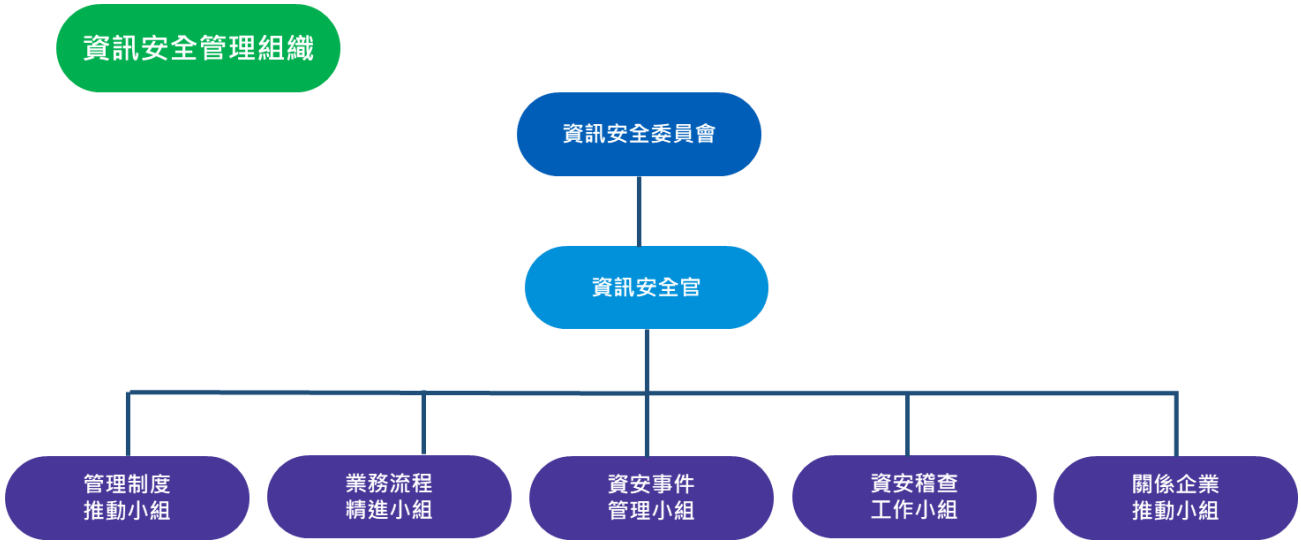
中興保全科技股份有限公司

114 年資訊安全運作情形報告

(一) 資訊安全風險管理架構

為確保資訊安全管理制度之執行，落實資訊安全政策，故成立「資訊安全管理組織」，負責執行資訊作業安全管理規劃，建置與維護資訊安全管理體系，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核。

資訊安全管理組織定期召開會議檢討執行情形，並每年定期向董事會報告執行情形與檢討。資訊安全管理組織圖及各角色功能如下：



- 資訊安全委員會：
  由本公司資安長擔任召集人，負責資訊安全相關事項之決議。
- 資訊安全官：
  由資訊安全委員會召集人指派專人擔任，負責規劃各項資訊安全作業。
- 管理制度推動小組：
  由資訊安全委員會召集人指派各單位人員組成，負責執行各項資訊安全作業。

- 業務流程精進小組：
  由資訊安全委員會召集人指派核心業務單位人員組成，負責執行處理業務層面資訊安全作業。
- 資安事件管理小組：
  由資訊安全委員會召集人指派法務部、對外發言系統及資訊中心人員等組成，負責處理資訊安全事件。
- 資安稽查工作小組：
  由管理制度推動小組負責規劃本公司資訊安全管理制度稽查作業，稽查員聘請外部顧問或技術專家協助，稽查作業包含稽查計畫之撰寫、檢查表之擬定、稽查發現之改善追蹤等。
- 關係企業推動小組：
  由資安管理室負責協助確認關係企業所適用「個人資料檔案安全維護辦法」之法律遵循實施情形。
  由資安管理室負責規劃及督導關係企業資訊安全管理制度實施情形。

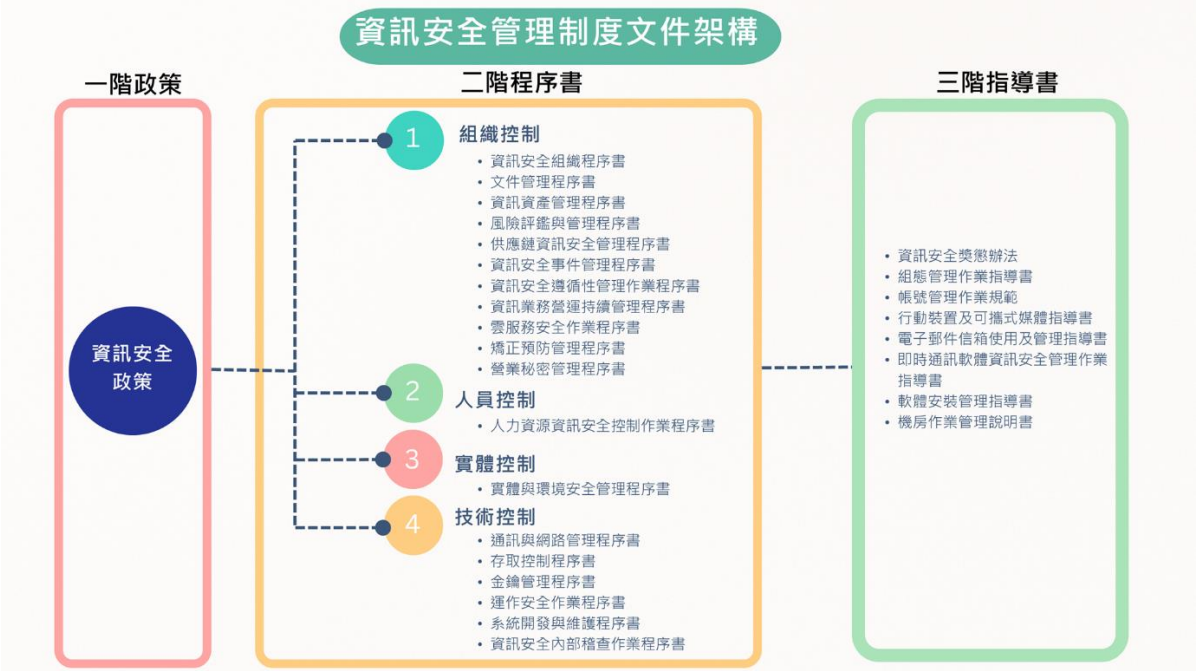
(二) 資訊安全政策目標

本公司於 113 年 3 月 28 日頒布適用於全組織之資訊安全管理政策及規範，並導入建立完整的資訊安全管理系統（ISMS, Information Security Management System），從系統面、技術面、程序面降低企業資安威脅。為維護本公司資訊資產之機密性(C)、完整性(I) 與可用性(A)，並保障使用者資料隱私之安全。藉由本公司全體同仁共同努力來達成下列目標：

- 保護本公司業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
- 保護本公司業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
- 建立本公司資訊安全營運持續計畫，以確保本公司業務服務之持續運作。
- 本公司執行各項業務之資訊服務須符合政府相關法令或法規之要求。

為確保公司的資安防護能力與時俱進，我們的資安管理制度每年都會進行全面性的檢視與更新。這些重要的調整不僅採納了外部資安驗證專家的專業建議，更密切因應了外部資安威脅環境的快速變化，同時也更貼合內部組織文化的實際運作。透過這項持續性的優化機制，我們致力於建立一個更為堅固、彈性且高效的資安防護體系，以有效保障公司資訊資產的安全。

本公司資訊安全管理制度文件於 114 年 3 月 28 日改版發行，本次改版發行文件共計二階程序 4 本、三階規範 4 本、四階表單 2 份、以及廢止四階表單 1 份，現行資訊安全管理制度文件架構如下圖所示：



(三) 具體管理方案

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

- **定期盤點及風險管理：**
  - ✓ 針對全組織定期盤點並建立資訊資產清冊及個人資料盤點清冊，依資安及個資風險評鑑進行風險管理，落實各項管控措施。
- **網路、端點及應用安全：**
  - ✓ 導入端點偵測與回應（EDR, Endpoint Detection and Response）

機制，持續性針對端點設備進行異常偵測及防護。

- ✓ 定期清查端點應用程式，導入應用程式白名單（Application Whitelisting）機制。
- ✓ 整體資訊系統網路安全存取優化，定期審查重要主機及系統特權帳號。
- ✓ 強化遠端連線管理及審查機制。

- ➢ **資料洩漏預防機制：**
  - ✓ 管理及限制可攜式媒體(USB)之使用。
  - ✓ 啟用郵件 DLP(Data Loss Prevention)功能。
- ➢ **提升資安防禦能力：**
  - ✓ 定期針對核心系統及對外提供服務之網站進行脆弱度分析(弱點掃描)及滲透測試，並加以補強與修護，以降低資安風險。
  - ✓ 重要資訊系統或設備建置適當之備援或監控機制並訂定演練計畫，定期演練維持其可用性，於每次演練後進行檢討修正。
- ➢ **供應鏈安全：**
  - ✓ 制定供應鏈資訊安全管理程序，本公司委外合約均應套用「供應商資安暨個資規範」，以此要求供應商所交付之商品 (含資通系統或資通設備)符合本公司資安品質、資安驗證及檢測、個資蒐集及保護等相關措施、資安事件因應措施、及實地稽核等要求。
- ➢ **資安保險之安排：**
  - ✓ 本公司已投保資安險作為企業解決資安威脅風險的方法之一，保護公司於發生網路攻擊時，能將潛在損失降至最小的範圍。
- ➢ **教育訓練：**
  - ✓ 定期舉辦資安教育訓練(線上課程)、高階主管資安課程(實體課程)、透過郵件不定期資安宣導、及社交工程釣魚郵件測試，以提升資安意識，使資安的運作在高階主管與各部門的支持下，落實到每一位員工身上。
- ➢ **資安聯防：**

- ✓ 本公司已申請加入「資安主管聯盟」、「TWCERT/CC 台灣電腦網路危機處理暨協調中心」等資安聯防組織，並與法務部調查局簽署「資安聯防與情資分享 MOU」，提供本公司國內外資安事件及資安情報交流、企業資安通報及危機處理等服務，提升本公司整體資安防護能量。

➢ **資安事件通報與應變能力：**

- ✓ 本公司建有通報平台，事件發生時依據本公司資安事件通報程序，依事件嚴重程度等級進行影響和損失評估，採取對應的應變及復原行動。

➢ **法令遵循及國際資安認證標準：**

- ✓ 本公司已符合「上市上櫃公司資通安全管控指引」各項要求，並持續通過 ISO27001 國際資訊安全認證作為達成各項風險管理的方法與檢驗依據。

(四) **投入資訊安全管理之資源**

項目	投入資源之執行情形
資安宣導	**於內部系統發布，執行全員資安宣導：** ◆ 切勿安裝來路不明及破解軟體宣導(113/08/30) ◆ 電子郵件社交工程演練宣導_113 年下半年(113/09/03) ◆ 機敏資料(含個資)管理宣導(113/09/12) ◆ 遠距辦公資訊安全宣導(113/10/08) ◆ 信件詐騙識別方式宣導(113/10/18) ◆ 釣魚郵件提醒宣導-相信音樂(113/10/15) ◆ ULTRA VNC 遠端服務隱私設定宣導(113/10/24) ◆ 釣魚信件提醒宣導-DHL 和新進能源公司(113/11/01) ◆ File Server (S 槽)使用，資訊安全注意事項(113/12/03) ◆ 社交攻擊郵件主旨情資宣導(113/12/26) ◆ 連續假期資訊安全宣導(114/01/22)

	◆ 近期郵件收發注意事項安全宣導(114/02/04) ◆ 辦公室搬遷，資料銷毀及保護須知(114/02/19) ◆ 近日釣魚郵件提醒宣導-華灣國際有限公司(114/2/21) ◆ 電腦 USB 連接埠功能關閉，注意事項!(114/03/27) ◆ 釣魚郵件_詐騙信件宣導!!-上曜建設開發股份有限公司(114/03/31) ◆ 電子郵件社交工程演練宣導(114/05/26) ◆ 五月份資訊安全宣導(郵件、加密隨身碟、社交工程攻擊等)(114/05/19) ◆ 六月份資訊安全宣導(不隨意安裝軟體、密碼定期更新、定期關機)(114/06/27)
稽查作業	每年執行一次全組織資安暨個資稽查作業： ◆ 分公司：114/06/06-114/08/18 ◆ 總公司：114/08/18-114/09/25
資訊系統營運持續演練	◆ 災害演練 ◆ ERP 系統每季 HA 演練 ◆ 新 TODO 系統資料庫備份還原 ◆ 健康照護系統 HC 備份還原 ◆ NOTES 系統資料庫備份還原 ◆ 總帳系統每季 HA 演練
聯防組織/情資蒐集	**來自 TWCERT/CC、調查局、資安設備原廠、資安社群...等情資：** 與內部相關情資：0 則。 與外部相關情資：7384 則。
資安會議	◆ 113 年第 3 次資訊安全會議 (113/11/12)，重點討論議題： ■ 前次會議追蹤事項 ■ 軟體派送與安裝包統一說明 ■ 社交工程演練成果說明 ■ 總公司各樓層 Wifi 清查

	■ 各單位 NAS 後續管理 ■ 資訊安全宣導 ◆ 114 年第 1 次資訊安全會議 (114/01/09)，重點討論議題： ■ 前次會議追蹤事項 ■ 針對 113 年外部稽核發現的缺失，討論改善方案及落實計畫 ■ DLP 產品導入評估 ■ EDR 安裝情形追蹤 ■ 加密隨身碟設定及發放情形追蹤 ■ 弱點掃描/滲透測試追蹤 ■ 資訊安全宣導 ■ 南港新大樓零信任網路規劃 ◆ 114 年第 2 次資訊安全會議 (114/04/10)，重點討論議題： ■ 前次會議追蹤事項 ■ 使用者安裝軟體權限移除 ■ 限制使用本機帳號登入 ■ E-mail 安全強化措施 ■ Win 10 EOS 議題及系統汰換對策 ■ USB 管理進程 ■ 弱點掃描/滲透測試追蹤 ■ 中保科與博訊 ISO 27001 合併驗證母子證書可行性討論 ■ 資訊安全宣導 ◆ 114 年度資安與個資內部稽查課程暨總公司內部稽查啟始會議 (114.6.18) ■ 內部稽查介紹 ■ 資安及個資查核技巧分享 ■ 稽查時程規劃及項目

	課程名稱	日期	上課人數

教育訓練	資訊安全通識教育訓練	114/01/08- 114/05/30	2349
	立保保全個資保護管理制度建置啟動會議	114/04/14	16
	114 年度資安暨個資盤點及風險評鑑課程(一)	114/04/14	38
	114 年度資安暨個資盤點及風險評鑑、內部稽查說明課程(北部)	114/04/23	29
	114 年度資安暨個資盤點及風險評鑑、內部稽查說明課程(中部)	114/05/12	15
	114 年度資安暨個資盤點及風險評鑑、內部稽查說明課程(南部)	114/05/15	18
	社交工程演練教育訓練	114/07/10- 114/08/31	164
資安險	**承保範圍：** ◆ 第三人責任-洩漏隱私及機密保障、網路安全保障、媒體責任保障 ◆ 營業中斷損失 ◆ 危機管理-鑑識費用、資料洩漏反應費用、損失理算費用、聲譽維護費用 ◆ 第一人損失-網路勒贖 **保險賠償限額：1 億元**		

(五) **資訊安全事件與因應措施**

依據本公司「資訊安全事件管理程序書」，將資安事件分為三級：

1 級事件：

- ✓ 非核心業務 CIA 遭破壞(如該事件為個案)。
- ✓ 小於 100 筆個人資料遭外洩且該事件受到媒體關注之可能性較低或該事件尚未經執法機關或目的事業主管機關通報。

2 級事件：

- ✓ 核心業務 CIA 遭輕微破壞(如賣斷系統評估影響超過 1000 家客戶以上或租賃系統評估影響超過 300 家客戶以上)。
- ✓ 約 100 筆至 5000 筆個人資料遭外洩且該事件已受媒體關注(媒體詢問，可能尚未報導)或該事件已經執法機關或目的事業主管機關通報。

3 級事件：(達發布重訊標準)

- ✓ 核心業務 CIA 遭嚴重破壞(如賣斷系統及租賃系統影響超過 5000 家客戶以上) ，且其中斷時間超過該系統或業務之最大可容忍中斷時間(MTPD)。
- ✓ 事件高於 5000 筆個人資料遭外洩且事件已受到媒體或社群平台廣泛報導或事件已被當事人提起訴訟，或經執法機關或目的事業主管機關提起行政調查。

事件統計區間	3 級事件	2 級事件	1 級事件	個資侵害申訴
113/8/1-114/7/31	0	2	4	0

1 級事件多屬客戶設備密碼遭破解或成為中繼站之個案；2 級事件則為系統遭揭露存在安全漏洞，相關事件皆已依照內部資訊安全事件管理程序即時回應及處理。

於統計區間內(113/8/1-114/7/31)未發生需發布重大訊息之 3 級資安事件及個資侵害申訴案件。

◆ 本公司已導入 ISO27001 資通管理系統，並定期取得 ISO27001 認證，已於 113/12/20 通過 ISO/IEC 27001:2022 之轉版認證作業，目前證書之有效期為 114 年 1 月 3 日至 117 年 1 月 3 日。

Certificate TW16/00020

The management system of

Taiwan SECOM Co., Ltd.

6F, NO. 139, Cheng Chou Road, Taipei 103612, Taiwan, R.O.C.

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities

Provision of operation, maintenance and management activities for Data Center and its associated infrastructure, data communication networks and information processing facilities in accordance with Statement of Applicability version 1.8.

This certificate is valid from 03 January 2025 until 03 January 2028 and remains valid subject to satisfactory surveillance audits.

Issue 4. Certified since 03 January 2016

Certified activities performed by additional sites are listed on subsequent pages.

L. Moran

Authorised by

Liz Moran

Business Manager

SGS United Kingdom Ltd

Rossmore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK

t +44 (0)151 350-6666 - www.sgs.com

This document is an authentic electronic certificate for Client' business purposes use only. Printed version of the electronic certificate are permitted and will be considered as a copy. This document is issued by the Company subject to SGS General Conditions of certification services available on Terms and Conditions | SGS. Attention is drawn to the limitation of liability, indemnification and jurisdictional clauses contained therein. This document is copyright protected and any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful.

Page 1 / 2

Certificate TW16/00020, continued

Taiwan SECOM Co., Ltd.

ISO/IEC 27001:2022

Issue 4

Sites

Taiwan SECOM Co., Ltd.
6F, NO. 139, Cheng Chou Road, Taipei 103612, Taiwan, R.O.C.
Provision of operation, maintenance and management activities for Data Center and its associated infrastructure, data communication networks and information processing facilities in accordance with Statement of Applicability version 1.8.

Taiwan SECOM Co., Ltd. Computer room of SECOM
3F, No.111, Ln. 76, Ruiguang Rd., Neihu Dist., Taipei City 114062, Taiwan, R.O.C.
This site is the main computer room that supports activities within the certification scope of the main site.