宇峻奧汀科技股份有限公司

資訊安全管理規範

1 目的：

為提昇本公司資訊管理安全性，確保資料、系統、設備及網路安全，及保障使用者權益訂定本規範。

2 適用範圍：

本公司全體同仁、業務相關之外部人員。

3 定義：

3.1 資訊安全

將安全保護措施實際應用於公司資訊環境，並使研發與辦公系統可正常運作。

3.2 資訊管理部人員

公司內部資訊管理單位。

3.3 外部人員

所有非公司編制內部同仁。

3.4 可攜式媒體

舉凡如隨身碟、抽取式硬碟與筆記型電腦，無線網路設備等可移動式設備之相關規範，統稱為可攜式媒體。

4 權責：

4.1 外部人員：

遵守公司資訊安全管理作業。

4.2 公司同仁；

- 遵守公司資訊安全管理作業。
- 外部人員可攜式媒體使用核可。

4.3 資訊管理部人員：

- 各項資訊安全狀況之掌握與排除。
- 資訊安全政策之執行。
- 各種資訊安全訊息的傳達與教育公司同仁。
- 公司同仁可攜式媒體使用核可。
- 資訊安全管理作業擬定。

4.4 處級主管以上：

所屬部門同仁可攜式媒體使用核可。

5 作業程序：

5.1 設備使用管理

- 未經資訊管理部允許，不得對主機進行拆裝的相關動作。
- 若有硬體故障或配備升級需求，請與資訊管理部聯絡。
- 內部人員在攜入使用可攜式媒體前，需經「系統需求與服務申請單」提出申請，由資訊管理部與處級以上部門主管同意，方可攜入使用。
- 內部人員在攜出使用可攜式媒體前，需提出書面申請，由資訊管理部或處級以上部門主管書面同意，方可攜出使用。
- 可攜式媒體介接於公司網路，使用前應先確認未感染病毒或帶有惡意程式。
- 外部人員可攜式設備應帶至會議室使用，並使用獨立連外線路，若需於辦公區域中使用時，接洽人可就風險高低判斷是否請對方填寫「私人設備使用切結書」。
  - 例：若僅短時間查詢資訊且有內部同仁陪同，可免填切結書。
  - 例：若接洽人本身有資訊外洩、病毒感染等資安風險疑慮時，則可請對方填寫「私人設備使用切結書」，以降低風險。

5.2 帳號密碼管理

5.2.1 帳號管理

- 帳號泛指系統帳號與應用程式等帳號。
- 應移除或停用不必要之帳號，並盡妥善保管帳號之責任。
- 未經權責主管允許，不得啟用 Guest 類型的帳號。
- 未經權責主管允許，不得多人共用同一帳號。
- 帳號之權限應僅依照實際之業務需求開放。
- 新進人員、職務異動及人員離職時皆需依「離職、異動交接清單」向各管理單位回報，以便進行帳號及權限之異動。

5.2.2 密碼管理

- 重要系統密碼應定期變更，並不得與上次重複。若因工作需求無法定期變更密碼時，請聯絡 MIS 同仁，由 MIS 部門協助設定系統組態，以增加安全強度。密碼應符合複雜性原則。如：密碼字元應包含數字、特殊符號及大、小寫英文字母任二種以上之組合。
- 密碼長度至少包含六個以上的字元。
- 應避免使用與個人或公司有關之資料做為密碼，並盡妥善保管密碼之責任。

5.2.3 帳號鎖定

- 應限制帳號登入錯誤的次數為 10 次，以避免密碼暴力攻擊手法。
- 應設定自動解除帳號鎖定的時間為 10 分鐘，以自動解除帳號鎖定。
- 應視情況定期檢視帳號錯誤登入次數以及早發現攻擊事件。

5.3 作業系統設定

5.3.1 事件紀錄

重要主機之系統紀錄，應依照資訊管理部的設定檔做設定，並不得更動設定或清除 LOG，如有變更的需要，請先與資訊管理部連絡。

5.3.2 服務關閉

應關閉不需要的服務，降低被滲透或攻擊的可能性。

5.4 桌面淨空政策

5.4.1 螢幕鎖定

離開座位時，應避免將機密資料顯示於螢幕，並關閉螢幕電源。

5.4.2 工作區域

- 應確保機密及內部限制文件於離開座位時，均放置於安全場所，以避免文件遺失及機密資訊外洩。
- 處理機密資料時，若有同仁或外部人員來訪時，應避免將機密資料顯示於螢幕上，避免機密資料外洩。
- 下班時間，應將工作用電腦關機，避免資料外洩或被當跳板。若因工作需求無法關機時，請聯絡 MIS 同仁，由 MIS 部門協助設定系統組態，以增加安全強度。

5.4.3 辦公設備

- 列印文件後應儘速將文件取回，以避免不必要的資訊外洩。
- 文件於傳真後應儘速將文件取回，若需透過傳真方式接收機密文件時，請先與對方約定傳真時間，並在約定時間到傳真機前等待，以取得文件。

5.5 網路服務使用準則

- 資訊管理部基於資訊安全，同仁於公司內的網際網路存取行為將留下記錄，以做為資安事件發生時之參考。
- 禁止私自利用網路芳鄰功能來分享無加密資料夾，若有相關需求，請利用公司的 File server 資源來完成。
- 依據內部重大資訊處理作業程序，同仁不得於社交網站上討論公司的機密資訊，及任何有可能對公司帶來負面效果的話題。
- 即時通訊服務之使用應以公務用途為主。
- 網路資源之使用應僅限於工作用途。
- P2P 或有可能對其他同仁造成影響的服務測試，請事先以書面與資訊管理部聯繫。未經確認下，資訊管理部得依公司網路需求，終止異常連線服務。
- 不得私自串接網路，若有相關需求，請與資訊管理部聯繫。
- 未經資訊管理單位的許可下，不得對公司外部網路提供服務，如遠端連線軟體與 Web、FTP 服務。
- 外部人員若有連線至網際網路之需求時，請使用會議室內的外部人員專屬網路。

5.6 軟體使用準則

- 相關規範請參考「軟體使用管理之規範」。
- 依照資訊管理部的規定，安裝防毒軟體，並不得任意停止防毒軟體的服務。
- 不使用來路不明或經過破解之軟體；不使用有非法或惡意意圖之軟體。
- 應確保各項軟體之重大安全性更新套件皆已更新。

5.7 資料備份

- 為保護公司資產及確保業務之持續進行，請定期備份重要資料。
- 資料備份時，不得違背資訊安全相關規定，若有特殊需求，請與資訊管理部討論，並由處級主管進行裁示。
- 備份資料應有適當的實體及環境保護。
- 備份媒體應做標示，但應儘量避免使用明顯的描述字眼來做標示，以免被輕易地辨識。

5.8 資訊交換

- 資料交換應利用公用資源(網路分享、公用資料夾)或公開服務(例如：mail、FTP)進行資料交換。
- 機密文件、檔案傳遞時應進行加密傳遞。
- 機密文件、檔案交換時，不得置於無密碼或權限控管之公用資料夾分享。
- 檔案伺服器之暫存區與公用資源僅提供資料交換，將不定期進行資料清除。

5.9 遠距工作

- 公司網路架構稱內部網路，ISP 代管設備在公司外部機房，非上述群集連線為外部網路。
- 外部網路連結公司內部網路，需透過管理處資訊管理部提出申請。
- 外部網路連結公司外部機房，需透過營運處系統部提出申請。
- 內部網路連結公司外部機房，需透過營運處系統部提出申請。
- 內部網路連結外部網路特定服務或線路，需透過管理處資訊管理部提出申請。
- 業務相關單位處理遠距工作需求時，均要文件留底，以便查核。
- 若需在外網連線至公司內網資源時，應使用加密協定，並避免資料外洩。

5.10 資安通報

若遭遇資安威脅、資安相關建議或需求，請向資訊管理部門連繫，以協助同仁保護重要資訊資產。

6 罰則：

違反上述規定者，除要求限期改善，回復公司要求設定外，將依情況回報所屬部門上級主管處理。情節重大者，依員工獎懲辦法處理。

7 參考文件：

- 系統需求與服務申請單
- 內部重大資訊處理作業程序
- 員工獎懲辦法
- 軟體使用管理之規範
- 控制重點一覽表
- 私人設備使用切結書
- 離職、異動交接清單

8 實施日期：

8.1 本作業流程須經總經理核准，修改時亦同。

8.2 本作業流程訂於民國九十九年五月六日。