鈺緯科技開發股份有限公司

資訊安全規則

修訂記錄					
版次	生效日期	經辦	審核	核准	修正內容
A	2021/10/29	資訊專員	資訊課副理	行政長	新制訂
01	2023/04/24	資訊專員	資訊課副理	行政長	合併資訊安全管理辦法
02	2025/06/25	資訊專員	資訊課副理	行政長	1. 增訂修訂記錄 2. 施行辦法重編號為五,原為四同管理措拖

總則

一、目的

鈺緯科技開發股份有限公司(以下簡稱本司)為強化資訊安全管理，確保公司資訊之可用性及完整性，及避免公司資訊資產遭受內、外部蓄意或意外之威脅與破壞，以及防止本司之營業及業務機密等應行保密資訊外洩，爰訂定本規則。

二、適用對象及目標範圍

(一) 適用對象:

1. 本司之全體人員及與本司有業務往來之廠商及訪客人員等，均應遵守本規則。
2. 資訊安全之定義，係指維持本司資訊業務正常運作之硬體、軟體、文件、人員及資料等有關資訊安全之事項，除另有規定外，悉依本規則辦理。

(二) 目標範圍:

為保護本司資訊系統避免遭受不當的使用、竄改或破壞等情事及為確保本司應行保密資訊，本司資訊安全目標如下：

1. 保護本司資訊系統之機密性避免未經授權之存取。
2. 保護本司資訊系統之完整性避免未經授權之修改。
3. 保護本司資訊系統之可用性確保資訊及重要服務在人員需要

時可以取得服務。

4. 兼顧本司機密資訊保護及保障同仁個人隱私保障。

5. 確保本司各項資訊作業均符合相關法令要求。

三、資訊安全組織權責

為落實資訊安全，應成立資訊安全組織，負責推動、協調及督導下列資訊安全管理事項：

（一）資訊安全政策之核定及督導。

（二）資訊安全責任之分配及協調。

（三）資訊資產保護事項之監督。

（四）資訊安全事件之檢討及監督。

（五）其他資訊安全事項之核定。

（六）定期召開資訊安全會議。

四、管理措施：

（一）公司全體人員應接受資訊安全教育訓練，並定期進行資訊安全宣導事項以提升全體人員資訊安全水準。

（二）應建立資訊系統資產等級之分類以及相對應之管控層級作業。

（三）資訊系統應採行防範及保護措施以偵測及預防電腦之惡意軟體或行為之危害確保系統正常運作。

（四）針對資訊系統的新增、變更與移除與使用等作業建立相對管控

機制。

（五）為確保本司資訊安全應不定期檢測各電腦及網路之使用狀況。

（六）應以防火牆及其他安全設施管控與外界網路之連接以避免外部非授權之存取。

（七）為保護資訊系統資料處理的完整系統異動或變更應依變更程序執行。

（八）基於本司營業秘密及業務祕密以及資訊安全之維護，本司除不定期檢測各電腦外，本司對於本司提供之電腦設備(包括但不限於硬體設備、軟體等與電腦通訊設備相關)設有必要之控管、監察、查核、存取權限，惟為兼顧同仁個人隱私，資訊單位不得任意調取相關電磁紀錄，僅得於員工之電子郵件有異常流量、有未經授權之存取、修改、或經單位主管發現有疑似洩密等情狀，經資訊單位或該單位主管依循通報程序通報後，並經總經理書面同意，方得進行調取。

（九）資訊處理中心(即資訊機房)應建立門禁管控及環境週邊設備管理。

（十）資安事件發生時應依循本司通報程序進行通報。

五、施行辦法

（一）帳號管理

1. 資訊系統均需有帳號及密碼登入管理功能，依業務功能不同，區分帳號種類，每一種類每一同仁使用一組帳號及密碼。
2. 原則上同仁帳號採一人一帳號，但考量授權數成本限制及新型態系統服務差異(例如: SAP 系統及雲端服務軟體採授權使用，在不同時間下同帳號可以不同人員登入)，得申請共用帳號，且系統的共用帳號使用不得存在授權問題，須在同個部門下，不得跨部門使用(例如：使用單位(開發)開立請購單，核可單位(財會)核可的作業下，共用帳號不得跨二個單位)。
3. 使用者須妥善保管個人帳號、密碼，密碼需符合密碼規則如下。個人密碼應絕對保密，若發現外洩應即更改，以確保資訊安全。
    1）密碼最小長度: 至少 6~8 碼
    2）密碼複雜度: 至少英數混合
    3）密碼記憶歷程: 3~5 次以上
    4）最長使用天數: 90 天以內
    5）錯誤鎖定次數: 3 次以上
4. 同仁異動經權責主管核定後，應依其異動狀況調整、停用或

刪除其帳號及許可權。

5. 帳號使用人員有離職或職務異動時，原使用之帳號，在接收到職務異動單或離職單時應進行密碼變更(共用帳號)或停用(非共用帳號)，異動後系統需求則開立帳號權限申請單另行申請。

(二) 資料存取

1. 系統資料庫由資料庫管理者依使用者群組訂定不同使用權限，無權限者不得直接存取資料庫內容。
2. 系統應依資料之重要性設定安全機制，並應可追蹤資料流及使用者操作記錄。
3. 系統資料儲存異常時，應有自動警報或回復功能。
4. 資料依重要性區分，設定不同的保存或銷毀期限，除另有規定外，保存期限至少為二年以上。
5. 重要系統(例如: SAP ERP 系統)除資料備份外，同時需開啟稽核記錄功能，稽核記錄檔需保存期限至少為二年以上。
6. 使用單位經由系統所取得之機密性資料均應嚴加管制，限制傳閱、影印、複製、攝影、轉出或以其他方式記錄。
7. 系統存取及應用之監督，應建立及製作異常事件及資訊安全事項的稽核軌跡，並妥善保存，以作為日後調查及監督之

用，系統稽核軌跡應包括下列事項：

(1) 使用者識別碼。

(2) 登入及登出系統之日期及時間。

(3) 盡可能記錄端末機的識別資料或其位址。

（三）網路安全管理

1. 網路應安裝監控系統，監控通訊線路、通訊協定、資料流量、資料內容及使用物件，由資訊部門指定專人辦理。
2. 重要伺服器均應裝置於公司受到保護的網路內，內、外網路須安裝安全防護設備(防火牆)區隔，並依業務所需設定安全存取權限。
3. 防火牆安全權限之異動申請，經資訊部門核定後，由專責人員修改，並紀錄異動歷程。
4. 資訊部門應定期檢討防火牆安全權限及電腦網路安全事項，並應建立網路入侵偵測系統，以有效偵測惡意入侵事件。
5. 經由公眾網路傳輸機密資料時，應採取資料加密機制。
6. 防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。
7. 憑證安全管理：

(1) 資訊平台與外部連結時，須建置憑證金鑰。

(2) 憑證金鑰之產生、儲存、使用、備份、銷毀、更新及復

原作業等，應建立嚴格的安全管理機制。

（四）系統異動管理

1. 資訊系統程式、批次作業及環境參數異動(新增、修改、刪除)應透過「系統需求申請單」申請，並經相關單位授權執行。

2. 資訊系統異動上線應按資訊內控循環要求落實系統驗證測試作業，並於申請單中簽核確認，未確認之異動不得進行上線，避免因系統調整不完善造成資料異常。

（五）備份還原

1. 為確保資訊系統之資料完整與正確，應設有二層以上備份資料保護機制，確保災害發生時，能根據不同等級的損害進行資訊資料的重建工作。

(1) 本機資料備份：存放於運行中的主機上。

(2) 異地資料備份：存放於異地機房或雲端服務，備援地點不可與運作中的機房為同一棟大樓，且須具備運行系統服務的硬體設備。

2. 資訊部門應依業務及重要性設定系統完整之備份計劃，且須設定密碼後方能執行，並詳細記錄主機名稱、日期、起迄時間、內容、編號、狀態、保存位置及操作人員。

3. 備份軟體須確保備份資料的完整性及安全性。

4. 備份以雲端為主，其他媒體為輔，且與主機異地安全保存。

5. 重要資料備份記錄，應設定保存期限且至少保存一年以上。

6. 備份資料應依系統特性及重要性安排回復測試作業，並詳細記錄日期、內容及結果。

7. 資訊部門應定期(至少半年)演練備援作業程序，以便發生災害或儲存媒體失效時，可迅速回復正常作業。

（六）病毒防治

1. 公司所有伺服器主機、個人電腦、筆記型電腦均應安裝規定之防毒軟體，並設定排程定期掃毒以採取必要之措施；所有伺服器亦應按月執行掃毒作業，並將紀錄留存備查，以防制及偵測電腦病毒與惡意軟體等的侵入。

2. 使用防毒軟體，應依下列原則辦理：

(1) 定期或即時更新版本及病毒碼。

(2) 定期或即時掃描電腦系統及資料儲存媒體。

(3) 使用之防毒軟體由資訊部門審核後，方可使用。

(4) 對來路不明及內容不確定的資訊媒體，應在使用前詳加檢查是否感染電腦病毒。

(5) 定期將必要的資料及軟體予以備份。

3. 電腦設備如遭病毒感染，應立即離線(拔除網路線連結)處理，若無法處理應通知資訊人員協助，直至確認病毒已消除後，方可重新連線。

（七）個人資料保護

資訊系統之運作功能及資料存取應符合個人資料保護規範，依據「個人資料保護管理辦法」相關規定辦理。

（八）實體及環境安全管理

資訊機房之安全管理，依「機房管理辦法」相關規定辦理。

（九）資安遵守規範

1. 資訊部門應制定系統使用規範，並防止內、外非相關人員取得機密資訊或影響系統正常運作；同仁不得利用系統進行非正常或未經許可之作業，以獲取不當之資訊或利益。
2. 同仁應遵守公司資訊安全政策之相關規定，違者按情節輕重依「人事評議委員會規章」相關規定予以處分。
3. 同仁應遵守業務機密之相關法令規定，在職及離退職後均不得洩漏所知悉之資訊機密，或為不當之使用，違者按情節輕重依「人事評議委員會規章」相關規定予以處分，必要時並得追究相關法律責任。

六、附則：

（一）本規則每年至少評估一次以反映相關法令規範、資訊技術環境及資訊業務之最新狀況確保資訊安全及營業秘密保護之實務作業之有效性，本規則如評估後有修改，均應公告之。

（二）本規則未盡事宜悉依相關法令以及本司相關規定辦理。