瑞磁生物科技集團股份有限公司

資通訊管理控制作業

Version	Date
5	2022.04

目錄

職稱	權責人員
資通訊管理部門主管	Jerry Kowalski
資訊工程師	Laurence Tung
資訊工程師	Justin Nguyan

系統	模組
Windows Server Backup	Datto Siris 4 Professional

報告名稱	系統
新增使用者權限申請表	
資產汰舊紀錄	
員工註銷權限表	
資產分派紀錄	

資通訊管理部門職務與責任

資通訊部門的主要職責是維護本公司的資通訊系統並保障資通訊系統的安全控管按照內部控制作業執行。

資通訊管理部門的責任包括:

- 設立與維護電腦運算工具以及其處理資訊的相關政策。
- 開發管理系統或專案，用以維護硬體運算工具與安全性管控，包括但不限於資通訊網絡的建置與維護。
- 管理使用者權限與帳號密碼。
- 排除硬體或軟體故障與其影響。
- 提供使用者必要的教育訓練與操作守則。

使用者的責任包括 (全職與非全職雇員):

- 遵循電腦運算工具及處理資訊的相關政策與程序。
- 提出系統升級或改善等需求以符合工作規定的操作需求。
- 提出系統使用權限的申請由資通訊部門與對應的管理部門進行審核以提供使用權限。
- 協助測試由第三方承攬單位提供的系統、專案或服務。

公司應設置安全性事件應變小組並清楚定義其成員的職務，小組成員應清楚明瞭他們的工作職責。當安全性事件發生時，應變小組要負責記錄在安全性事件報告中、建議應對措施、呈報安全性應變主管審核，並通報影響部門。

系統與專案開發的管理文件

所有系統開發或資通訊管理部門的執行變更或第三方承攬商的流程皆需要被妥善的紀錄與管理。相關的管理文件包括但不限於系統功能、安裝指引、專案變更文件、系統測試紀錄、使用者手冊的簽收紀錄等。所有相關的文件在變更時須遵循內部控制程序。

無論是第三方承攬商或公司自行開發的系統或專案產生的使用者手冊都需要提供給具權限的使用者，並被妥善管理。 其他的管理文件則由資通訊管理部門在專屬區域保管與維護。 文件管理的原則應具備清楚的標示與編碼，並具備文件總覽表，由專責人員保管與維護。文件的出借、出借原因、出借日期、歸還日期，以及對應的簽署，都應有完整的帳目管理。 過期的文件應經由權責人員審核放行後予以處分。

程式 數據庫 與作業系統的權限

程式、數據庫、與作業系統的權限都應該有密碼管理。 密碼的組成應具複雜構成(文字、數字與特殊符號)，並應每隔 90 天進行變更。 密碼的長度應至少 8 個字元。 同樣的密碼不得沿用，至四次變更後方得重複使用。 系統將會在 3 次登入失敗後自動鎖住該用戶的帳號。

所有程式、數據庫、與操作系統的新用戶申請都需要經過對應的管理層級審核與放行。 如果使用者需要新增權限，必須要提出申請表，經由對應使用者的主管與資通訊管理部門的審核與放行。

當雇員離職時，管理主管應按層級通報資通訊管理部門進行該用戶的終止、權限註銷、以及變更通訊錄與關聯程序指引。 資通訊管理部門將變更用戶密碼，或註銷權限，或將該用戶完全移除，或將該用戶鎖住，使離職雇員失去接觸程式、數據庫、或作業系統的能力。

對管制數據進行變更需要先予以紀錄，以及經由對應的權責管理人員進行審核與放行，方能執行變更。

程序、數據庫、與作業系統的操作權限需要有資通訊管理部門人員定期性的維護與審閱。

網絡使用權限

本公司使用適當的工具以管理網絡權限。並依照不同的資通訊服務內容、使用者、作業系統的特性將網域分散，以保護重要的系統與資料。

使用者被規定設置複雜的密碼(包括文字、數字、與特殊符號)，並每隔 90 天需重設。此重置密碼頻率規定並適用於本公司會計處理系統。 密碼的長度應至少 8 個字元。 同樣的密碼不得沿用，至四次變更後方得重複使用。

當新雇員到職時，其對應的管理單位通知資通訊部門。 資深資通訊專員將新使用者加入網絡，更新網絡用戶清冊並透過電子郵件提供其對應的網絡使用權限。 並提供初始的密碼，在初次登入後進行重設。 若使用者的網絡使用權限需要變更，其對應的管理單位提出權限(變更)申請表，資通訊部門遵循內部控制程序予以變更。

當雇員離職時，其對應的管理單位通知資通訊部門，資通訊部門終止該用戶並更新網絡用戶清冊。 資通訊部門並變更該用戶的密碼，使離職雇員失去使用網絡的能力。

若使用者需要使用虛擬私人用戶操作網絡，需要先取得其對應管理單位的同意，並由管理單位提出權限申請表。

軟體年限

多數的軟體都是賣斷的產品。 公司並不開發必須自主維護存續的軟體。 第三方承攬商在開發與建置軟體過程必須有公司全職雇員的審視。

當公司有軟硬體的維護需求並使用第三方承攬商的服務時，公司必須要審查，依照該服務的性質，包括但不限於其進程、完成期限、維護守則、請款流程、所有權、軟硬體需求、核准放行文件、懲罰性補償、安全防護措施等，以維護公司的權益。

涉及輸入變更，如非重大性變更(金額變動不超過 1,000 元)，同時輸入項目不更動數據庫內存資料，則該變更不需要提出變更申請表。 如變更屬重大性(金額變動等於或大於 1,000 元)，或輸入項目包括更動數據庫內存資料，則必須要提出變更申請表。

第三方承攬商設計並回報開發進度給該程序的負責人。 程序負責人指派使用者進行初版、進階版、與驗收測試，以完成開發工作。 使用者驗收測試要驗證數據的完整性與穩定性。 使用者在進行測試前要將測試方法進行文件化交由程序負責人審查，同樣將測試結果數據文件化交由程序負責人審查。程序負責人遵循內部控制程序審查結果與評估進度是否符合系統變更申請表上提出的上線日期。

在上線期限之前，資通訊管理部門需要管理並掌控軟體版本、備份先行版本、並妥善記錄，確保當更新版本不能滿足驗收需求時，仍能夠重置到先行版本。 敏感性程式與數據庫需要特別註記限制清單。

資訊備份與復原

本公司每日都進行資訊備份。 重要程式、關聯文件與原始碼，都應備份在原工作站以外的位置或在線上。取決於資料的敏感度，檔案可以採封包式或單一備份。 以下是對於備份的需求以及保存長度。

頻率	**保存長度**
每天	存放 7 天
每周	存放 4 周
每季度	無限期存放

當使用者需求一個檔案進行復原，使用者須向資通訊部門提出申請。 **如果資料存放的位置是屬於高敏感度區域，則申請者需要得到資通訊部門的審核通過方能從備份區中復原出檔案。**備份檔案都會先在暫存區內供使用者確認後，始得復原到適當的區域。

資通訊部門每半年都會測試一次復原功能，從上個月備份的檔案中隨機抽選復原到暫存區，以驗證備份和復原功能。

資通訊危機應變

1. 本公司應設定資通訊危機應變演練計畫，透過定義演練目的與各個人員的角色，以及具體應變時間目標，遵循公司的風險管理程序來進行演練。

2. 本公司應執行資通訊危機應變演練，由資通訊部門人員記錄實際應變時間，整合演練中的測試資料，提交給對應的管理者進行審核再保管紀錄。

會計紀錄

會計紀錄的輸入與輸出管理審查應在每次期末與出具財務報表時進行討論。

取得與處分資產

資通訊部門遵循公司的固定資產管理政策進行取得與處分，詳見取得與處分資產政策文件。

資通訊部門在處分任何的資通訊資產前應先將其硬碟進行備份並選擇一部新資產進行資訊轉移。

資通訊部門應完成整份安全性資訊處分流程，將硬碟進行格式化，移除作業系統，數據，以及任何具版權的程式軟體，再將該資訊載體進行物理性毀損 (例如，絞碎或破碎該應硬碟或儲存器)。

安全防護

本公司有定期性檢查表以保障硬體與軟體的可操作性並縮限其不可操作時間。 定期性檢查表由資深品保專員進行編寫與維護。

本公司安裝防毒軟體以掃描網絡與電腦上的檔案。 使用者不得自行變更預設的防毒軟體掃描與升級排程。

本公司的資產與資訊使用須知已揭露在員工手冊之中。 新到任雇員同意查閱與理解本公司的政策。任何的政策變更採取包括但不限於電子郵件通知和員工管理教育訓練通知。

在 30 分鐘內如果登入失敗 3 次，系統將會把該使用者進行封鎖。 使用者需要聯絡資通訊部門並獲得臨時登入密碼以取得網絡權限。 資通訊部門將會調查登入失敗的原因，如有需要，也將記錄登錄失敗，並呈報給對應的管理層級。

所有的資通訊硬體都需要存放在具有安全管制的空間內。無權限的訪客進入該管制空間需要被記錄並有管理權限的人陪同。 資通訊部門需每季測試工作站與不斷電系統的電源，並清理散熱風口。

本公司不具有網上銷售，或其他有大量訪客登入風險的商業模式，故不執行網絡耐受性風險測試。

資訊流向安全性檢查

重要的軟體與數據應經過加密，並且登入密碼應常態性進行變更。

資訊安全應定期由資通訊部門檢視，年度檢查確保不使用來路不明的軟體，違法複製或非法無效化任何數據。

公司官網上揭露的資訊應當由對應的人員定期檢視並立即移除任何非屬大眾需知的敏感性與保密性資訊。全體雇員應避免提交、接收、下載與職務不相關的電子郵件或程式，同時應避免公司的網路資源遭職務以外的使用佔據，並避免電腦脆弱性問題遭攻擊。

遵循金管會指引的資訊揭露與申報

資通訊部門應設置與維護設備、系統與網連結能力，確保能按台灣金管會指引揭露與申報資訊。

網絡上的申報系統、使用者權限、帳戶與密碼應由管理階層謹慎的處置，並只交付給可信賴的人員進行操作和資訊上傳。 當第一次登入時，密碼應進行變更並重設為高複雜度，並定期進行變更。 增加的使用者權限、帳戶、密碼應由被賦予權限的人在管制的區域內保管。

公司應遵循相關法令法規發布公告或重大訊息，並在規定的期限內完成發布。

任何要上傳的資料應先經過對應的各級核決權限主管審查其內容完整性與準確性後，方得上傳。