113年度資訊安全報告

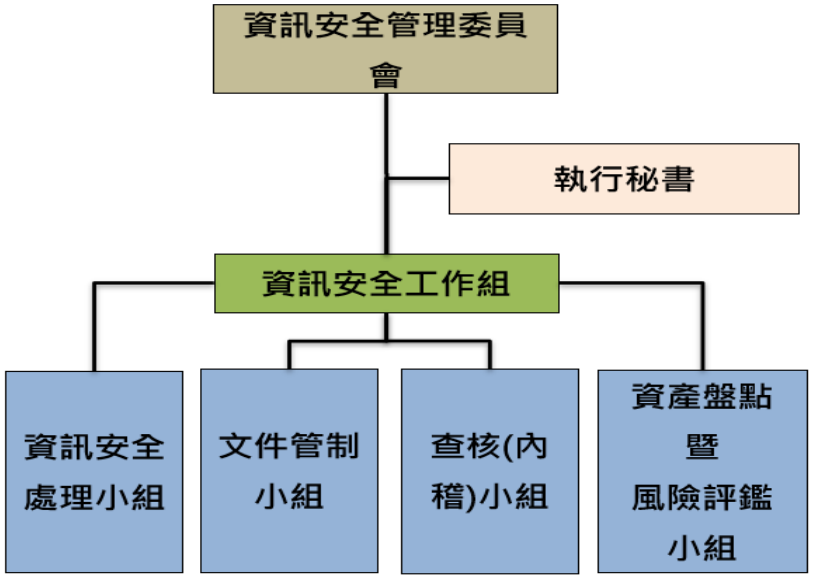
Date: 114/01/13

113年資安報告

報告綱要

- 資訊安全管理委員會
- 風險評估與因應措施
- 安全管理措施
- 資訊安全管理模式
- 資訊安全投資與改善

資訊安全管理委員會



- ✓ 111/09/01 成立資訊安全室，設有專責主管及資訊安全專責人員各一名。
- ✓ 113/12/18 為推動資訊安全管理系統(ISMS)的導入與運行，成立資訊安全管理委員會，總經理擔任召集人並指派副召集人及執行秘書，資訊安全管理代表由各事業單位及功能單位的管理階層擔任，負責協助推動和監督各單位的資訊安全工作。

風險評估與因應措施

威健核心資通營運系統	風險評估	因應措施
Email System	1. 使用者帳密被盜，成為垃圾廣告郵件跳板。 2. 郵件主機因被當跳板而被列為黑名單，無法收發郵件。 3. Email主機軟硬體故障之風險。	• 導入Office 365 Outlook(SaaS服務)進行電子郵件收發，並啟用2FA的雙重認證，降低帳密被盜風險及因軟硬體故造成服務中斷。
ERP System	1. 營運資訊資料 C,I,A (Confidentiality, Integrity and Availability) 的管控。 2. ERP 軟硬體的維運。 3. 系統開發維運人員的人才不足。	• 每年進行ERP使用者帳號/權限盤點，由各部門主管覆核。 • 進銷存流程需進行電子簽核達到資料正確性。 • IT部門計畫性更換ERP伺服器，並採用虛擬化方式提高系統完整性與可用性。 • 招募培訓新進從業人員，以利系統開發與維運。

風險評估與因應措施

威健核心資通營運系統	風險評估	因應措施
WMS System	1. WMS為自行開發的系統，使用Client/Server的架構，且DB均已虛擬化，故相對於ERP的風險較小較可控。 2. 出錯貨(date code)的人為操作風險。	• WMS伺服器以虛擬化平台建置於中華電信IDC 機房，並計畫性汰舊換新。 • WMS Client 在內部網路使用並未暴露於Internet，且使用者須申請安裝 WMS Client 端軟體方能存取資料。 • 倉庫對從業人員定期進行教育訓練。
WorkFlow	1. 目前使用華苓AgentflowV3.7，華苓已對該版本不進行維護。	• 已規劃執行升級Agentflow V4計畫。
個資法的遵行	1. 「人事系統」由人事部門管理，並委外維護。 2. WKT並無CRM系統或過多的客戶資料對於個資也都採最小資料(僅知原則)保存，故風險相對較小。	• 113年9月12資安室委由中華電信舉辦「個資法教育訓練」，線上出席合併會後觀看影片439人次。 • 「核心系統」之測試環境對個資訊息進行遮蔽。

安全管理措施

管理類別	管理措施	執行項目
權限管理	人員帳號、權限管理與系統操作行為之管理措施。	新進員工帳號申請、定期覆核有效帳號、離職員工帳號失效。
存取控管	人員存取內外部系統及資料之控制措施。	定期覆核使用者系統使用權限。
外部威脅	內部系統潛在弱點、中毒管道與防護措施。	主機弱點檢測及更新措施，病毒防護與惡意程式偵測，基於中華電信HiNet SOC的情資分享加強防火牆的設定。
弱點分析	針對PC與伺服器系統弱點掃描與檢查、修補措施。	定期檢查與修復高風險性弱點，若無法修補則進行補償性措施。
社交工程與資安教育訓練	針對使用者同仁定期宣導資安觀念（email與新人訓練）。	MIS/ICS不定期發送email分享資安新聞、宣導資安注意事項，並於新人訓練時闡明威健資安相關規範與措施。

資訊安全管理模式

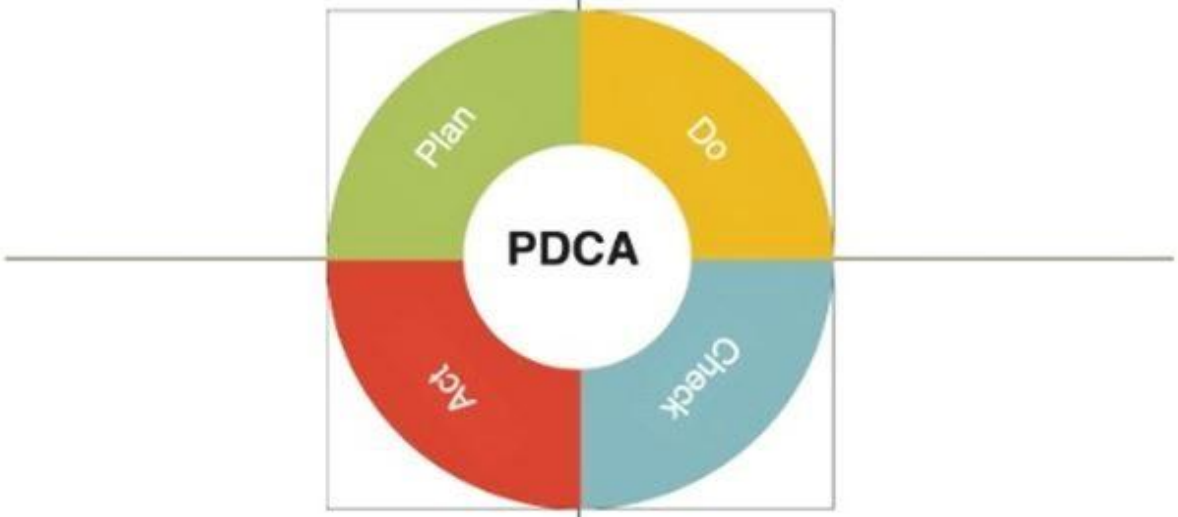
採用PDCA 循環流程管理模式，確保資訊安全管理目標之達成並且持續改善。

資安管理

- 成立資訊安全管理委員會
- 頒布『資訊安全政策』

推動執行

- 資訊安全措施導入
- 資訊安全宣導與人員教育訓練



風險改善

- 改善內部作業程序
- 引進外部解決方案

風險評估

- 資訊安全資產弱點掃描與風險評估

資訊安全管理模式

資訊安全管理 (Plan)

- 成立資訊安全管理委員會

  - ✓ 111/09/01 成立資訊安全室，設有專責主管及資訊安全專責人員各一名。
  - ✓ 113/12/18 為推動資訊安全管理系統(ISMS)的導入與運行，成立資訊安全管理委員會，總經理擔任召集人並指派副召集人及執行秘書。

- 資訊安全管理委員會職責

一.審核資訊安全管理系統目標及實施範圍。
二.審核資訊安全管理相關作業執行情形及改善的有效性。
三.檢討資訊安全相關政策及規定，協調資源之分配及使用。
四.監督營運持續演練之辦理。
五.審核實施矯正措施所需之資源，包括人力、時間及經費。
六.審核矯正措施之有效性。
七.每年至少招開管理審查會議1次，必要時得召開臨時會議。

- 資訊安全工作組

一.資訊安全處理小組
二.資產盤點季風險評鑑小組。
三.文件管制小組。
四.查核(內稽)小組

- 增訂『資訊安全政策』(114/1/13 提報董事會)

資訊安全管理目標與內容

一.本公司各事業單位執行業務時必須遵守政府相關法規(如：專利法、著作權法、個人資料保護法、個人資料保護法施行細則等)之規定。
二.設置資訊安全管理委員會，負責本公司資訊安全管理系統之建立及推動事宜。
三.建立組織全景評鑑機制，以界定資訊安全的方針與資訊安全管理系統的實施範圍，並了解組織全景及關注方的需要與期望。
四.訂定文件控管作業規定，以律定資訊安全制度相關文件之制定、修改、編碼、發行等管理原則。
五.建立資訊資產之管理機制，以統籌分配、有效運用有限資源，解決關鍵安全問題。
六.建立風險評鑑管理辦法並識別出各類資產的風險，以採取適當之風險處理措施，加以管控、降低風險至可接受之程度。
七.定期實施業務相關之資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

- 增訂『資訊安全政策』(114/1/13 提報董事會)

  資訊安全管理目標與內容

八.建立機房實體及環境安全防護措施，並定期施以相關保養維護。
九.明確規範資訊系統、網路服務、敏感資訊之使用權限，防止未經授權之存取行為。
十.建立資訊系統獲取、開發及維護作業流程，明確規範系統於開發及委外相關遵循之依據，且資訊系統或服務應於建置或推出前，應將資訊安全相關議題納入，以防範危害系統安全之情況發生。
十一.訂定及執行資訊安全內部稽核活動，以落實資訊安全管理制度，針對未盡事項執行矯正措施。
十二.訂定資訊安全之營運持續計畫並實際演練，確保本公司遭受突發事故時業務得以持續運作。
十三.本公司所有人員皆負有維持資訊安全之責任，且應瞭解及遵守相關之資訊安全管理規定，並於工作職責中落實。

資訊安全管理模式

推動執行 (Do)

- **資訊安全措施導入**

導入Office 365 Outlook(SaaS服務)，結合中華數位的Mail SPAM SQR攔截過濾垃圾郵件與威脅郵件成果良好。
113年第1~4季(113/01/01~113/12/31)：
正常郵件: 12,741,937 封
垃圾郵件:　583,964 封
威脅郵件:　195,350 封
攔截精準度：99.84% (統計自 113/01/01 ~ 113/12/31)

- **資訊安全宣導與人員教育訓練**

資安宣導: MIS/ICS每月定期進行「MIS資安宣導 資訊安全與軟體使用」及「資安情報」不定期宣導。(113 年度 Total 宣導次數: 27次)。
資安教育: 新人訓練- MIS/ICS於新人訓練時針對駭客、病毒、網路釣魚、電腦蠕蟲、社交工程、密碼維護等議題，提出說明與宣導。 113年度計有44人次。
資安教育訓練- 一般人員每年1小時/資訊人員每年3小時。113/09/12 個資法教育訓練(3小時/439名參與課程)。

資訊安全管理模式

風險評估 (Check)

- 資訊安全資產弱點掃描與風險評估

防火牆規則盤點及控管。
每年進行伺服器弱點掃描。
每年進行開發程式源碼掃描。
以中華電信HiNet SOC 做為資安情資收集， MIS/ICS會依據所提供的資訊加強防護。

風險改善 (Action)

- 改善內部作業程序

IT人員於 113/12 更新防毒軟體 WithSecure ,目前如下：

EDR and EPP for Servers	(端點檢測和響應Server)	授權:10
EDR and EPP for Computers	(端點檢測和響應PC)	授權:100
EPP for Computers	(端點防護PC)	授權:400

- 引進外部解決方案

【台灣資安主管聯盟】 113/11/29成為其「上市櫃會員」
中華電信輔導ISO27001:2022，預計114年6月取得認證。

資訊安全投資與改善

- 資安事件與因應：

駭客病毒入侵： 113年無重大駭客或病毒入侵事件。
電腦網路故障： 113年無重大網路中斷事件。
環境設施故障： 113年無重大環境設施(泛指機房冷氣,供電等設施)故障。
重大資安事件： 113年無因發生重大資通安全事件所遭受之損失或影響營運、商譽等之情事。
113年無經證實侵犯客戶隱私或遺失客戶資料投訴之情事。

- 113年度 資安人員相關教育課程與活動：

主辦單位	課程/活動名稱	日期	時數(小時)	參加人員	證(明)書
中華公司治理協會	董事會資安治理監督策略	113/05/17	3	資安室主管	中華公司治理協會研習證書- TCGA11302370
中華電信	個資法教育訓練	113/09/12	3	資安室主管	無
台灣金融研訓院	資訊安全意識、必備知識與責任	113/12/3	2	資安室主管	台灣金融研訓院證書-IS100100001640
台灣金融研訓院	資安事件說明及預防措施	113/12/5	2.5	資安室主管	台灣金融研訓院證書-IS100110001640
台灣金融研訓院	上市上櫃公司資通安全管控指引說明	113/12/6	1.5	資安室主管	台灣金融研訓院證書-IS100120001641
元智大學遠距離教學	資安事件的緊急應變處理	113/10/17	3	資安室人員	元智大學證書- YZULE3700188

- 資訊安全投資計畫：

因應ISMS(ISO27001:2022)導入，經顧問團隊(中華電信)規劃如下:

第一階段 (114/03前完成)
1.網路防火牆(第一年設定及維護)
2.源碼檢測&主機/網站弱點掃描(每年)
3.萬用憑證(每年)

第二階段 (114/03前完成)
1.應用程式防火牆(每年)
2.HINET SOC 監控(每年)

第三階段 (114/Q4建置)
1.伺服器儲存HA架構
2.IDC NAS更換

年度預計金額NT$1,146萬元