宇峻奧汀科技股份有限公司

資訊安全管理規範

1 目的：本規範旨在建立完善的資訊安全管理體系，以保護企業核心資產，降低資訊安全風險，確保資訊機密性、完整性與可用性。透過風險評估、存取控制等措施，提升企業競爭力，符合法規要求，並保障使用者權益。

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資訊設備之相關規範，統稱為可攜式媒體。

3.5 資安專責單位

公司資訊安全管理單位。

4 權責：

4.1 外部人員：

- 遵守公司資訊安全管理作業。
- 委外廠商請於相關文件中載明資安要求及對委外廠商資安稽核權。公司於委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。

4.2 公司同仁：

- 遵守公司資訊安全管理作業。
- 所有使用資訊系統之人員，每年接受資訊安全宣導。

4.3 資訊管理部人員：

- 各項資訊安全狀況之掌握與排除。
- 每年定期資訊安全宣導與教育公司同仁。
- 資訊安全政策之執行。
- 定期辦理核心業務持續運作演練。

- 公司同仁可攜式媒體使用核可。

4.4 資安專責單位：

- 資訊安全管理作業擬定。
- 發生安資事件依規定進行資安通報。
- 每年接受資訊安全專業課程訓練。
- 定期盤點資通系統，並建立資訊資產清冊。
- 定期辦理資安風險評估，就資通系統鑑別其可能遭遇之資安風險。
- 定期辦理弱點掃描。
- 每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。

5 作業程序：

5.1 設備使用管理

- 非資訊管理部人員，不得對個人電腦主機進行拆裝的相關動作。
- 若有硬體故障或配備升級需求，需經「資訊需求與服務申請單」提出申請。
- 內部人員在攜入使用可攜式媒體前，需經「資訊需求與服務申請單」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，需經「資訊需求與服務申請單」提出申請，由資訊管理部或處級以上部門主管同意，方可攜出使用。
- 可攜式媒體介接於公司網路，需經「資訊需求與服務申請單」提出申請，使用前應先交由資訊管理部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。
- 內部人員若需於辦公區域中使用時，為保護公司智慧財產與維護資訊安全杜絕機密外洩，不建議個人攜帶私人筆電進公司，倘若因工作需求必需使用到個人筆電，請務必恪遵以下事項：
- 經主管同意後填寫「資訊需求與服務申請單」，申請筆電攜入公司。
  - 電子表單申請通過後，請將筆電帶至資訊管理部安裝公司防毒軟體以確保設備安全性與網路控管。
  - 簽署紙本「私人設備使用切結書」以保證所知悉資訊或獲取之機密事項不交予他人外洩，並負一切法律責任。
  - 個人筆電之電腦名稱必須可辨識，如個人中文名全名或公司個人帳號以利設備控管，若無法辨識將遭系統封鎖。
  - 預設筆電不開放 USB 儲存功能，若有開放 USB 儲存需求請填寫〔資訊需求與服務申請單〕，申請開通筆電 USB。
  - 非必要筆電不開放公司有線網路，若有公司無線網路需求請填寫〔資訊需求與服務申請單〕，申請開通筆電無線網路。

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或刪除。

5.2.2 密碼管理

- 密碼應符合複雜性原則如下：

  (一) 最小長度 8 個字元 (英文大寫+小寫+數字+符號) 三種以上之組合

  (二) 錯誤嘗試 3 次鎖定

  (三) 密碼歷程不得與前 3 組重覆

  (四) 最長使用天數 90 天

  (五) 最短使用天數 1 天（即密碼變更後 1 天內不得再變更）
- 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 3 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

建立資通系統及相關設備適當之監控措施，包含身分驗證存取紀錄、存取資源紀錄、重要行為、重要資料異動、偵測攻擊與未授權之連線、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。

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，需經「資訊需求與服務申請單」提出申請，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。
- 公司網路資源（如 E-Mail、付費服務帳號等）之使用應僅限於工作用途。
- 資安偵防類軟體或壓力測試工具有可能對其他同仁造成影響的服務測試，請事先以「資訊需求與服務申請單」提出申請，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。
- 未經申請不得私自攜帶任何網路設備如 Hub、Switch、WIFI 分享器、4G 、5G 等無線網卡設備，更不得私自串接公司網路。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，不得對公司網路提供服務，如遠端連線與 Web、FTP、其他檔案分享等服務，資訊管理部得依公司資安需求，終止異常連線服務。
- 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訪客網段專屬網路，嚴禁任意連線至公司網段。
- 辦公室網路斷網時間為每日晚間 10 點至隔日早上 7 點，夜間加班需求請事前經「資訊需求與服務申請單」提出申請，若有突發事故需於公司加班超過十點且需使用網路，可口頭向單位處級主管報告後連絡資訊管理部進行臨時授權，權限以當日為限。
- 依網路服務需要區隔獨立的邏輯網域，設立伺服器網段、辦公室網段、訪客網段，各網段依需求設置隔離政策。

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。
- 常見免費軟體或個人購買之個人版軟體，均禁止商業使用該授權多數僅供個人家用，請勿任意自行安裝，以避免侵權。
- 若有安裝個人購買可用於商業授權之正版軟體，請回報資訊管理部並提供軟體商業授權證明備查後始可續用。
- 若經查有非法安裝軟體軟體之情事，將查核結果通知各處級主管督導並限期改善。

5.7 資料備份

- 為保護公司資產及確保業務之持續進行，個人重要日常作業資料及開發資料請定

期存放至部門或專案資料夾備份，以避免個人電腦故障時檔案資料損毀。

- 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

- 資料交換應利用公司資源（FileServer 網路分享、專案或部門資料夾）或公司服務(例如：E-mail、雲端硬碟等)進行資料交換。
- 機密文件、檔案傳遞時應進行加密傳遞，不得置於無密碼或無權限控管之公用資料夾或雲端硬碟分享。
- 公司檔案暫存區僅供臨時檔案交換並定期執行暫存區清空作業，檔案使用完畢後請刪除，勿長期佔用空間，嚴禁放置機敏資料或非法影音及盜版軟體，以免觸犯智慧財產權法。
- 不得私自以可攜式媒體或雲端硬碟、Email、通訊軟體等網路媒介，將公司之機密資料或研發資料攜出，如經查獲以盜竊公司資產進行處置。
- UBS 權限全面禁止，有特定需求之專案或部門，須清楚敘明理由並提出一名人員為代表，該專案或部門僅保留該電腦權限，有需要者至該人員電腦(或特定人保管之公用機)進行 USB 操作，此以專案或部門為單位，上限一名，且該電腦將受監控。其餘 USB 權限申請僅限短期臨時開通，每月底將一律清除所有 USB 權限，次月需沿用者，應於每月 25 日前提出申請，每次申請最長不得超過 30 日，USB 傳輸過程及檔案均有監控記錄。

5.9 遠距工作

- 辦公室網路架構稱內部網路，ISP 代管設備在公司外部 IDC 機房以及雲端伺服器為外部網路。
- 外部網路連結公司內部網路，需透過管理處資訊管理部「資訊需求與服務申請單」提出申請。
- 外部網路連結公司外部機房或雲端伺服器，需透過產品技術部「資訊需求與服務申請單」提出申請。
- 內部網路連結公司外部機房或雲端伺服器，需透過產品技術部「資訊需求與服務申請單」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「資訊需求與服務申請單」提出申請。
- 業務相關單位處理遠距工作需求時，將進行全面網路、螢幕、行為監控以便查核。
- 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。
- 每月底將一律清除所有遠端連線權限，次月需沿用或新申請者，應於每月 20 號起敘明原因，以「資訊需求與服務申請單」提出並完成簽核至處級，次月得繼續使用，另此動作需於每月 25 號前完成。期間因特定需求；如專案新上線者可不

限定時間提出，但同樣於次月清除並重新申請，流程不變。

- 遠端存取資通系統，須建立安全的遠距連線機制、採多重身分驗證、採加密連線、採最小授權原則、留存完整使用者操作稽核軌跡、監控與警示異常操作行為、執行安全性漏洞更新等安控措施。

5.10 資安通報

若遭遇資安侵害事件，資安專責單位依資安事件紀錄表(附表 1)完成資安事件應變處置及通報作業程序

5.11 公司資訊環境需具備下列資安防護控制措施

- 防毒軟體。
- 網路防火牆。
- 如有郵件伺服器者，具備電子郵件過濾機制。
- 入侵偵測及防禦機制。
- 如有對外服務之核心資通系統者，具備應用程式防火牆。
- 進階持續性威脅攻擊防禦措施。
- 資通安全威脅偵測管理機制。

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：

- 資訊需求與服務申請單
- 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
- 上市上櫃公司資通安全管控指引

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。

8.3 本作業流程修訂於民國一一三年十月二十一日。

附表1.資安事件紀錄表

填寫人		
填寫日期與時間	_____年_____月_____日_____時_____分	
資安事件等級	□一級事件:影響部分資訊設備、組織仍可持續營運 □二級事件:非核心業務受影響、組織仍可持續營運 □三級事件:部分核心業務受影響 □四級事件:組織核心業務受影響	
受影響主機資訊	主機內外部IP	
	用途	
	主機URL	
	作業系統	
事件說明		
應變處置說明		
CIA 影響等級	機敏性衝擊	□非核心業務資料洩漏 □核心業務系資料洩漏 □公司重要資訊基礎建設系統或資料洩漏
	完整性衝擊	□非核心業務資料遭竄改 □核心業務系資料遭竄改 □公司重要資訊基礎建設系統或資料遭竄改
	可用性衝擊	□非核心業務運作遭受影響或短暫停頓 □核心業務運作遭受影響或短暫停頓，無法於可容忍中斷時間內恢復正常運作 □公司重要資訊基礎建設遭影響或系統停頓，無法於可容忍中斷時間內恢復正常運作
系統運行中斷紀錄	□於_____年____月____日____時____分暫停服務 □系統持續運行	
事件處理紀錄\時間		

簽名(日期) 處理人：　　主管：