資訊安全政策

一、目的

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司企業應用產品發展處之業務持續運作環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。確保本單位開發資訊之機密性、完整性與可用性。

機密性：確保被授權之人員才可使用資訊。
完整性：確保使用之資訊正確無誤、未遭竄改。
可用性：確保被授權之人員能取得所需資訊。

二、依據

1. ISO/IEC 27001：2022(ISO／IEC 27001：2022 Information security, cybersecurity and privacy protection - Information security managementsystems - Requirements)。
2. 個人資料保護法。
3. 著作權法。
4. 資通安全管理法。
5. 刑法 第三十六章 妨害電腦使用罪
6. 營業秘密法
7. 電子簽章法

三、適用範圍

1. 本企業應用產品發展處資訊安全管理制度（ISMS）所涵蓋範圍皆適用之。
2. 資訊安全管理涵蓋14項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本單位帶來各種可能之風險及危害。管理事項如下：
   - ► 資通安全政策之制定及評估
   - ► 資訊安全組織之職責與分工
   - ► 人力資源安全
   - ► 資訊資產管理
   - ► 存取控制
   - ► 密碼措施
   - ► 實體與環境安全
   - ► 作業安全
   - ► 通訊安全
   - ► 資訊系統獲取、開發及維護
   - ► 供應商關係
   - ► 資通安全事故管理
   - ► 營運持續管理之資訊安全層面
   - ► 遵循性。

四、資訊安全政策內容

維護研發過程資訊機密性、完整性與可用性,保障研發資料安全

4.1 資訊安全政策：

4.1.1 依營運要求及相關法律與法規,提供資訊安全之管理指導方針及支持。

4.1.2 資訊安全政策由管理階層定義並核准,且對內部及相關外部傳達。

4.1.3 資訊安全政策應定期或發生重大變更時審查,以確保合宜、適切及有效性。

4.2 資訊安全之組織：

4.2.1 建立管理框架,以於組織內啟動及控制資訊安全之實作及運作。

4.2.2 確保遠距工作及使用行動裝置之安全。

4.3 人力資源安全：

4.3.1 確保員工及承包者瞭解其將承擔之責任,並適任其角色。

4.3.2 確保員工及承包者認知並履行其資訊安全責任。

4.3.3 將保護組織利益納入聘用變更或終止聘用過程之一部分。

4.4 資產管理：

4.4.1 識別組織之資產並定義適切之保護責任。

4.4.2 確保所有資產依其對組織之重要性,受到適切等級的保護。

4.4.3 防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。

4.5 存取控制：

4.5.1 限制對資訊及資訊處理設施之存取。

4.5.2 確保授權使用者得以存取,並避免系統及服務的未授權存取。

4.5.3 令使用者對保全其鑑別資訊負責。

4.5.4 防止系統及應用遭未經授權存取。

4.6 密碼學：

4.6.1 針對資料機密性要求及風險評估結果,對須防護其機密性之資料本體進行加密作業或對其傳輸過程進行加密作業。

4.6.2 對於加密使用之金鑰,須對其取得、安裝、儲存、備份、回收及展延進行管理,以確保加密機制之完整及可用。

4.7 實體及環境安全：

4.7.1 防止組織資訊及資訊處理設施遭未經授權之實體存取、損害及干擾。

4.7.2 防止資產之遺失、損害、遭竊或破解,並防止組織運作中斷。

4.8 運作安全：

4.8.1 確保資訊處理設施之正確及安全操作。

4.8.2 確保資訊及資訊處理設施,以防範惡意軟體。

4.8.3 防範資料漏失。

4.8.4 紀錄事件即產生證據。

4.8.5 確保運作中系統之完整性。

4.8.6 防範對技術脆弱性之利用。

4.8.7 使稽核活動對運作中系統之衝擊降至最低。

4.9 通訊安全：

4.9.1 確保對網路及其支援之資訊處理設施中資訊之保護。

4.9.2 保護組織內及與任何外部個體所傳送資訊之安全。

4.10 系統獲取、開發及維護：

4.10.1 確保資訊安全係跨越整個生命週期之整體資訊系統的一部分。此亦包括經由公共網路提供服務之資訊系統的要求事項。

4.10.2 確保於資訊系統之開發生命週期內,設計及實作資訊安全。

4.10.3 確保測試用資料之保護。

4.11 供應者關係：

4.11.1 確保對供應商者可存取之組織資產的保護。

4.11.2 維持資訊安全及服務交付之議定等級與供應者協議一致。

4.12 資訊安全事故管理：

4.12.1 確保對資訊安全事故之管理的一致及有效作法,包括對安全事件及弱點之傳達。

4.13 營運持續管理之資訊安全層面：

4.13.1 資訊安全持續應嵌入組織之營運持續管理系統中。

4.13.2 確保資訊處理設施之可用性。

4.14 遵循性：

4.14.1 避免違反有關資訊安全相關之法律、法令、法規或契約義務,以及任何安全要求事項。

4.14.2 確保依組織的政策及程序,實作及運作資訊安全。

五、適用性聲明書

依據「ISO 27001 資訊安全管理系統-要求」要求產出「適用性聲明書」,以書面方式列舉資訊資產是否適用其標準所列之控制措施,及其不適用之原因。當組織架構、人員、設備、實體環境等變動時,ISMS 資安小組應重新定義控制措施之適用性。

六、實施

6.1資訊安全政策配合管理審查會議進行資訊安全政策審核。
6.2本政策經主任委員核定後實施,修訂時亦同。