風險管理政策與程序

風險管理政策

本公司風險管理政策在於透過系統化的風險評鑑方法，釐清資產所可能面臨的風險，藉由風險審查結果決定資產之可接受風險等級，並針對高於可接受等級風險資產，控制其風險在網路家庭可接受的程度以內，確保網路家庭資產之安全，進而達到維持網路家庭業務持續運作之目的。

風險管理程序

本公司風險管理程序如附件

(附件名稱)
文件名稱：風險管理程序 版 本：V1.3文件編號：
PP-AA-202-D 資訊等級：內部使用
生效日期：20180901

管理流程依附件第10頁之程序進行管理

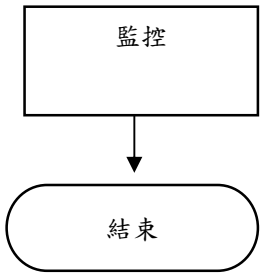
附件一：風險管理流程

風險管理流程

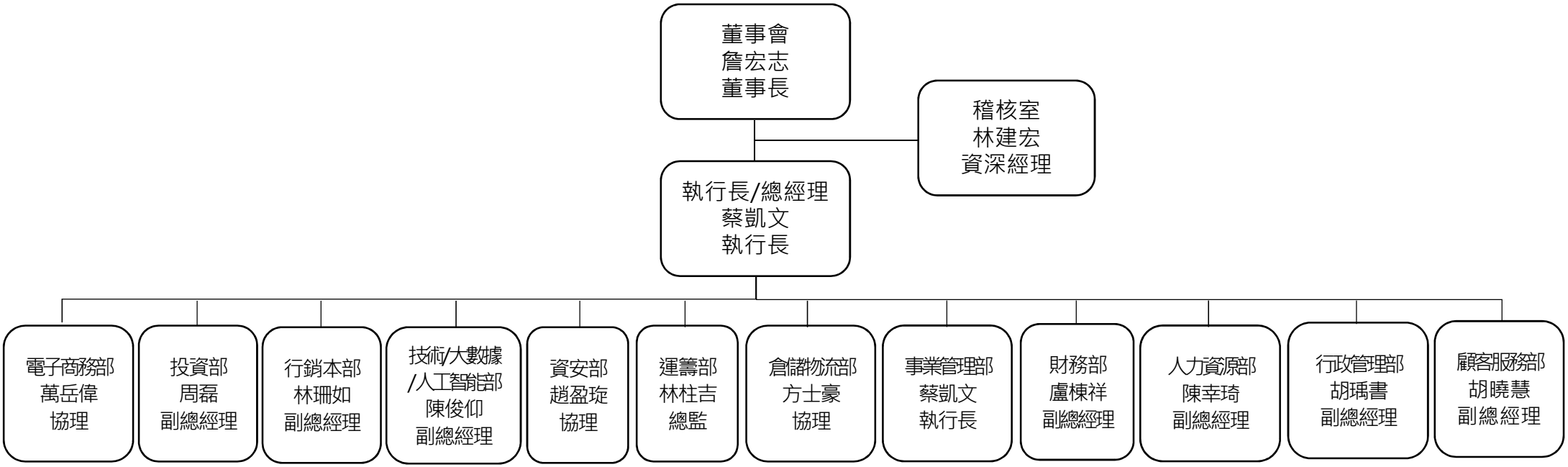
流程	說明	相關文件/表單	負責單位
開始			
關鍵業務審查	1. 依年度之業務進行審查。 2. 決定出該年度之關鍵業務，作為業務持續運作計劃。	關鍵業務審查準則	小組經理 制度管理小組 管理代表
建立資產清冊	1. 網路家庭服務相關之項目。 2. 網路家庭之資訊資產清冊。	資產分類說明	制度管理小組
資訊資產評價	1. 對資訊資產機密性、完整性、可用性與個資性進行評價。 2. 決定資訊資產價值。	資產評價說明	制度管理小組
威脅弱點評價	1. 對可能面臨之威脅與弱點進行評價。 2. 分別以問題集方式進行弱點與威脅之評估。	威脅弱點評價說明	制度管理小組
計算風險等級	依據資產價值、威脅與弱點等級計算可能之風險值。	1. ISO 27001 標準	管理代表 制度管理小組
決定風險等級	依據資訊安全性政策與風險分析計算結果決定”可接受風險等級”。	1. 資訊安全政策	管理代表 制度管理小組
撰寫風險評鑑工作報告	1. 依據審查結果撰寫風險評鑑工作報告。 2. 將風險評鑑工作報告呈管理代表審核。	1. 風險評鑑工作報告	管理代表 制度管理小組
選擇安控機制	1. 評估可行之安控機制。 2. 增修文件。	1. 執行結果紀錄	管理代表 制度管理小組
規劃執行安控機制	1. 依文件執行。 2. 開發採購以符合選擇之安控機制。	1. 各安控機制之程序、規範、辦法文件 2. 採購程序	管理代表 制度管理小組
有效性評估	1. 評估審查規劃執行之安控機制之有效性。	1. 資訊安全政策 2. 風險審查評估結果	管理代表 制度管理小組

No

Yes

	1. 稽查各種安控機制執行有效性並撰寫報告。 2. 每年至少一次提出稽核報告及相關建議事項予品質暨資訊安全代表。 3. 稽核之執行參照稽核計畫。	1. 稽核計畫 2. 稽核報告	管理代表 稽核小組

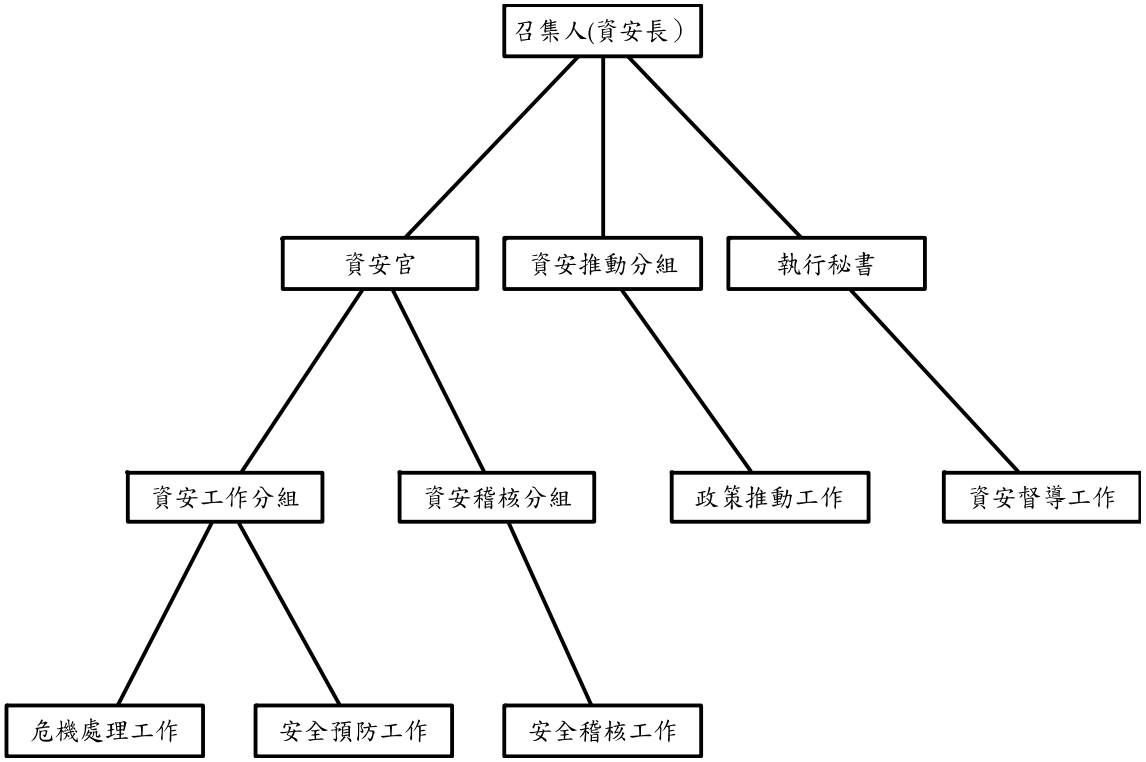
風險管理架構圖


董事會
詹宏志
董事長
稽核室
林建宏
資深經理
執行長/總經理
蔡凱文
執行長
電子商務部
萬岳偉
協理
投資部
周磊
副總經理
行銷本部
林珊如
副總經理
技術/大數據
/人工智能部
陳俊仰
副總經理
資安部
趙盈璇
協理
運籌部
林柱吉
總監
倉儲物流部
方士豪
協理
事業管理部
蔡凱文
執行長
財務部
盧棟祥
副總經理
人力資源部
陳幸琦
副總經理
行政管理部
胡瑀書
副總經理
顧客服務部
胡曉慧
副總經理

資安報告

資訊安全風險管理架構

為強化資訊安全管理，建立可信賴之各項資訊應用系統，因而成立專責部門對集團內所有資安風險進行評估與控制 同時制定相關管理規範 以達到**提升網路服務之資訊安全及服務品質，並確保營業能力及資訊服務效能**

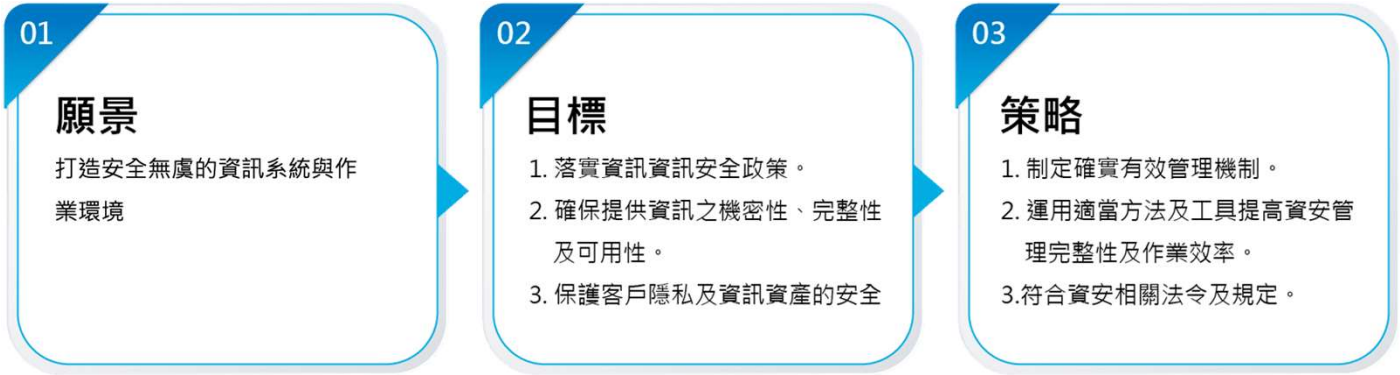


完整版資訊詳見
PCHOME-ISMS-B001-
資訊安全組織程序書

職務	負責人員	資訊安全職掌說明
召集人 (資安長)	由總經理指派擔任	▪ 主持資訊安全小組會議 ▪ 覆核各單位風險水準及控管措施 ▪ 資訊安全政策與目標之核定及督導 ▪ 資訊安全責任之分配、協調與督導 ▪ 資訊安全文件之核定 ▪ 擔任安全管理代表 ▪ 其他資訊安全事項之核定 ▪ 內、外部資訊安全議題或需求之決定
執行秘書、助理	執行秘書、助理由資安長指派擔任	▪ 協助舉行資訊安全小組會議 ▪ 主持資訊安全相關會議 ▪ 協助資訊安全事務之協調 ▪ 控管資訊安全相關文件 ▪ 其他資訊安全事項之協助 ▪ 辦理本公司資安教育訓練 ▪ 協助資安稽核工作之執行 ▪ 其他資訊安全事項之協助 ▪ 擔任本公司對外資安窗口 ▪ 綜理內、外部資訊安全議題或需求
資安推動分組	由資安長指派各事業單位高階管理者擔任，或各單位自行指定	▪ 政策推動工作： • 瞭解公司資安執行方向 • 主持分組內分組會議 • 推動資安工作 • 建立單位資安組織與分工授權 • 擬定單位風險水準及控管措施 • 派遣及協調單位資安執行資源 • 審定單位資安重要文件 • 監督審查單位資安執行事項 • 檢討改善單位資安能力 • 資訊安全事件之檢討與追蹤 ▪ 安全稽核工作： • 配合資安稽核工作之執行

職務	負責人員	資訊安全職掌說明
資安官	由資安長指派擔任	▪ 資訊安全文件制定 ▪ 資訊安全年度計畫制定 ▪ 提昇公司整體資安意識 ▪ 規劃與落實公司資安治理作為 ▪ 資安工作分組之分配、協調與督導 ▪ 資安稽核分組之工作分配與督導 ▪ 其他資訊安全事項之技術支援 ▪ 協助內、外部資訊安全議題或需求
資安工作分組	由資安官指派	▪ 安全預防工作： • 蒐集資安訊息、培育資安技術 • 辦理單位資安風險評鑑 • 擬訂資安控管措施 • 協助辦理業務持續計畫與演練 • 協助執行資安矯正措施 • 協助與追蹤弱點修補及風險狀態 • 協助資安文件及紀錄 • 彙集單位內、外部資訊安全議題或需求 ▪ 危機處理工作 • 協助規劃危機處理 • 協助查明危機事件原因 • 協助確定影響範圍並作損失評估 • 協助執行緊急應變措施 • 協助辦理資安事件通報相關事宜 • 追蹤資安事件處理情形 ▪ 安全稽核工作： • 配合資安稽核工作之執行
資安稽核分組	由資安官指派，並遴選各單位稽核成員擔任	▪ 安全稽核工作： • 籌組資訊安全稽核小組 • 培訓資訊安全稽核人力 • 規劃及執行資訊安全稽核計畫 • 辦理定期或不定期資安稽核作業 • 彙編資訊安全稽核報告 • 不符合事項之追蹤

資訊安全政策訂定與佈達



資訊安全管理範疇涵蓋12項領域:

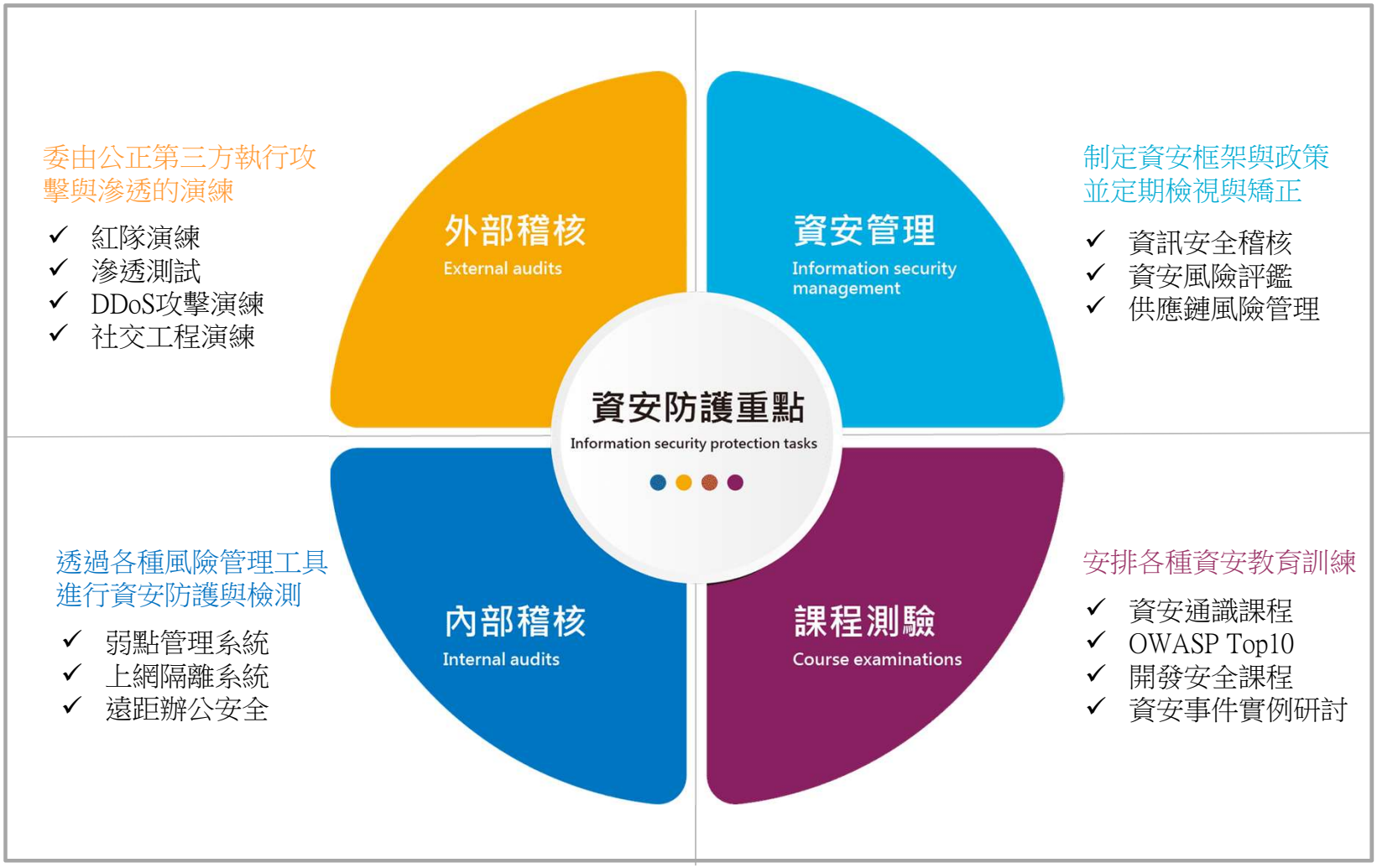
- 資訊安全組織
- 人員安全
- 資產管理
- 存取控制
- 委外管理
- 系統開發與維護
- 實體及環境安全
- 事故通報暨緊急應變程序
- 通訊與作業安全
- 矯正程序
- 營運持續管理
- 資安稽核作業

近3年版本更新公告紀錄

110 年 08 月、 110 年 07 月、 108 年 06 月

完整版資訊安全政策詳見
PCHOME-ISMS-A001

資訊安全具體管理方案


委由公正第三方執行攻擊與滲透的演練
✓ 紅隊演練
✓ 滲透測試
✓ DDoS攻擊演練
✓ 社交工程演練
外部稽核
External audits
資安管理
Information security management
制定資安框架與政策並定期檢視與矯正
✓ 資訊安全稽核
✓ 資安風險評鑑
✓ 供應鏈風險管理
資安防護重點
Information security protection tasks
透過各種風險管理工具進行資安防護與檢測
✓ 弱點管理系統
✓ 上網隔離系統
✓ 遠距辦公安全
內部稽核
Internal audits
課程測驗
Course examinations
安排各種資安教育訓練
✓ 資安通識課程
✓ OWASP Top10
✓ 開發安全課程
✓ 資安事件實例研討

公司治理評分(資安項目)

需同時符合以下三項要件，始能於構面計分。

[要件一]

建置資訊安全風險管理架構（如：成立資安委員會，定期檢討資安政策，並定期向董事會報告等）。

[要件二]

訂定並揭露資訊安全政策。

[要件三]

訂定並揭露資訊安全具體管理方案（包含是否投保資安險，若無，則詳述相關預防措施）。

[備註]

公司揭露110年仍在效期內之ISO27001或CNS27001認證，可直接於構面計分。