規格，於程式中加上註解，且保留測試文件。
4. 單元測試完成會同申請單位於測試環境進行測試，將測試結果記錄於「資訊需求申請單」，並檢附相關報表及測試畫面交由申請單位驗收，若仍需改善，則再由專案開發小組進行評估及更正。
5. 經由資訊單位直屬主管授權之執行人員負責將系統上線至系統正式環境，並建立軟體版本更新之機制。
6. 上線完成後，將「資訊需求申請單」交由資訊單位確認後歸檔留存。程式及運作流程修改後，相關之系統文件，資訊單位應配合修正。
7. 資訊系統委外開發時，應於事前審慎評估可能潛在安全風險，並與廠商簽訂資訊安全保密協定，以課予相關的安全管理責任。
8. 合約內容包含委外時程表、完成時間、維護方式、付款方式、版權、軟硬體需求、交付文件、相關賠償方式及所有必要之安全要求等，委外作業合約內容應完備嚴密。
9. 應於委外資訊系統規畫之需求分析階段，即將安全需求納入；新發展的資訊系統或是現有系統功能之強化，應明訂資訊安全需求，並將安全需求納入系統功能。
10. 委外作業之開發、設計、程式撰寫、測試及驗收等各階段須依合約規定程序進行，並備妥各階段之相關文件。
11. 委外開發系統程式撰寫完成後，委外廠商須自行測試無誤後再交付資訊單位主管，由資訊組人員協同申請單位共同測試，確定程式邏輯性之合理及其運用、驗證系統功能是否符合申請單位之需求規格。
12. 委外系統上線作業前，應確實執行適當的測試計畫，以驗證系統功能符合既定的安全標準。。

二、參考資料：無。

三、使用表單：

- (一) 資訊需求申請單。
- (二) 系統規格說明書。

CC-103

系統開發及程式修改控制作業(續)

一、作業程序：

◆ 程式修改控制

1. 系統分析人員於修改程式前，需與申請單位進行討論瞭解細部需求，依申請單位之需求提出「資訊需求申請單」並留存各階段會議紀錄，須由申請單位確認。
2. 與申請單位確認需求後，系統開發人員於系統開發環境中執行程式修改並完成單元測試，確定程式邏輯性之合理性及其運用、驗證系統功能是否符合申請單位之需求規格，且於修改之程式加上註解，並保留相關測試文件。
3. 單元測試完成由資訊單位會同申請單位於測試環境進行測試，將測試結果記錄於「資訊需求申請單」，並檢附相關報表及畫面。
4. 上線完成後，將「資訊需求申請單」由資訊單位人員確認後歸檔留存。
5. 已上線之系統，若有程式修改之需求，應由使用單位填寫「資訊需求申請單」提出需求。
 - a. 變更作業控制程序，應確保系統安全控制程序不會被破壞，且任何的系統變更作業，皆應經資訊單位主管同意
 - b. 使用單位若有緊急修護系統之需求時，仍須依規定由各級權責主管核准後方由資訊單位辦理。
 - c. 為維護作業之正常運作，除非必要，應避免不必要之修改。
 - d. 修改程式應建立正式的變更控制程序，並嚴格執行，以降低可能的安全風險。

二、控制重點：

1. 需求單位有增、修程式之需求時，是否依規定填寫「資訊需求申請單」，是否經適當核准，是否經相關部門之確認。資訊單位是否評估程式開發效益。
2. 完成系統設計或程式修改後是否會同相關單位進行功能測試，無誤後方交由需求單位使用。
3. 相關文件是否隨程式修改而配合修正。
4. 系統納入使用前是否經充分測試。
5. 系統上線至系統正式環境，資訊人員應建立軟體更新的版本控制機制。

三、參考資料：無。

四、使用表單：

- (一) 資訊需求申請單。
- (二) 程式測試紀錄。
- (三) 修改紀錄日誌。

CC-104

編製系統文書
控制作業

一、作業程序：

(一) 系統文件，系統標準化之建置：

1. 新資訊系統開發，委外廠商應編寫系統文件，包含：『系統規格說明書』、『系統文件』、『使用者操作說明書』、『系統測試紀錄』、『驗收文件』等。
2. 系統開發人員編寫、維護系統程式時，應於程式中註解，並依程式異動內容，適時修改相關文件。
3. 資訊系統於開發、維護完成後，資訊部門人員得協助使用單位編制作業手冊，以作為日後使用者操作之標準。
4. 各項系統文件與使用手冊，避免未授權之存取；人員離職時，主管應指派交接之人員。
5. 若確定舊版本之系統文件、使用手冊已無需再使用，應於資訊單位主管核准後將其銷毀。
6. 自行開發系統軟體或購買套裝軟體程式，資訊單位均應編製或轉交使用者操作說明書予使用單位；若有借閱需求時則須填寫電腦軟體/書籍借用紀錄表。

(二) 文件的存取：

1. 文件的存放取用應有資訊單位人員管理。
2. 對於文件的取用權利應有適當之限制。
3. 過期或不適用文件應加以銷毀。

二、控制重點：

- (一) 系統文件是否由資訊單位保管。
- (二) 系統修改時，系統文件、程式文件、操作文件是否隨之修改。

三、參考資料：無。

四、使用表單：

- (一) 電腦軟體/書籍借用紀錄表。
- (二) 系統文件/系統規格書。
- (三) 系統測試紀錄。
- (四) 驗收文件。

CC-105

程式及資料存取控制作業

一、作業程序：

- (一) 本作業程序所提電腦系統使用單位，包括公司管理單位及飯店單位。
- (二) 使用者用完電腦時必須離線，個人電腦不使用時需關機。
若欲申請使用 ERP 系統、使用特殊網路服務應填具「資訊帳號申請單」，並符合職能分工的牽制原則，經部門主管核准後，再送資訊部主管簽核。
- (三) 系統程式應對有權存取某特定檔案的程式，限制其功能〔例如：僅讀、寫、讀寫...〕。
檔案讀取，限於預先許可之工作權限內為之。
系統使用者之密碼均應定期更換，且避免使用以前使用過的密碼。
- (四) 電腦系統使用單位操作人員因故離職或調職時，資訊部門必須在員工職務調整或離職後刪除或修改此系統之權限，以避免人為之非法使用。

二、控制重點：

- (一) 程式檔案之存取使用是否依密碼之權限加以管制。
- (二) 非資訊部門人員是否無存取主機系統公用程式、工具及指令之權限。
- (三) 使用者是否定期更改密碼，密碼設定均應限制其最低字元，並結合文字、數字。

三、參考資料：無。

四、使用表單：

- (一) 資訊帳號申請單

一、作業程序：

(一) 資料輸入管理：

1. 資料之輸入及修改需經適當之覆核及授權。
2. 使用單位應依照需輸入資料之性質，設計適合之「資料修改申請表」；若作業流程不適合產生異動單據，使用單位應適時保存原始相關資料。
3. 原始相關資料及憑證，應由專人負責保管，並存於安全處所。
4. 各項輸入「資訊需求申請單」應配合填寫該內容，資料輸入控制應配合單號控管，遇有漏號、單據遺失，應立即追蹤，以確保資料之完整性。
5. 資料輸入完成後，應將異動單據及原始憑證等相關資料，送交各相關單位存查。
6. 為確保資料輸入正確，在輸入之資料轉換為電腦可閱讀之形式時，須嚴加控制，自動化控制須與人工程序適當併用，其人工控制方法包括：資料檢誤、資料驗證、文件數量之核對、批次控制之核對。
7. 系統應建立作業流程以確保輸入之資料係經過驗證和編輯且盡可能符合交易實質內容，程式化之輸入格式可確保資料係依正確之格式輸入正確之欄位，利用電腦自動化控制包括：序號之核對、極限值之核對、範圍之核對、有效性之核對、合理性之核對、檢查號碼之核對、完整性之核對、重複性之核對、邏輯關係之核對。
8. 系統間資料拋轉之輸入，應設計資料完整性、正確性之自動檢查功能；若系統檢查發現錯誤，應自動產生相關異常警訊或報表，並由專人負責追蹤。

(二) 輸出的控制：

1. 僅有經適當授權人員始可進行資料或報表之輸出或列印作業（分為螢幕上列印、印表機列印、轉成檔案、透過網路傳送等方式）。
2. 輸出資料應分發予適當授權人員，機密性、敏感性之資料輸出設計有適當管控程序，由專人負責輸出、分送、保管，並建立分發清單及簽收記錄。
3. 系統應產生重要資料鍵入、主檔變更及系統自動產生交易之審計軌跡報告（如交易明細報告），以供核對及調節原始輸入憑證。
4. 各單位依照各自輸出資料之性質，訂定保存方式、保存期間、銷毀方式等適當之規範。

(三) 更正例外或異常輸出項目：

1. 發現資料錯誤應會同相關人員查明原因，須填寫「電腦系統資料異動申請單」報請權責主管核准修正後，更正資料並將申請單與相關文件妥善保存備查。
2. 更正例外或異常項目之再輸入應調節至原例外或異常項目。

二、控制重點：

- (一) 輸入資料(原始單據)之編製、核准及覆核是否適當分工。
- (二) 錯誤資料之更正，是否經過適當之申請程序，並經主管人員核准。
- (三) 是否由有權限之人員進行輸出作業。
- (四) 機密性及敏感性資料的輸出是否有適當之管制。

三、參考資料：無。

四、使用表單：

- (一) 電腦系統資料異動申請單。

一、作業程序：

1. 電腦主機作業

- a. 負責資料處理之電腦主機及相關設備於保固期到期後應簽訂維護合約。
- b. 若出現異常情況時，先行採取排除異常之應變措施。如無法自行排除時，應立即通知維護廠商派員前來處理，並留下服務紀錄服務單。
- c. 機器運轉中如發生異常狀況，應判斷是否會影響進行中之工作，如需立即停機時，立刻通知使用者暫停作業，並隨即進行修復，待修復完畢並運轉正常後，再行通知使用者重新使用。
- d. 機器故障損及資料時，資訊人員應先進行資料回復作業並通知使用者自行查驗，避免影響日後資料之正確性及完整性。
- e. 凡與主機相關之重大異常狀況需紀錄於機房工作記錄表，並說明異常狀況及處理方式以便於日後追蹤
- f. 資訊單位針對使用者操作說明書，將會定期檢視並更新，以確保適用於目前作業狀況。

2. 應用系統軟體

- a. 系統內部作業應建立驗證資料正確性之作業程序，避免正確輸入至應用系統之資料因系統處理錯誤而產出不正確之結果。
- b. 系統應針對重要資料、重要批次作業，分別設計產生自動檢核序號、處理參數的複查機制之控制。
- c. 人工或系統之處理控制應能確定交易業已記錄於適當之會計期間。
- e. 系統應提供使用者作業處理中各項錯誤或作業失敗之訊息，並產生錯誤報表以利追蹤更正。
- f. 使用者有變更或更新資料處理程序時，應先提出申請並經過相關權責主管核准。
- g. 資訊人員應及時追蹤並更正例外或異常之訊息，並由專人覆核、更正並定期追蹤處理情形。
- h. 資料媒體內外應貼有標籤，標籤上註明日期及檔案名稱。
- i. 進行資料轉換前須先擬定資料轉換計畫，並進行資料備份，並比較資料轉換前後新舊系統之執行結果是否正確。
- j 如有運用外界電子資料處理中心以處理電子資料時，對於資料往返傳輸應具有上述之相關控製作業，以確保資料之完整性及安全性。
- k. 資訊單位針對使用者操作說明書，將會定期檢視並更新，以確保適用於目前作業狀況。

二、控制重點：

- (一) 新密碼之申請，是否均依權責呈核。
- (二) 資料處理完，其輸出報表有無核對其正確性。
- (三) 輸出資料發現錯誤，是否確實更正。

三、參考資料：無。

四、使用表單：

- (一) 服務紀錄單。
- (二) 機房進出表。

一、作業程序：

1. 資料檔案之安全作業

- A. 應用程式及資料檔，應妥善備份；資料應依其重要性，進行日、週，等不同週期之備份作業，並設定適當之存放期限，針對應永久保存之資料則應另行使用適當媒體儲存。
- B. 備份之資料媒體需適當記錄於備份記錄表中，並應於備份儲存媒體貼上內外標籤以利辨識備份內容。
- C. 備份資料應定期執行測試作業，適當記錄於備份資料測試紀錄表，以確保備份資料之可用性。
- D. 備份資料應異地存放，媒體存放處所環境應合於電腦機房安全標準。
- E. 資料及文件應就其重要性妥適區分安全等級，並透過系統設定或文件管理達到安全控管之目的。
- F. 系統使用單位對於檔案之使用應依照程式及資料存取控制作業辦理。
- G. 為避免檔案資料或硬體設備遭病毒毀損，應建立系統自動偵測病毒之機制，並要求所有人員定期更新病毒碼。
- H. 備份資料至少保留三天。

2. 電腦設備之安全作業。

- A. 資訊設備於購入時，資訊單位應會同使用單位驗收，移轉資訊設備則應填具資產異動申請單，經移出與移入單位經辦人員與主管簽核後送交資訊組存查。
- B. 電腦設備及其存放之資料於報廢時應填具資產異動申請單，申請進行報廢程序，以避免機密資料流失。
- C. 行動式電腦設備之攜出攜入則應填寫「設備借用記錄表」。

3. 電腦報廢流程之規範

- A. 各使用單位報廢電腦應辦理固定資產異動，繳回管理資訊部門。
- B. 進行報廢電腦檢測，區分良品與非良品。
 - a. 良品做為資訊設備備品用，減少資源重複購買浪費，降低各部門費用支出。
 - b. 非良品的儲存裝置如：硬碟、光碟片、記憶卡，進行內部儲存資料刪除銷毀。
- C. 儲存裝置內資料的消除，透過格式化，將儲存內部資料徹底清除。
- D. 人事及股務、財務個人資料之硬體儲存裝置進行物理性破壞，避免公司及個人資料外洩。

CC-108

檔案及設備安全控制作
業（續）

4. 電腦機房作業

- A. 電腦機房應設有適當之門禁管制（例如：門鎖、刷卡或指紋機）；資訊組人員對非作業人員進出電腦機房，應請其登記於電腦機房進出表，並於資訊組人員陪同下方可進入，嚴禁未經許可人員擅入機房。
- B. 資訊單位主管應定期覆核授權進出機房人員，並檢視門禁管制記錄。
- C. 各項資訊設備依預定使用目的存放於電腦機房內，不應放置其他易燃或危險物品。
- D. 機房內應設置獨立之空調設備以維持穩定正常之溫濕度狀態。
- E. 機房內應設置高架地板，或將設備固定於合乎安全標準之架上。
- F. 需備有自動火警偵測及緊急照明設備，以警示火災訊息，滅火器應置於明顯易取得之位置。
- G. 應安裝自動電壓穩定裝置，以維護設備安全及系統穩定性。重要設備應裝設不斷電系統（UPS）及電源供應器以避免作業因停電而中斷。
- H. 滅火器及不斷電系統等機房防護設備，應定期檢查與維護，並測試其堪用性。
- I. 電腦機房使用之空調、電源等相關設備，應有適當之備援對策。

二、控制重點：

- （一）資訊人員是否定期執行檔案備份作業。
- （二）備份儲存媒體之調借是否填寫相關單據並經權責主管核准。
- （三）電腦機房是否限制非相關人員進入。
- （四）系統發生異常狀況時，是否加以瞭解原因、改進及紀錄。
- （五）系統應有定期偵測病毒功能，資訊部門應定期更新偵測病毒軟體之版本。

三、參考資料：

- （一）無

四、使用表單：

- （一）資訊設備借用表
- （二）機房進出紀錄表
- （三）備份紀錄表

CC-109

硬體及系統軟體之購
置、使用及維護控制作
業

一、作業程序：

1. 電腦硬體及系統軟體之作業

A. 使用單位依業務需求，欲購置電腦硬體及系統軟體時，須以『簽呈』方式經主管覆核後送交資訊單位。經資訊單位評估相容性、擴充性、業務特性及成本效益後，開立符合需求之硬體設備，並經主管核准後，依「資訊設備採購暨管理辦法」執行請購作業。

B. 資訊硬體及系統軟體統一由資訊單位負責請購，由資訊人員填寫「請購單」，經資訊單位主管覆核後送交採購單位進行採購，驗收作業則統一由資訊單位執行，確認驗收完成交付使用單位保管使用。

C. 為確保尊重智慧財產權，落實使用合法版權軟體。

D. 若為委外開發之系統，其版權與相關製作之文件應屬於公司資產，於開發完成後交由資訊單位歸檔。

2. 電腦硬體及系統軟體使用作業

A. 使用單位對於電腦硬體及系統軟體之使用及維護應依照操作手冊之說明進行操作。

B. 使用者於應用系統使用完畢後必須離線或登出，個人電腦不使用時需關機或將螢幕上鎖。

C. 使用者借用資訊設備或系統軟體，應填寫「設備借用記錄表」。

3. 軟、硬體設備維護作業

A. 重要之系統主機與應用系統，若經資訊單位評估須由委外廠商提供維護服務者，應與委外廠商簽訂維護合約，並將資訊安全相關議題納入考量，訂定適當之資訊安全協定，規範委外廠商系統維護所接觸資料之安全管理。

B. 資訊單位各承辦人員應於合約到期前提出續約申請，經相關權責主管核准後進行採購作業。

C. 電腦設備維護如為委外處理者，委外廠商執行人員應留下服務紀錄交由資訊單位留存。

D. 主機系統維護工作，應避免停機並干擾使用者，儘可能安排在夜間、假日或無人使用狀態下進行停機作業之處理。

E. 一般事務性電腦設備於發生故障時，使用者應填寫報修單通知資訊單位派員維修，並記錄機器故障原因及維修狀況。

F. 經資訊單位人員確認硬體設備故障需送交廠商維修者。依「電腦使用者軟、硬體使用規範」進行送修之管理作業。

二、控制重點：

(一) 軟硬體之購置是否有「請購單」，並經請購單位及資訊部門驗收，並由財產管理單位編入財產目錄。

(二) 軟硬體之維護是否與供應廠商簽訂定期維護合約或由 IT 單位自行維護。

(三) 更新系統軟體是否經適當核准，且有關其中之設定文件是否適當存檔與保管。

三、參考資料：無。

四、使用表單：請購單

CC-110

系統復原計劃制度及測試程控制作業

一、作業程序：

1. 系統復原計畫之規劃

- A. 應建立跨單位之系統復原計畫，研訂及維護系統災害復原程序。
- B. 研擬備援及回復計畫，其內容包括下列項目之說明：資料庫、檔案及程式之備援及回復。
- C. 不管是電腦系統或是電力、空調、消防系統發生異常，事後相關人員確實檢討原因，並謀求改進與對應預防措施。
- D. 所訂定之重大異常狀況系統復原計畫應至少一年演練一次，以使相關人員熟悉重大異常狀況發生時，系統之應變措施及復原程序。
- E. 相關復原計畫請參考”資料備份及還原流程圖”

2. 系統復原計畫之測試及演練作業

- A. 系統復原計畫可能因事前的假設不正確、規劃不周全或設備及人員的職務調整變更，而無法發揮預期的作用，應至少一年一次測試及演練，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。
- B. 測試與演練過程紀錄於”資料復原測試紀錄表”，於事後召開檢討會議，針對測試缺失謀求改進，並留存記錄，作為計畫更新之參考依據。
- D. 若將復原計畫委外施行，應與委外廠商簽定合乎上述要點之合約，並定期監控委外廠商之作業是否合於作業規範。

3. 系統復原計畫更新作業

- A. 系統復原計畫應配合業務、組織、系統及人員的調整變更而一年一次定期更新，以發揮計畫投資的效益及確保計畫持續有效。
- B. 更新系統復原計畫後應與部門內部溝通協調，並將相關訊息通知相關人員。

二、控制重點：

- (一) 是否定期測試系統復原計劃需製作資料復原測試紀錄表。
- (二) 事件發生時是否依重大意外事故之資料復原計劃辦理。
- (二) 是否有異地備份。

三、參考資料：備份清單。

四、使用表單：

- (一) 資料復原及還原流程圖。
- (二) 測試紀錄表。

一、作業程序：

(一) 系統安全監控

1. 公司內部應有專業人員負責處理有關資訊系統安全預防及危機處理相關事宜，以防範電腦網路犯罪與危機，維護資訊系統安全。
2. 應建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取，造成機密資料之外洩，資訊部門應關閉不必要之網路服務，其他部門若有需要應經適當核准方能申請，另遠端登入管理資訊系統亦應經適當核准。
3. 對於跨公司之電腦網路系統（例如：飯店與總公司之間的網路系統），應特別加強網路安全管理，並且對內安裝防毒軟體，設置對外之網路防火牆，以防止電腦病毒、攻擊性之惡意軟體入侵，而造成公司網路系統癱瘓。防火牆應定期檢查，併同網路服務項目之系統日誌檔記錄於「系統備份復原測試紀錄表」並經適當主管核准。
4. 員工電子郵件之申請及使用規範，由資訊部門統一辦理，另須教育員工正確使用合法軟體之概念，促使員工正確認知電腦病毒的威脅，進一步提昇員工的資訊安全警覺。

(二) 分工及權限

1. 網路申報系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的人員管理，防止非相關人員存取系統資訊。
2. 最高使用權限人員，應依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，應立即撤銷該使用者之帳號及權限。
3. 使用者之帳號及密碼，應避免使用容易被識破及猜測的密碼，並且應定期更改密碼。

(三) 資料備份及維護方式

1. 網路系統管理人員應負責網路安全規範的擬訂，執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性。
2. 個人電腦及網路系統伺服器，應具備電腦病毒掃瞄工具，並且定期掃瞄電腦病毒與更新病毒碼。
3. 個人電腦及網路系統之資料，應定期備份重要檔案及資料，以備不時之需。
4. 申報之資料應經適當之保存。

二、控制重點：

(一) 公司內部是否有專業人員負責處理有關資訊系統安全預防及危機處理相關事宜，範圍包括了公司管理單位及飯店單位。

(二) 是否建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，防止未經授權的系統存取。

(三) 對於跨公司之電腦網路系統（例如：飯店與總公司之間的網路系統），是否對內安裝防毒軟體，對外設置網路防火牆。

CC-111 資通安全檢查作業 (續)	<p>(四) 網路申報系統的最高使用權限，是否經權責主管人員審慎評估。</p> <p>(五) 公司是否依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，是否立即撤銷該使用者之帳號及權限。</p> <p>(六) 使用者之帳號及密碼，是否避免使用容易被識破及猜測的密碼，並且是否定期更改密碼。</p> <p>(七) 個人電腦及網路系統伺服器，是否具備電腦病毒掃瞄工具。</p> <p>(八) 個人電腦及網路系統之資料，是否定期備份重要檔案及資料。</p> <p>(九) 申報之資料是否儲存於電腦內，並以光碟儲存備份。</p> <p>三、參考資料：</p> <p>(一) 資通安全政策</p> <p>(二) 資訊系統管理辦法</p> <p>資訊安全規範</p> <p>四、使用表單：</p> <p>(一) 系統備份復原測試紀錄表</p> <p>(二) 電腦系統使用狀況抽查表</p>
---------------------------	--

CC-112

公開資訊申報作業

一、作業程序：

(一) 網路申報系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的人員管理，防止非相關人員存取系統資訊，申報人員與私密金鑰保管人員應由不同人擔任，金鑰保管人員應妥善保管，申報人員應經適當核准方能向保管人員索取金鑰使用。

(二) 最高使用權限人員，應依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，應立即撤銷該使用者之帳號及權限。

(三) 使用者之帳號及密碼，應避免使用容易被識破及猜測的密碼，並且應定期更改密碼。

(四) 公司應申報之公開資訊、重大訊息等項目，應依相關法令辦理，並於規定時限內申報完成。

(五) 資料製作及申報方式：公開資訊之申報檔案分為格式化檔案及非格式化檔案兩大類。

(六) 申報資料、方式與申報時限：

1. 申報人員應依「公開發行公司應公告或向本會申報事項一覽表」及「公開資訊觀測站」申報操作手冊之規定辦理。

2. 應申報項目之檔案格式、資料內容、申報時限及申報方式，日後如有增減變動或名稱變更時，應依主管機關最新頒布之函令辦理。

3. 申報人需先行將上傳之公開資訊列印出來，並經權責主管簽核後，始能予以申報。

4. 上傳後之公開資訊，申報人需妥善予以保管二年。

(七) 金鑰磁片之使用及保管由公司授權專責人員負責。

(八) 上傳之原始資料經部門主管書面核定後交金鑰磁片保管人申報。

(九) 上傳後之原始文件由製作部門負責管理及保存。

(十) CA 憑證應於有效期間內使用，逾期得提出申請。

(十一) CA 憑證應做適當之備份並妥善保管。

(十二) 已上傳之資料如有錯誤，應立刻進行更正。

二、控制重點：

(一) 隨時注意證券主管機關訂定「公開發行公司應公告或向本會申報事項一覽表」更新情形，各項應申報資料應於期限內辦理。

(二) 資訊公開前應經權責主管核准。

(三) 各項資料申報應於期限內辦理。

(四) 檔案上傳後應確認已上傳成功並為證期局指定之資訊申報網站所接受。

(五) 資訊對外揭露後，相關資料應以電子檔案或書面形式分類歸檔留存。

三、參考資料：

(一) 公開發行公司網路申報公開資訊應注意事項

(二) 「公開資訊觀測站」申報操作手冊

(三) 其他相關法規

四、使用表單：無。