寶綠特資源再生工程股份有限公司

電腦化資訊系統管理制度

二〇一八年一月

目　錄

BRT-EP-01 資訊處理部門之功能及權責劃分

1.目的

明確規範資訊單位之功能及使用部門之職責劃分，確保公司作業電腦化規劃及資料處理之獨立性。

2.範圍

資訊單位功能及職掌之界定，並明確劃分資訊單位與使用者部門之權責。

3.權責單位

3.1.資訊單位：集團資訊系統由本公司統籌管理，在權責劃分原則下善盡職責，適當分工並達到控制、勾稽功能。

3.2.使用單位：依實際及未來作業狀況向資訊單位提出作業需求，包含集團內所有子公司。

4.控制重點

4.1.資訊單位應持超然獨立之立場執行其職務，並不得逾越未經授權之事宜。

4.2.資訊單位與使用單位應適當劃分職責、權限。

4.3.各項電腦及週邊設備應經資訊單位簽核始可辦理異動。

5.程序內容

5.1.資訊單位之功能

5.1.1 設置獨立於使用單位以外之專職資訊人員，俾達成下列功能：

5.1.1.1.推展各項應用系統，加強電腦化。

5.1.1.2.促進各部門對電腦軟硬體之充分有效使用。

5.1.1.3.發揮電腦作業迅速、省力及連貫作業之特性，提高公司各項作業之效率及品質。

5.1.1.4.運用電腦自動勾稽機能，達到內部控制目標。

5.1.2.協助與電腦相關之自動化工作。

5.2.資訊單位之職責

5.2.1.統籌規劃全公司作業及應用系統之安全、運用及系統整合事宜。

5.2.2.全公司電子計算機軟、硬體需求等之審核與驗收。

5.2.3.「電腦化資訊系統管理制度」之訂定及維護。

5.2.4.災難回復管理之規劃與執行。

5.2.5.設備規劃與管理

5.2.5.1.公司電腦及週邊設備、套裝軟體之規劃、評估與控制。

5.2.5.2.電腦及週邊設備、套裝軟體使用之管理、調度及維護。

5.2.5.3.機房空調、電力、不斷電系統(UPS)及消防設備之規劃與管理。

5.2.5.4.電腦網路與通訊系統之規劃、管理。

5.2.6.電腦作業管理

5.2.6.1.機房門禁、作業系統及檔案管理。

5.2.6.2.機房電腦主機及各週邊設備運轉之管理。

5.2.6.3.資料輸出／輸入設備使用管制作業。

5.3.職務代理

資訊單位應根據職責劃分原則及系統安全控管精神制訂職務代理制度，其規範原則請詳「職務代理人制度」作業說明。

5.4.與使用單位之職責劃分

5.4.1.各使用單位得視本身現行與未來作業情況，提出作業需求。資訊單位則參酌電腦軟硬體發展情況與相關部門會商決定開發之優先順序後辦理。

5.4.2.使用單位自行登錄及處理資料者，除因業務需要並經使用單位同意及授權，資訊單位不得擅自變更其資料。

5.4.3.使用單位若有機器移動應依規定辦理，並知會資訊單位簽核，由資訊單位指派人員陪同使用人員方可移動。

6.相關程序

6.1.「職務代理人制度」

7.相關辦法

無。

8.使用表報

無。

BRT-EP-02 系統開發及程式修改作業

1.目的

明訂應用系統(程式)或軟體之購置、開發及修改程序，以確保電腦化作業之軟體符合企業及使用單位需求。

2.範圍

本作業程序適用於應用系統(程式)或軟體之購置、開發及修改程序之申請、審核與驗收作業。

3.權責單位

3.1.資訊單位：依照使用單位之需求執行應用系統(程式)或軟體之分析、修改、設計、購置、開發等作業。

3.2.使用單位：使用需求之提出及驗收。

4.控制重點

4.1.系統軟體、應用系統（程式）或軟體之委外開發、購置，應依規定之作業程序辦理，並考慮使用單位之需求。

4.2.評估紀錄等書面文件應經適當簽核。

4.3.開發或購置之系統軟體、應用系統（程式）或軟體之申請需求，應與實際開發或購置之系統相符。

4.4.系統之外購應經核准，並簽訂合約。

4.4.相關單位與資訊單位應就書面設計與實際設計作最後比對。

4.5.系統測試及修改應設立獨立之環境。

4.6.程式變更修改應確實經核准後辦理。

4.7.系統修改後，須會使用單位測試其可行性。

5.程序內容

5.1.申請單位因實際作業而有系統開發或程式修改需求時，填寫【電腦作業需求單】，檢附相關資料，依權限呈核後，送交資訊單位審核，倘決議自行開發 / 修改者，則依 5.2. 程序執行。倘決議委外開發 / 修改者，則依 5.3.程序辦理。

5.2.系統自行開發或程式修改

5.2.1.可行性分析作業

系統開發人員應與相關人員討論作業現況、系統之需求及收集相關資料。後將分析、規劃結果，可行性方案彙總填入【電腦作業需求單】，視需求可列附件，依權限送呈簽核。

5.2.2.系統規劃分析之作業程序

系統開發人員依據所收集的資料進行析規劃，進而確立系統之規劃藍圖、功能細節、操作流程及作業範圍，並據此撰寫系統規劃。過程應會同使用單位或相關單位進行確認。

5.2.3.程式設計作業程序

系統開發人員依系統規劃之內容進行程式設計、撰寫及佈署。

5.2.4.系統測試之作業程序

系統開發人員完成個別程式模組之撰寫、編譯、佈署後應就個別程式模組進行測試工作，測試資料應小心選擇，保護及管制，並確認程式是否運作正常或符合需要。重要之資料庫應分為測試區及正式區，所有測試工作應於測試區完成後，方可導入正式區使用。

5.2.5.系統建置(轉換)及程式修改上線之作業程序

5.2.5.1.系統開發人員會同使用單位及相關單位之主管或關鍵用戶做最終確認。

5.2.5.2.系統開發人員撰寫操作手冊或技術手冊等設定文件及培訓資料。

5.2.5.3.系統開發人員會同使用單位及相關單位進行培訓，並約定上線時間，測試可行後，使用單位應回復驗收情況。

5.2.5.4.上線應由權責人員執行且于上線前確認已備有權責主管覆核之【電腦作業需求單】。

5.2.5.5.系統開發人員於計畫時間切換系統，並將【電腦作業需求單】、系統規劃等其他相關文件按「編製系統文書之控制」作業辦理結案歸檔。

5.3.系統軟體、應用系統（程式）或軟體之委外開發購置

5.3.1.本公司之整合性管理資訊系統采外購軟體者，由資訊單位依據公司需求，經與廠商議價，權責主管核可後購置，並與原開發公司簽訂長期維護合約，合約內容應注意保固期限、維護服務、教育訓練、系統檔及操作方式範圍等規範，並考慮機密性、可用性、完整性之適用性；委外開發時亦同。

5.3.2.外購軟件或開發之測試、文件準備、用戶培訓、上線等工作比照 5.2.5 自行開發程式之作業程序辦理。

5.4.系統軟體、應用系統（程式）或軟體委外改版更新(upgrade)或修改

5.4.1.使用單位因業務需要、或供應廠商定期更新版本、或資訊單位整體規劃需求時，應辦理系統軟體、應用系統（程式）或軟體之版本更新或修改。

5.4.2.資訊單位應與原供應廠商（如合約廠商、原廠保證廠商）聯係，安排修改事宜，相關之合約、需求表或採購訂單應存檔備查。對於提供服務之委外廠商，應于服務合約中適當列明其系統安全政策及權責歸屬問題，並考慮企業本身之安全需求，擬定測試之機制，以瞭解委外廠商之政策遵循及其安全控管之適當性。

5.4.3.實際發生費用時，除按相关付款规定辦理請款外，應加附 5.4.2.之相關附件。

5.4.4.更新或修改之測試、教育訓練及驗收應比照 5.2.5.項辦理之。

5.4.5.新設或修改系統，應於使用前提交使用部門進行模擬測試，經充分討論及驗證後，始可取代舊系統。

5.4.6.相關操作手冊、技術手冊及設定文件、培訓資料等，應按「編製系統文書之控制」作業辦理。

6.相關程序

6.1.「編製系統文書之控制」

7.相關辦法

無。

8.使用表報

8.1.【電腦作業需求單】

BRT-EP-03 編製系統文書之控制

1.目的

為利於電腦系統文書資料之管理，特訂定本作業程序。

2.範圍

本作業程序適用於電腦系統文書編製及保管之控制。

3.權責單位

3.1.資訊單位：電腦系統文書資料之管理。

4.控制重點

4.1.資訊單位所有之電腦文書及檔案文件應編號列冊，並設專人保管。

4.2.資訊單位於新系統開發及進行修改作業時，其相關之電腦文書應同時予以更新。

5.程序內容

5.1.電腦系統文書編製

5.1.1.資訊單位於完成系統測試程序及驗收程序後(含新購、版本更新及修改)，將【電腦作業需求單】及操作手冊編號存查列管。

5.2.文書資料保管

5.2.1.資訊單位應將各項系統分析、開發及設計文件按序分類歸檔，對於具機密性資料、文件應特別裝櫃加鎖以避免資料的外洩。

5.2.2.當作業人員因公借閱系統文件紙本原件時，應登記有關事項於【檔案資料借閱簿】後方得借用，並依照規定還件日期歸還，資料保管人員應定期催討逾期未還者。

5.2.3.如借閱之文件屬於機密或敏感性文件，須經權責主管核准後方可借閱。

6.相關程序

無。

7.相關辦法

無。

8.使用表報

8.1.【電腦作業需求單】

8.2.【檔案資料借閱簿】

BRT-EP-04 程式及資料之存取控制

1.目的

為建立本公司各使用者對系統程式及資料存取之權限及範圍，特製定本作業程序。

2.範圍

本作業程序適用於網路及個人電腦，其程式及資料之存取控制。

3.權責單位

3.1.資訊單位：對各使用者之需求權限進行設定。

3.2.使用單位：提出使用權限新增與異動之需求。

4.控制重點

4.1.程式檔案的存取使用應依個人權限加以管制。

4.2.重要之系統公用程式、工具及指令應依其使用者權限限制其存取權限。

4.3.一般應用系統之使用者除執行應用系統外，應無存取系統公用程式、工具及指令之權限。

4.4.程式檔案的存取使用均應留下可追蹤的紀錄。

4.5.權責主管應定期覆核相關紀錄。

4.6.程式及檔案應依業務應用及稽核使用加以區分。

4.7.密碼不可顯示於電腦螢幕上，亦不可未經亂碼化即列印於任何報表。

5.程序內容

5.1.網路系統內之存取控制作業

5.1.1.各使用單位主管於建置新的應用管理系統、有新進人員或使用權限異動時，應依其所轄職員之業務權限，填寫【電腦權限申請單】並呈核後，交資訊單位人員設

定使用者權限。

5.1.2 資訊單位依【電腦權限申請單】創建、賦予、異動或刪除帳戶權限時應注意申請權限之部會權責，有疑義得會同相關單位諮詢。

5.1.3.新進人員使用系統時應先按 5.1.1.申請取得新帳戶密碼方可使用，帳戶應具有可識別性，並禁止使用共同帳戶。

5.1.4.電腦系統使用單位操作人員因故離職時，離職人員應將【移交清冊】交資訊管理單位刪除使用者權限。

5.1.5.員工離職，其使用代碼應立即註銷或更新。

5.1.6.對於軟硬體廠商維護時使用之使用者代號應限制其存取權限，且不得重複使用。

5.1.7.使用預設密碼登入系統時，應要求使用者於登入後立即變更密碼。

5.1.8.帳戶密碼于身分驗證時，相關資訊不以明文顯示與傳輸，且系統應具備帳戶鎖定機制。

5.1.9.系統密碼應有設定原則，如最低密碼複雜度。

5.1.10.權責主管應定期審核帳戶與權限之建立、修改、啟用、禁用及刪除之狀況。

5.2.使用個人電腦之存取控制

5.2.1.個人電腦之使用應依崗位需求向資訊單位提出，視情況依『固定資產-調撥作業』或『固定資產-請採購作業』取得個人電腦，並依 5.1.1 申請個人電腦帳戶權限後方得使用。

5.2.2.使用者所使用之磁片或軟體必須經資訊單位核可認定後，方可於公司電腦上使用或安裝，以防止電腦病毒入侵，破壞存檔之資料。

5.3.權限控制

5.3.1.資料使用權限應有分層授權系統，稽核及管理人員無權限更新資料庫。應用系統、

作業系統及資料庫之最高權限管理帳號，由資訊單位最高主管管理，並應定期變更密碼。

5.3.2.負責系統或程式上線人員應於執行上線程序時，依系統安全及使用者職權之所需設定程式及資料檔案之存取權限。

5.3.3.設定系統程式對有權接取某特定檔案的程式限制其接取權利。

5.3.4 原則上公司內網不開放外部電腦接入，如有作業需求者，應填寫【電腦權限申單】，經權責主管核准後，交資訊單位設定權限。

5.3.5.資訊單位應不定期檢視遠端連線狀況，避免有非授權人員接入之情況。

6.相關程序

無。

7.相關辦法

無。

8.使用表報

8.1.【電腦權限申請單】

8.2.【移交清冊】

BRT-EP-05 資料輸出入之控制

1.目的

確保資料之輸出與輸入均經適當控制。

2.範圍

本作業程序適用於資料輸出，輸入及錯誤更正。

3.權責單位

3.1 資訊單位：資料輸出入使用權限之設定及應用程式錯誤之修改。

3.2 使用單位：外部資料之輸入與核對輸出報告之正確性。

4.控制重點

4.1.輸入作業

4.1.1.若系統支援，應啟用稽核紀錄管理，保留特定事件(如：特權帳號所執行之各項活動)之稽核紀錄。

4.1.2.程式內對輸入資料的正確性應有自動核對功能。

4.1.3 錯誤資料更正，是否依既定程序辦理及保留相關軌跡。

4.1.4 適時審查使用者活動、異常或錯誤之紀錄，並適時採取適當行動。

4.2.輸出作業

4.2.1.機密性或敏感性資料之輸出應適當管制。

4.2.2.輸出產生時，應留下記錄以供追蹤查核。

4.2.3.報表輸出後應立即分送有關單位。

4.2.4.輸出資料使用後，若無保存需要，應經適當的毀棄處理。

4.2.5.輸出資料若以磁性媒體保存，應定期檢查，以確定在必要時能以報表方式列出。

5.程序內容

5.1.資料輸入控制

5.1.1.使用單位應依照系統所需之輸入資料，輸入異動單據。

5.1.2.各項輸入異動單據必須要有配合系統規格的單據號碼。

5.1.3.使用單位之主管應就其具有影響性之系統操作功能提出使用者權限規範，並確保具有關鍵性之操作能由訓練合格之成員完成，及負責系統運作之結果。

5.1.4.對錯誤資料之發生原因應進行分析，以期改善。

5.1.5.資料輸入人員於收到原始憑證、單據時，應先審核資料內容業經權責主管簽核且無異常情形者，方得據以登錄。

5.1.6.資料登錄完畢後，應即對原始憑証做適當的記號以防止重覆輸入，並依規定分類存檔。原始憑證應依照規定年限妥善保存。

5.1.7.整批資料輸入處理時應採下列方式控制：

5.1.7.1.各批次資料予以識別號碼。

5.1.7.2.各批次資料數量予以適當限制。

5.1.7.3.總和控制。

5.1.7.4.批次資料的傳送登記。

5.1.8.輸入處理時，應採下列方式控制：

5.1.8.1.輸入錯誤時，螢幕顯示錯誤訊息，提醒使用者更正。

5.1.8.2.系統應依據資料的合理性、存在性及完整性等進行細部檢查。

5.1.9.介面系統輸入處理時，系統自動調節及結轉至系統結轉資料檔內。

5.1.10.標準參數及重要主檔資料之輸入及更正應經適當授權，並依其職權嚴格限制其存取權限。

5.1.11.應於程式設計時，加入適當之限制或自動檢查輸入之原始資料，以防止人員輸入錯誤，及早發現問題。

5.1.12.所有 IT 人員非經授權，不得直接由後台修改數據。

5.2.資料輸出控制

5.2.1.輸出資料於產生時應注意：

5.2.1.1.依不同單位及人員之需求，供已授權之單位或人員使用。

5.2.1.2.若有輸出錯誤且無需存檔之報表應予以銷毀。

5.2.1.3.有機密性或敏感性資料之輸出應設定適當控制。

5.2.2.重要或敏感性之報表列印應有適當之權限設定，輸出資料應先確認處理項目、單位無誤後再行分送，若分送資料為報表或媒體時，應經主管核准後，方可分送有關單位。

5.2.3.收受單位應於收受報表時，與留存之原始憑證或相關資料核對，資料有誤時應會同相關人員查明錯誤原因，並經權責主管同意後方得修正。

5.2.4.若透過媒體或線路傳送資料時，收受單位應列印或查詢確認資料的正確性，有誤時應再傳送或送交正確之媒體。

5.2.5.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。

5.3.錯誤更正之控制

5.3.1.因輸入錯誤，導致報表與其他報表勾稽不平時，經辦人員應經主管核准後，輸入正確之資料，並附於原始憑證之後備查。

5.3.2.因應用程式錯誤而造成報表錯誤，使用單位需填寫【電腦作業需求單】送交資訊單位申請修改，其後續作業比照「系統開發及程式修改作業」辦理。

5.3.3.若機器故障時，操作人員應通知資訊單位人員通知維修廠商修復。

5.4.軟、硬體設備報廢

5.4.1.有關電腦及磁性儲存媒體之報廢，為避免個資外洩，使用單位應會資訊單位進行報廢媒體之勘驗。

5.4.2.使用單位應先自行清空電腦硬碟資料，並將該電腦硬體含硬碟送交資訊單位進行實際勘驗。

5.4.3 資訊單位於勘驗後，應將機密性、敏感性資料及授權軟體確實予以移除，實施安全覆寫或實體破壞，並確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，通知使用單位取回可報廢的硬碟，以完成最終之財產報廢程序。

5.4.4 若欲報廢的電腦設備為筆電者，則由使用單位逕行將整台筆電送交資訊單位進行前述作業。

6.相關程序

6.1.「系統開發及程式修改作業」

7.相關辦法

無。

8.使用表報

8.1.【電腦作業需求單】

BRT-EP-06 資料處理之控制

1.目的

建立軟、硬體於資料處理時之控制程序，以確保資料處理之正確性。

2.範圍

本作業程序適用於硬體及系統軟體於資料處理之控制程序。有關資料處理之輸出 / 入控制依資料輸出入之控制作業辦理。

3.權責單位

3.1 資訊單位：對於系統開機與系統執行及軟、硬體之資料處理進行控制及系統軟、硬體異常狀況排除。

3.2 使用單位：提出系統使用需求及通報系統軟、硬體異常狀況。

4.控制重點

4.1.系統運作發生異常時應即修護、排除。

4.2.系統異常之修護、排除過程序應予記錄。

4.3.程式中應設定適當之控制功能，確保資料處理的正確性。

4.4.系統應自動檢核或產生重要資料之序號。

4.5.制訂適當控制處理程序以達到下列目的：

4.5.1.確定所有為系統接受之交易係經系統適當處理。

4.5.2.確定系統內部自動產生之交易係經系統適當處理。

4.5.3.確定交易業已記錄於適當之會計期間。

5.程序內容

5.1.硬體於處理資料之控制

5.1.1.相關之硬體設備應定期檢查，並將檢查情形予以記錄。

5.1.2.硬體設備如有異常現象發生，應根據各項設備使用手冊之指示設法排除或是即刻通知廠商前來維修，並作成維修紀錄。

5.2.系統開機

5.2.1.各作業權責單位依據規定啟動各項電腦系統並記錄異常狀況。

5.2.2.電腦主機設備如發現不正常情形，應根據各項設備使用手冊之指示設法排除或是即刻通知廠商前來維修，並作成維修紀錄。

5.3.系統執行

5.3.1.營業時間內相關作業人員應隨時掌握各項可能突發之異常現象，以便採取因應之對策。

5.3.2.硬體設備如有異常現象發生，應根據各項設備操作手冊之指示設法排除或是即刻通知廠商前來維修。

5.4.系統軟體於處理資料之控制

5.4.1.一般系統軟體係指作業系統及公用程式，通常由廠商提供，若需修改或更版系統軟體時，應比照「系統開發及修改作業」辦理。

5.4.2.不同使用者應有不同的使用權限控制，其使用權限設定比照「程式及資料存取控制」作業辦理。

5.5.應用軟體於處理資料之控制

5.5.1.對於資料之處理，應於系統作業中，利用程式設定防錯機制。其使用等級或權限之設定比照「程式及資料存取控制」作業辦理。

5.5.2.為確保處理資料的一致性，若有兩個以上應用作業系統同時更新檔案資料時，程式中應判斷一次只能由一應用系統更改該筆資料，另一應用系統須等該檔案已更

改完後方能變更該筆資料內容。

5.5.3.處理控制應與輸入控制相互配合，於程式控制中應有適當之檢查方式，如：

5.5.3.1.由某一程式處理資料將結果傳給另一程式時，應有處理總數之控制以確保資料無遺漏。

5.5.3.2.合理化之檢查：如極限值、範圍的控制，檢查號碼、字型型態檢查、借貸平衡檢查、四捨五入的原則等勾稽方式，以強化資料正確性。

5.5.4.於執行應用軟體處理資料時，若有錯誤發生，應研判是資料或程式錯誤，若是資料錯誤應依錯誤更正程序辦理；若程式錯誤應依程式修改作業程序處理。

5.5.5.系統因故中斷，使用單位應立即通知資訊單位協助處理，檢查當筆資料應存在、應可進行還原或必須重新輸入。

6.相關程序

6.1.「系統開發及修改作業」

6.2.「程式及資料存取控制」

7.相關辦法

無。

8.使用表報

無。

BRT-EP-07 檔案及設備之安全控制

1.目的

為維護資料檔案及各項電腦設備之安全，特製定本作業。

2.範圍

本作業適用於資料檔案之拷貝、控管及電腦設備、機房之維護、安全控制。

3.權責單位

3.1.資訊單位：依資料檔案、電腦設備及電腦機房之安全進行控制。

3.2.使用單位：配合資訊單位訂立之使用規則進行檔案之存取。

4.控制重點

4.1.檔案安全管理

4.1.1.系統應定期做備份，並留存书面记录。

4.1.2.備份資料應指定專人保管。

4.2.設備安全管理

4.2.1.消防設備應定期檢查維護。

4.2.2.系統發生異常狀況時，應加以瞭解原因、改進及記錄。

4.2.3.各項支援防護設備應定期檢查、換新。

4.2.4.使用者對其使用或保管之各項電腦設備及週邊設備須不定期檢查，如有問題時，應通知資訊單位維修。

4.3.機房人員進出應確實管制。

4.4.應定期更新偵測病毒軟體之版本，並訓練所有人員使用偵測病毒軟體偵測外來磁片之病毒。

5.程序內容

5.1.資料檔案之安全控制

5.1.1.資訊單位之統籌控制

5.1.1.1.至少每週備份一次資料，存放之媒體可為網路硬碟、NAS、磁片等。

5.1.1.2.將平日取用之媒體分別各備兩份，分存於不同之地點(不同之廠區)。

5.1.1.3.歷史檔案之媒體依不同檔案性質(系統程式、應用程式、資料檔)定期備份一份存放於其他地點(不同之廠區)。

5.1.2.使用單位對檔案之控制

5.1.2.1.為防止公司電腦資訊遭電腦病毒侵入，資訊單位應依職權設定軟體安裝權限。

5.1.2.2.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。

5.1.2.3.備份儲存媒體除資訊單位外不得調借其他單位。

5.1.2.4.為確保資料完整性，資訊單位當設定控制程式，禁止非經核准之檔案存取。

5.1.3.為避免檔案資料遭病毒毀損，資訊單位應不定期自動偵測病毒。

5.2.電腦設備之安全控制

為確保系統運作順暢、安全，資訊單位應對各項電腦設備詳加規劃與管理，茲將電腦設備分成電腦機器、通訊、支援、電源設備四種，其使用之安全控制管理分述如下：

5.2.1.電腦機器管理：包含電腦主機、終端機、印表機、磁帶(碟)機。

5.2.1.1 凡機器設備於購入時，資訊單位應會同使用單位驗收，並由財務單位辦理建檔編號。

5.2.1.2.超過保存年限者應列單報廢，以避免留存不必要之設備。

5.2.2.通訊設備管理

5.2.2.1.通信網路應保持機密性，防止資料被他人截取。

5.2.2.2.若設備線路發生故障時，應立即檢查，以了解線路故障原因，通知廠商或電信公司進行維修。若有重要性資料需立即處理時，應報請主管同意改以人工作業代替之。

5.2.2.3.設備應適當防護，未經授權人員不得接近，且附近不可放置易燃或危險物品。

5.2.3.支援設備管理

5.2.3.1.備有火警設備，以警示有火災訊息。

5.2.3.2.於明顯及重要地點設置滅火器，以便火災時滅火用。

5.2.3.3.滅火器應定期更換，並有專人負責消防系統之定期檢查與維修。

5.2.4.電源設備管理

5.2.4.1.重要設備應裝設有不斷電設備(UPS)及電源供應器以防止較長時間的停電。

5.2.4.2.應安裝自動電壓穩定裝置。

5.2.4.3.使用的電源要具有電磁式開關及地線接地，以保護電腦設備。

5.3.電腦機房之管制

5.3.1.機房內應設置獨立之空調設備以維持機房溫度之適當性。

5.3.2.人員進出管制

資訊單位人員應禁止非作業人員進出電腦機房洽公，電腦機房應設置門禁管制，由資訊人員陪同並登錄【機房進出記錄簿】才可進入。

5.3.3.操作管理

5.3.3.1.操作機器發生異常時應留下異常記錄。

5.3.3.2.機房中所有機器設備操作人員應依操作手冊規定啟動及操作。

5.3.3.3.系統之控制台所留下之記錄需加以保留並定期由主管檢驗。

5.3.4.禁止事項

5.3.4.1.非操作人員未經允許，不得攜帶物品進出機房。

5.3.4.2.非操作人員不得使用電腦機房，若因緊急狀況需使用機房設備時，應經權責主管同意。

5.3.4.3.機房內除機台設備及其他必需品外禁止放置可燃物，或散置垃圾及私人物品。

5.3.4.4.機房內禁止吸煙及進用食物飲料。

6.相關程序

6.1.「程式及資料存取控制」

7.相關辦法

無。

8.使用表報

8.1.【機房進出記錄簿】

BRT-EP-08 硬體及系統軟體之購置、使用及維護控制

1.目的

為使硬體及系統軟體之購置、使用及維護處理有所遵循，特制定本作業。

2.範圍

本作業適用於電腦硬體及系統軟體之購置、使用及維護控制。

3.權責單位

3.1.資訊單位：電腦硬體及系統軟體之購置、使用及維護等相關控制。

3.2.使用單位：對電腦軟、硬體之購置及資訊設備之維修提出需求。

4.控制重點

4.1.電腦軟硬體購置、更新應經過管理階層之書面核准，確保公司新購之軟、硬體設備規格符合公司發展方向需求，另相關之系統設定文件應適當存檔與保管。

4.2.電腦軟硬體之使用須設定密碼控制，並依操作手冊執行。

4.3.電腦軟硬體當定期維護並記錄。

5.程序內容

5.1.電腦硬體及系統軟體之購置

使用單位依業務需求，欲購置電腦硬體及系統軟體時，須會同資訊單位辦理。

5.2.電腦硬體及系統軟體之使用

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

5.2.2.資訊單位對於電腦硬體及系統軟體之維護應依照系統手冊辦理。

5.2.3.資訊單位應依程式及資料之存取控制之密碼控制作業，規範各部門使用軟體之使用權限。

5.2.4.操作控制

5.2.4.1.應於系統設定使用者於連線後一定時間內未用電腦時，電腦自動離線；倘系統無法做此設定，使用者應自行於 PC 內設螢幕保護程式，進入時需再輸入密碼才可進入；個人電腦不使用時需關機。

5.2.4.2.禁止擅自利用資訊單位系統設備處理與本身業務無關的作業。

5.2.4.3.非辦公時間或假日要使用主機，應將使用目的及使用時間事先經權責主管核准。

5.2.4.4.工作人員按「開關機程序」開機或關機。

5.3.硬體設備及軟體維護

5.3.1.資訊單位對於硬體設備應定期維護保養，並記錄於【設備檢查表】。

5.3.2.公司所有之硬體設備，其型號應列冊記錄，以利維護作業。

5.3.3.使用者對其使用或保管之各項電腦設備及週邊設備須不定期檢查，如有問題時，應通知資訊單位維修。

5.3.4.各單位欲申請系統設備維修時，應通知資訊單位進行處理，若須外修應通知廠商維修，修畢驗收無誤後請申請人簽名並依規定辦理請款。

5.3.5.若通訊設備線路發生故障時，資訊單位應派員立即檢查，以了解線路故障原因進行維修。若有重要性資料需立即處理時，應報請主管同意改以人工作業代替之。

5.3.6.外購電腦軟體之修改程序比照系統開發及程式修改作業辦理。

6.相關程序

無。

7.相關辦法

無。

8.使用表報

8.1.【設備檢查表】

BRT-EP-09 系統復原計畫制度及測試程序之控制

1.目的

確保企業資訊系統遭受不可抗力之災害或其它人員破壞時，能在最短時間內復原至正常企業營運。

2.範圍

本作業程序適用於資訊系統復原計畫制度及測試程序之建立、實施與控制等作業。

3.權責單位

3.1.資訊單位：建立及測試資訊系統復原計劃，並予以適當維護。

3.2.使用單位：配合資訊單位完成測試資訊系統復原計劃。

4.控制重點

4.1.制定系統復原辦法並定期修訂，檢討內容之完整性與可行性，尤其是人員變動、資源變動等等。

4.2.是否定期確認系統復原所需資源之可用性，包含備援協定之約期、備份資料及系統軟體之回復性、備援設備及地點之可用性等等。

4.3.電腦系統及其設計，是否加入適當之預防措施，減低不當破壞之機率。

4.4.系統資料回復後，是否適當測試並比對。

4.5.備份資料應定期執行復原測試，以確保與財務報導有關之重要系統備份資料可用性。

5.程序內容

5.1.資訊單位於日常作業應依檔案及設備安全控制之規定進行檔案備份。

5.2.使用單位因系統遭受不可抗力之災害事故、或檔案被破壞、或機器故障致資料受損時，應立即呈報部門主管，並通知資訊單位處理。

5.3.資訊單位於事故發生時應參照相關系統復原辦法及測試程序作業，予以呈報管理階層，並分析檔案及資料受損情況，及其對企業營運之影響，按其重要性排定應用系統復原順序及規劃應執行之資料復原程序與資料處理範圍。

5.4.資訊單位處理情形與方式應及時提出書面報告，經呈報簽核並知會相關單位後自行存檔。

5.5.資訊部門應就資訊系統之實體環境、作業程序及應用現況進行風險分析，並擬定書面之系統復原辦法。風險分析之要素，應包含：

5.5.1.了解資訊系統之弱點、威脅及其對企業營運活動之影響。

5.5.2.界定企業之重要資源、辨認各業務活動之重要性及等待復原最長可容忍時間。

5.5.3.選擇符合成本效益的復原策略。

5.5.4.建立分散風險之措施。

5.6.書面資訊系統復原辦法，至少包括：

5.6.1.災變預防準備工作

針對現有資訊系統之安全性，對企業正常營運活動之影響性等進行評估並建立保護及因應措施，包括實體安全、備援協定(reciprocal agreement)、資料備份、分儲等，必要時，亦應就重要資訊設備辦理保險。

5.6.2.系統故障或異常之緊急應變措施

5.6.2.1.明訂一般處理原則，含適當之緊急關機程序、修護申請、程序及替代之人工作業程序，確保將影響減至最低。

5.6.2.2 設定系統自動記載緊急修護代碼，並定期之日誌複核，確保系統有效、正確運作。

5.6.2.3 記錄系統故障或異常之排除、處理之書面記錄程序，據以分析、遏止重複

發生，及加速應變之處理。

5.6.3.災後復原工作

5.6.3.1.災後情況之假設及其基本對策。

5.6.3.2.災後復原階段之劃分、目標之設定與復原預計時間。

5.6.3.3.復原小組成員與職掌之劃分，並適當授權復原小組負責人，足以因應緊急處理。

5.6.3.4.宣告災變之程序及復原小組之動員方式。

5.6.3.5.明訂各階段復原工作之內容（包括資訊單位及各營業單位復原）及列示重要應用系統回復之優先順序。

5.6.3.6.復原工作資源之準備與分配，如日常備份資料之取回、系統軟體、應用系統（軟體）文件、備援協定之廠商、備援之電腦設備與作業程序及復原地點之安排等，加速復原工作之實施。

5.6.4.系統復原計劃之維護

5.6.4.1.配合實際資訊系統、軟／硬體更新及人員變動，定期檢討，保持計劃之可行性。

5.6.4.2.設立專卷記錄更新情形，並確保復原小組人員保有之系統復原辦法。

5.6.4.3.定期演練假設之災變狀況。

5.6.4.4.相關資訊系統復原計劃、書面辦法應保持其安全性，並於公司外之第三地置放一份。

5.6.5.系統復原計劃之測試

5.6.5.1.明訂測試之時機，如一定之測試週期或特定事件發生時，並據以設定測試目標。

5.6.5.2.測試應按電腦設備及系統文件實施，使用單位並應參與測試。

5.6.5.3.測試結果應做成書面記錄，遇有異常應即反應並修訂。

6.相關程序

無。

7.相關辦法

無。

8.使用表報

無。

BRT-EP-10 資通安全檢查之控制

1.目的

明確規範資訊單位對資訊通訊安全之檢查及控制原則，預防資訊資料之洩漏或破壞。

2.範圍

本作業程序適用於資訊通訊安全系統之建立、實施與控制等作業。

3.權責單位

3.1.資訊單位：負責安全之建立、實施、宣導與控制。

4.控制重點

4.1.資訊單位應經常性取得資通安全新知，即時建制新的控制。

4.2.資訊單位將資通安全風險宣導告知電腦使用單位。

4.3.各項電腦及週邊設備、系統應經申請並授權後方得使用。

5.程序內容

5.1. 資通安全軟硬體之建制

5.1.1.於 internet 及 intranet 之間，應建立防火牆、流量監控、行為監控等網路管理之軟硬體。並應設置用戶密碼授權，防止設定遭到竄改。

5.1.2.電子郵件系統應建置垃圾郵件過濾機制，防止威脅透過電子郵件入侵。

5.1.3.電腦或服務器應設置防火牆、防毒軟件，防止病毒入侵。

5.1.4.電腦或服務器使用之應用軟件應先經過資訊單位評估，不使用來歷不明之軟件，防止病毒夾帶其中。

5.1.5.電腦或服務器使用之應用軟件或作業系統，應不定期更新，以防止黑客透過系統漏洞入侵。

5.2.資通安全之宣導

5.2.1.資訊單位應不定期對資通安全議題進行宣導、文章發布或培訓。

5.2.2.資訊單位應透過管理手段對電腦使用者進行適當之安全性評估，即時發現危險行為。

5.3.資通安全之控制

5.3.1.資訊單位應擬定適當之檢查、規範或評估，以保證資通安全作業執行落實。

5.3.2 資訊單位應經常性關注新型態之資訊風險，即時佈置新式安全機制及安全宣導，保證資通安全不被新型態之威脅入侵。

6.相關程序

無

7.相關辦法

無。

8.使用表報

無。

BRT-EP-11 公開資訊申報作業

1.目的

為落實公司治理及資訊揭露公開制度，爰依相關規定，制定本管理作業。

2.範圍

本作業程序適用於公開資訊申報作業，包含財務報告書、股東會年報、公開說明書、財務預測、每月經營狀況、內部稽核及內控執行情形等資訊。

3.權責單位

3.1.財會單位：負責財務、股務...等申報業務。

3.2.稽核單位：負責稽核相關業務申報。

4.控制重點

4.1.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。

4.2.資訊公開前應經權責主管核准。

4.3.資訊公開應依法令規定，於申報期限內辦理。

4.4.資訊揭露後應確實歸檔。

5.程序內容

5.1.權責人員應依證券主管機關發佈公開發行公司應公告或向本會申報事項一覽表辦理本公司公開資訊申報相關作業。

5.2.對外公開之資訊，應由權責單位人員詳細檢查驗證後，依法令規定格式、方式於規定期限內公告或申報之。

5.3.資訊公開之行為（如電子檔傳送、報紙公告以及其他對外文件發送等）應經權責主管核准後， 始可由經授權人員執行。

5.4.資訊對外揭露後，權責人員應將相關資料以電子檔案或書面形式分類歸檔留存。

5.5.電子憑證申請及到期展延程序：權責單位須依台灣網路認證股份有限公司電子憑證之申請規定辦理電子憑證申請及到期展延。

5.6.電子憑證保管方式：本公司所申請之電子憑證金鑰交由權責單位保管。

5.7.公開資訊申報程序

5.7.1 資料傳輸 : 申報單位傳輸資料時應由權限主管指定之人員輸入資料，經權限主管覆核無誤後方可完成傳輸。

5.7.2 錯誤更正 : 本公司申報之公開資訊經查有錯誤時，申報單位應即時輸入正確資料予以更正，經權限主管覆核無誤後方可完成更正資料傳輸。

5.7.3 資料保存 : 公開資訊申報完成後，權責人員應將相關資料依法規之規定年限歸檔留存。

5.8.若因其他原因無法以網際網路連線方式申報者，經主管機關、證交所或櫃買中心同意可暫時採書面申報，但應於事後二日內將相關資料補行輸入。

6.相關程序

無。

7.相關辦法

7.1.內部人申報管理規則。

8.使用表報

無。