2020 年 12 月 09 日	資訊安全政策白皮書	

遠雄建設

FARGLORY LAND

目錄

第一章、資訊安全管理政策

遠雄建設基於「公司獲利、客戶滿意、員工忠誠、股東認同、社會肯定」的企業責任，實施資訊安全管理，建立安全及可信賴之資訊環境，妥善維護客戶資料與遠雄建設資訊資產之機密性、完整性、可用性。為達成「永續經營」的企業精神，重要指導方針如下：

1 遠雄建設須建立資訊安全管理組織，負責規劃與推動各項資訊安全事務。

2 遠雄建設之資訊安全管理規定必須遵循相關法令規章，納入各項營運業務安全需求，適用範圍涵蓋各項作業所涉及之資料、人員、系統、設備及相關服務。

3 遠雄建設之合作夥伴及客戶於各項合約中應載明彼此在資訊安全上之責任與義務，以符合遠雄建設資訊安全政策。

4 遠雄建設之重大資訊安全異常事件，必須於規範時限內通報與處理，事後彙整相關資料以作為改進措施之依據。

5 遠雄建設之重要業務及其相關資訊資產，應針對可能發生之重大事故擬定業務永續運作計畫，並定期演練以維持其計畫可行性。

6 遠雄建設全體員工皆須具備其工作職掌所需之資訊安全知能，應認知各項資訊安全，並參與教育活動，確實瞭解並遵守遠雄建設資訊安全政策。

7 遠雄建設須建立資訊安全內控內稽機制，定期檢查各項資訊安全作業，對於不符合項目進行改善，達成良性循環之目的。

第二章、目的

1 『遠雄建設資訊安全政策白皮書』(以下簡稱本白皮書)為遠雄建設於各項作業必須遵守之資訊安全規定，目的為確保重要業務之安全性與永續性。

2 本白皮書適用之範圍涵蓋所有內部營運活動與對外業務服務。

3 資訊安全管理作業將根據『規劃 - 執行 - 檢查 - 行動』Plan-Do-Check-Act，PDCA)之流程方法，達成持續改進之目標。

第三章、組織與權責

1. 資訊工作安全推動組

由總召集人設置公司資安管理代表，為統籌資訊安全管理事宜，並設置「文件管制小組」、「資安處理與應變小組」、「資安稽核小組」以及推行委員們，資訊安全管理組織架構如圖 1。由文件管制小組負責資安標準與文件製作，由資安處理與應變小組負責相關技術與事故發生當時處理和事後改善建議，資安稽核小組則主要負責日常資安工作執行落實度驗證。必要時，本工作組得委請外部學者專家提供資訊安全顧問諮詢服務及技術支援協助，並依規定支給相關費用。

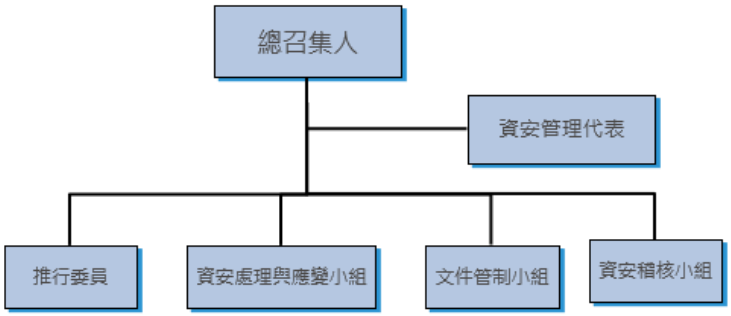


圖 1：資訊安全管理組織架構圖

2.1 溝通或傳達

為確保資安工作的有效執行，各溝通項目權責人員，遵循下表進行相關事項之溝通或傳達以達成溝通預期效果。

項	溝通項目	溝通時機	溝通對象	權責人員	預期效果	溝通方式
1	資訊安全政策	管理審查作業製/修訂時	範圍內人員	文件管制小組	人員對政策認知及了解	制定文件、政策審查，公告
2	組織角色、責任與職權	製/修訂時	範圍內人員	文件管制小組	確保責任與職權已溝通及瞭解	制定文件，公告
3	資訊安全風險處理計畫與接受殘留資訊	管理審查作業/風險評估完成時	風險擁有者	資安處理與應變小組	對風險項目及殘留風險認識	風險評鑑報告
4	不符合資訊安全管理的事件	管理審查作業	範圍內人員/委外廠商	資安處理與應變小組	確保不符合事項處理方式及不再發生	管理審查簽辦、會議
5	稽核結果	稽核完成管理審查作業	總召集人	資訊安全稽核小組	管理系統之落實度、符合性及有效性確認	查核報告管理審查簽辦、會議
6	資安運作狀況亟需改善之處	管理審查作業	總召集人	資安處理與應變小組	確保管理系統適用性、充足性與有效性	管理審查簽辦、會議
7	資安事件通報	資安事件發生時	董事會	資安處理與應變小組	通報資安事件發生之時間、範圍及原因等，必要時尋求協助	通報公告網站

表格 1

第四章、規範內容

1. 資訊安全政策的制定及評估

1.1 資訊安全政策之制定：資訊安全政策的目的為防禦一切有計畫的、意外的、來自內部的或外部的威脅，以保護資訊資產的安全。為表達對資訊安全推動之支持與決心，制定資訊安全政策。制定之資訊安全政策宣達至各階層之同仁，一體遵循。

1.2 管理階層審查為確保資訊安全管理制度持續有效運作，透過管理階層之審查，用以確保制度的適用性、適切性與有效性，並藉由稽核持續加以改善。相關內容及表單請參考預防與改善流程。

2. 資訊安全組織及權責。

2.1 資訊安全之角色及責任成立資訊安全組織以推動資訊安全事務，並透過正式的組織與管理階層授權，界定資訊安全責任。

2.2 職務區隔以實體防護及存取控制管制，以做適當之職權區分，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。

2.4 專案管理之資訊安全如遇重要資訊安全相關專案(例：重要網路設備異動、重要設備系統異動、重大應用系統異動...)時，依採購作業要求，必要時召開專案會議，針對該專案進行時可能的資訊安全風險進行分析評估。

2.5 行動裝置及遠距工作建立使用行動式電腦設備及遠距工作防護措施，以防止未經授權之存取行為或低失竊之風險，以達有效之安全管理。

3. 人員安全管理及教育訓練

3.1 人員安全管理

3.1.1 應人員於報到、離職或調動時，需依照人總室規定進行相關流程，並簽署保密協定。保密協定涵蓋期間包括從業期間與離職後，均有保密之責任，任何因未遵守本資訊安全管理規範導致之資訊安全意外事件將嚴格懲處。

3.1.2 各委外開發維護之廠商人員，必須簽署保密協定及切結遵守本資訊安全管理規範之規範。

3.2 人員教育訓練：每年度對內部同仁辦理資訊安全管理課程訓練，提升其危機意識與資訊安全觀念。課程中必須給予完整之軟體著作權與版

權觀念，嚴禁非法使用軟體，而自由軟體(freeware)與共享軟體(shareware)之安裝使用亦必須詳細了解其版權宣告並遵守。

3.3 資訊資產之安全管理

各項資訊設備除依照相關審計法規財產管理外，各單位自行負責設備之安全，移出、報廢或其他處分時經權責單位主管核定始得放行。機密或敏感資訊之安全管理機密性或敏感性的資料，需額外使用密碼進行控制。

4. 系統存取控制

4.1 使用者存取管理：帳號及通行碼嚴格禁止交付他人，職務代理時須建立代理帳號，禁制將帳號密碼張貼於公開之處。人員調動或是離職將依照人總室相關程序調整或禁用該帳號。

4.2 系統存取之責任： 同仁宜保持高度之警戒心，防範不法人士以社交工程方法(Social Engineering)獲取帳號及通行碼入侵。應具備高度之危機意識，如有發現疑似系統安全危機時，迅速通知資通安全執行工作小組人員。使用者具善盡保護個人密碼之責任。自動化登入系統之密碼，不宜存放在巨集或是功能鍵中。

4.3 網路系統之存取控制

網路使用者遵守之網路安全規定，於授權範圍內存取網路資源，不得以任何方式竊取他人之登入帳號、密碼，不得使用任何軟體、設備竊聽網路上之通訊，不得使用任何手段干擾或妨害網路之正常運作，不得嘗試入侵防火牆主機，亦不得於網路上儲存、建置或傳播色情文字、圖片、影像、聲音等資訊。如有違反以上情事，將依照相關法規查處。

4.4 應用系統之存取控制：應依資訊存取規定，配賦應用系統使用人員與業務需求相稱的資料存取及應用系統使用權限。

4.5 外部人員存取資訊之安全管理：對外部提供資料查詢或檔案傳輸服務，需評估風險，並簽訂正式的契約或協定以規範連線單位需遵守之規定及限定作業範圍與服務內容後始得提供服務。

5. 加密管理：郵件系統使用 SSL 方式進行加密處理。機敏性資料進行網路交換與儲存時依資料機敏性，考量加密處理控制。

6. 數位媒體、文件安全管理：數位媒體或文件其傳遞與與使用均須獲得單位主管授權始得使用。若有報廢之設備執行儲存媒體需要重新格式化(format)，移除相關作業軟體、資料及具有版權之系統軟體；報廢之磁帶、磁碟或光碟片等媒體進行實體銷毀。

7. 電腦系統安全管理

7.1 電腦病毒及惡意軟體之防範：同仁須使用具合法版權軟體，避免上網下載來路不明之軟體。

7.2 個人隱私之保護：資訊系統處理個人隱私資料時，依據「個人資料保護法」相關規定，審慎處理個人資料，非公務用途嚴禁調閱使用。

8. 通訊安全管理

8.1 網路安全規劃與管理

8.1.1 為維持網路能正常持續地運作，主要網路設備宜考慮或準備備援設備即時替換。

8.1.2 聯外網路宜安裝入侵偵測系統，網路系統管理人員須隨時監控非法入侵之犯罪行為，並收集入侵證據以作為法律控訴之證物。

8.2 電子郵件安全管理

8.2.1 網路使用者禁止以電子郵件騷擾他人、發送匿名郵件、偽造他人名義發送郵件或惡意發送大量不當郵件。

8.2.2 收到電子郵件時須先經過郵件掃毒軟體掃描，確保資料附件並未夾帶惡意程式後，再轉送至電子郵件伺服器供使用者讀取。

8.2.3 不開啟不明來源寄件者或信件標題異常之電子郵件，不開啟用途不明之附件，不開啟廣告信或垃圾信件，不點選電子郵件內容中不明連結。

8.2.4 電子郵件寄件前請檢查收件者是否正確，避免誤寄敏感或機密資訊給不適當的收件者。

8.3 聯外網路安全管理

除開放公眾瀏覽與下載之系統外，提供外部連結之系統均需建立個別之安全機制（至少需具備基本的使用者登入認證機制），以保障網路的安全性。

9. 供應商關係管理

9.1 供應商關係的資訊安全政策委外服務交付協議中之安全管控、委外服務之定義、委外廠商之監控審查及服務變更管理。

9.2 供應商協議內的安全處理在資訊服務委外給第三方時，於採購合約中明定與第三方服務的範圍與內容，並載明雙方之權利與義務。

9.3 供應商服務變更的管理供應商服務如變動時，需考量其變動所可能造成的風險，進行必要性之評估及因應。

10. 業務永續運作計畫之規劃及管理：應執行備援 / 備份作業之規劃與演練，對突發事件應變依資訊安全事件管理流程與服務持續性管理流程處理。任何突發之安全事件或造成運作中斷之事件，同仁不得隨意接受新聞媒體採訪發言，須依行政流程簽核後，統一發言。
11. 遵循性控制管理

    11.1適用於資訊安全管理制度相關的法律、法規與契約。

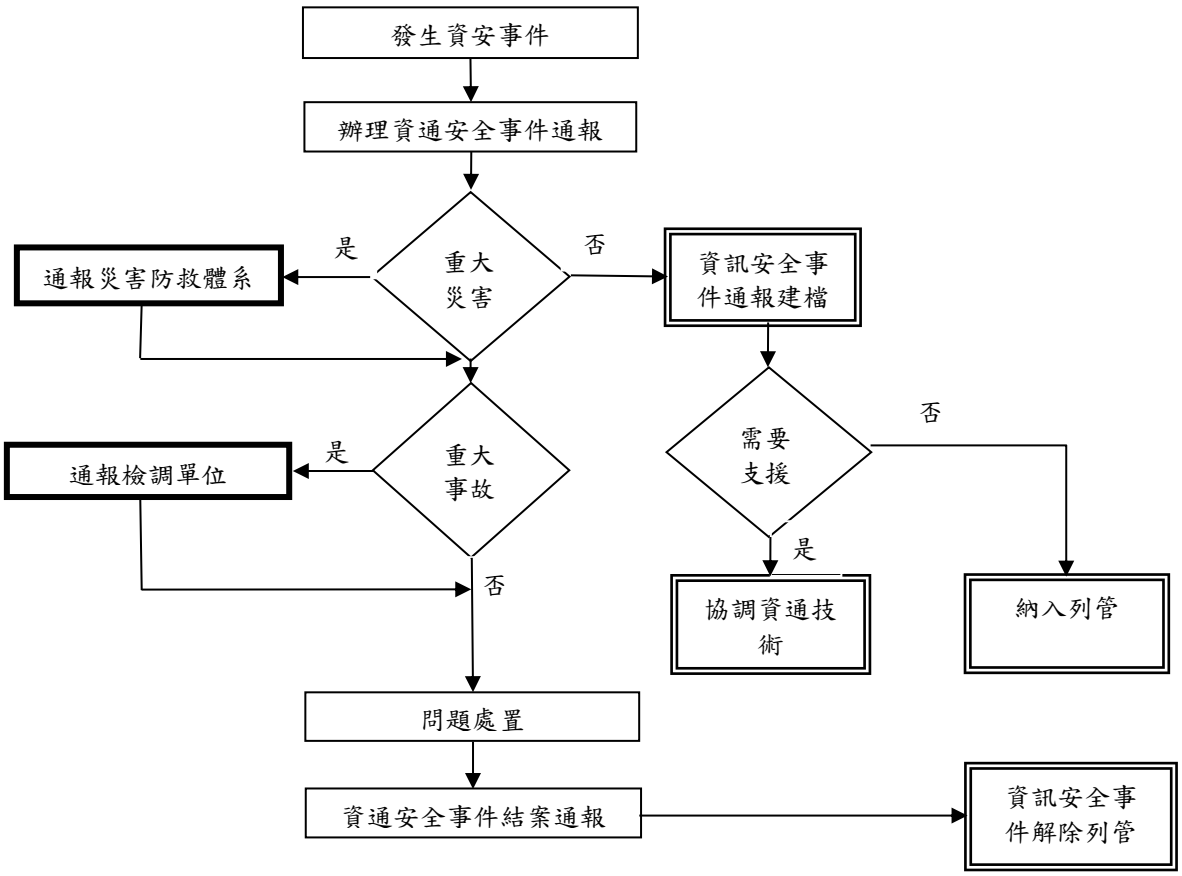
    11.2若法律、法規及相關條款或契約、保密書或切結書的涵意不清楚時，宜與相關單位諮詢或請其解釋。

第五章、資安事故通報與保全處理程序

1. 資安事故通報程序

1.1 使用者發現網路入侵之情事時需立即採取措施以防止災害繼續擴大。

1.2 通報流程如下：



2. 網路入侵的事後處理

2.1 入侵者之行為若觸犯法律規定，構成犯罪事實，由建管處會同法務室，並立即申告檢調單位，請其處理入侵者之犯罪事實調查。

2.2 應檢討網路安全措施及修正防火牆的設定，尋求適當之解決辦法，以防禦類似的入侵與攻擊。

3. 安全稽核事後處理：任何稽核計畫所得之資訊安全稽核結果，除特殊原因得簽奉核可不公開外，彙整相關單位之優缺點及綜合改進建議，簽奉核可後提供相關單位改進，各單位及人員不得將相關資訊安全稽核結果資料洩漏給不相關之第三者。為求資訊安全稽核工作之客觀性及有效性，得委請外部專家學者，協助進行資訊安全稽核工作。

第六章、附則

1. 獎懲措施

   員工違反本規範之作業規定，情節重大者，依公司內相關辦法辦理懲處。委外管理人員及委外服務人員違反本規範之作業規定，應通知受委託承商更換相關人員，並得視情節依合約規定要求承商賠償之損失。

2. 所屬單位未訂定資訊安全管理規範者得適用本規範。