資訊安全政策及管理

本公司資訊安全之權責單位為資訊室,負責訂定公司資訊安全政策,規劃資訊安全措施,並執行相關之資訊安全作業。基於資訊安全的重要性，權責單位每週定期向總經理報告執行情形。

一、資訊安全管理目標

1.維持各資訊系統持續運作

2.防止駭客、各種病毒入侵及破壞

3.防止人為意圖不當及不法使用

4.防止機敏資料外洩

5.避免人為疏失意外

6.維護實體環境安全

二、資訊安全設施與管理方式

1.電腦設備安全管理

(1)本公司電腦主機、各應用伺服器等設備均設置於專用機房，機房門禁採用感應刷卡進出，且保留進出紀錄存查。

(2)機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉；並放置藥劑式滅火器，可適用於一般或電器所引起的火災。

2.網路安全管理

(1)與外界網路連線的入口，配置企業級防火牆，阻擋駭客非法入侵。

(2)公司共有 2 個廠區，分別為本廠及生技一廠，網路皆由防火牆控管，避免資料傳輸過程遭受非法擷取。

(3)配置上網行為管理與過濾設備，控管網際網路的存取，可屏蔽訪問有害或政策不允許的網路位址與內容，強化網路安全並防止頻寬資源被不當占用。

3.病毒防護與管理

(1)伺服器與同仁終端電腦設備內均安裝有端點防護軟體，病毒碼採自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。

(2)電子郵件伺服器配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者端的 PC。

4. 系統存取控制。

(1)同仁對各應用系統的使用，透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊室建立系統帳號，並經各系統管理員依所申請的功能權限做授權方得存取。

(2)帳號的密碼設置，規定適當的強度、字數，並且必須文數字、特殊符號混雜，才能通過。

(3)同仁辦理離(休)職手續時，必須會辦資訊室，進行各系統帳號的刪除作業。

5. 確保系統的永續運作。

(1)系統備份：建置建置離線異地備援，採取週備份機制，電腦機房及生技一廠各存一份複本，複本於每週備份完後斷線，以確保系統與資料的安全。

(2)災害復原演練：各系統每年實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，再由使用單位書面確認回復資料的正確性，確保備份媒體的正確性與有效性。

(3)租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。

6. 資安宣導與教育訓練

(1)提醒宣導：要求同仁定期更換系統密碼，以維帳號安全。

(2)講座宣導：每年對內部同仁實施資訊安全相關的教育訓練課程。

三、114 年度執行情形

1.資訊室包含資訊安全主管 1 位及資訊安全人員 2 位。

2.投入建立基礎防護架構之經費，確保企業營運皆在安全範圍。

3.定期對內部同仁實施資訊安全相關的教育訓練課程，加強員工對於資訊安全風險之應變與警覺性。

4.異地備份每周 2 次。

5.每年進行資安稽核。