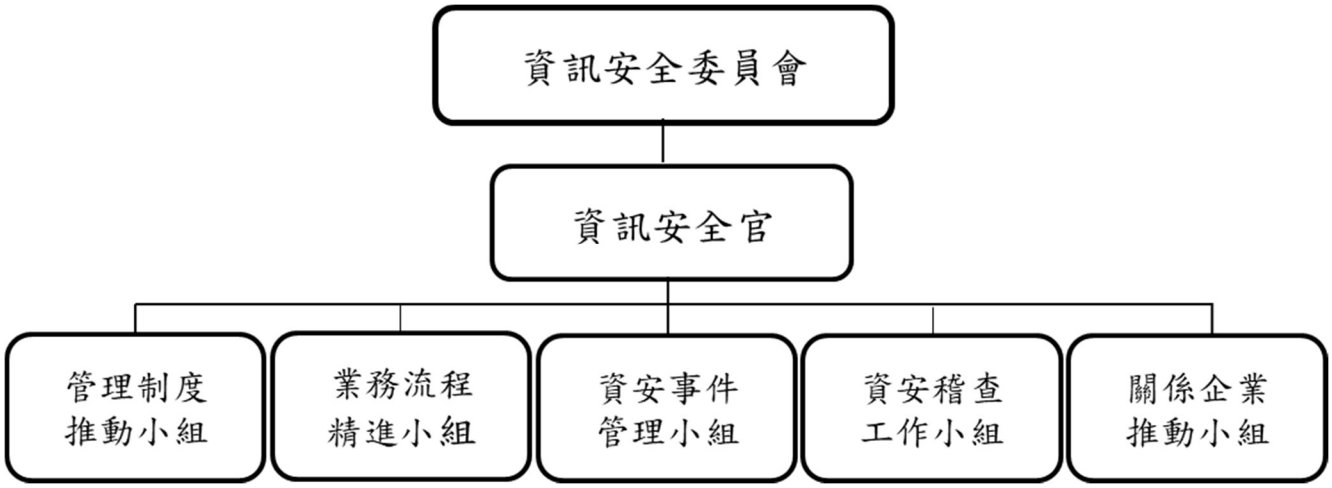
中興保全科技股份有限公司

資訊安全運作情形報告

(一) 資訊安全風險管理架構

本公司在 112 年成立「資安管理室」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。組織各角色及功能如下：



- 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：

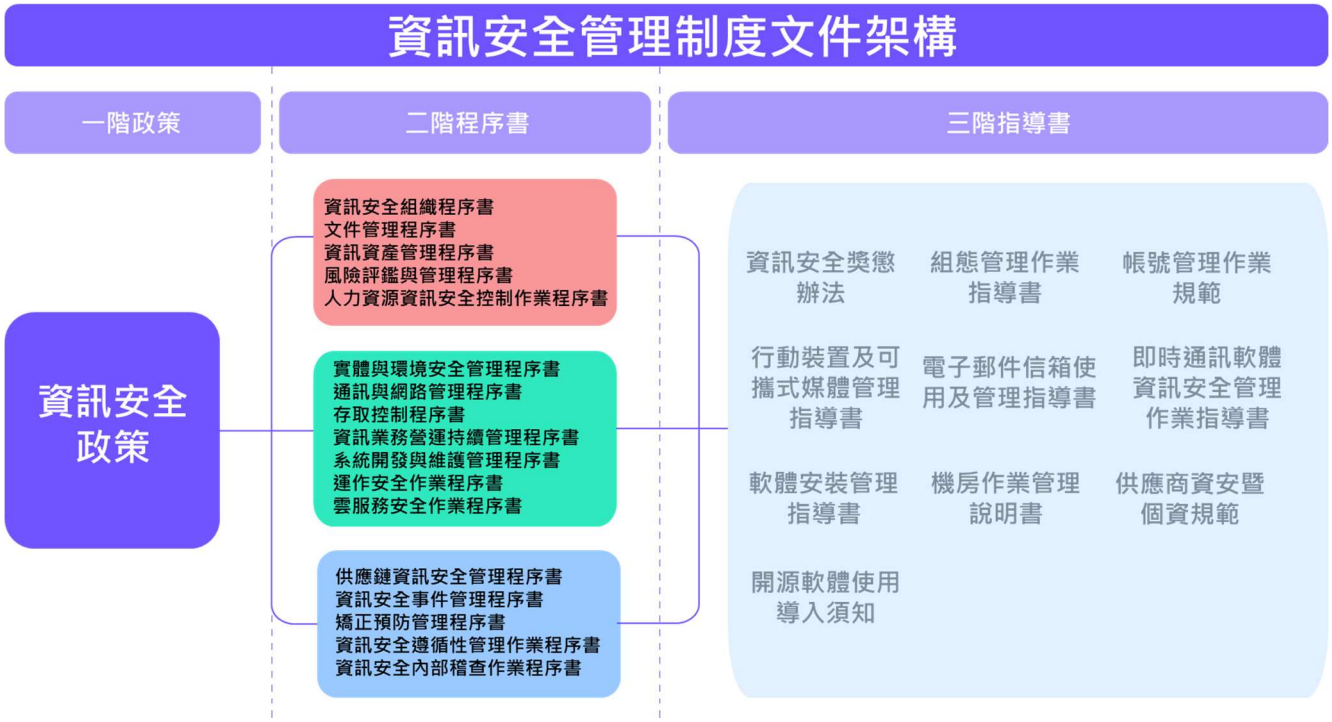
  由資安管理室負責協助確認關係企業所適用「個人資料檔案安全維護辦法」之法律遵循實施情形。

  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。



(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，依資安風險評鑑進行風險管理，落實各項管控措施。
- **增進網路、端點及應用安全：**
  - ✓ 提升端點設備的異常偵測及防護能力，包含導入端點偵測與回應（EDR, Endpoint Detection and Response）機制。
  - ✓ 定期清查端點應用程式，規劃應用程式白名單（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。

- ✓ 建置私有雲個資專區(加密區)。

- **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定期演練，維持其可用性。
- **資安事件通報與應變能力：**
  - ✓ 制定資安事件通報程序，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。
- **風險控制：**
  - ✓ 與國內知名事務所「KPMG 數位智能風險顧問公司」合作，透過其專業服務進行整體資安體檢，以公正第三方驗證之客觀結果，作為持續精進資安管理的依據。
  - ✓ 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。
- **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。
- **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，並與法務部調查局建立良好溝通管道，提供本公司國際資安事件及跨國資安情報交流、企業資安通報及危機處理等服務，提升本公司整理資安防護能量。

(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：** ◆ 個資法修法，外洩個資最高罰 1500 萬!! (112/05/17) ◆ 小心! 釣魚郵件不是好玩的，通通是詐騙!! (112/05/19) ◆ 小心商業詐騙，電子郵件易遭駭客竄改 (112/11/24) ◆ 防詐騙宣導海報 (113/01/29) ◆ 機敏資料安全保護： 銷毀作業規範宣導 (113/02/21) ◆ 電子郵件社交工程演練宣導 (113/03/29) ◆ 端點偵測與回應(EDR)安裝作業公告 (113/04/18) ◆ 釣魚郵件提醒宣導 (113/05/23) ◆ 使用生成式 AI 資安風險宣導 (113/07/09)
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：113/04/08 – 113/07/03 ◆ 總公司：113/07/29 – 113/08/27
資訊系統營運持續演練	◆ 災害演練 ◆ ERP 系統、保全系統每季 HA 演練 ◆ 網路骨幹服務管理(硬體設備 CoreSwitch 更換、北高線路繞路、自動切換) ◆ VSS 影像保全系統 DCDB 備份還原

	◆ 雲端門禁系統資料庫備份還原 ◆ NOTES 系統資料庫備份還原 ◆ 總帳系統每季 HA 演練 ◆ Gitlab 產品智財系統資料庫備份還原
聯防組織/情資蒐集	**來自 TWCERT/CC 情資：** 與內部相關情資：2 則。 與外部相關情資：114 則。
資安會議	◆ 112 年第 2 次資訊安全會議 (112/07/25)，重點討論議題： ■ 前次會議追蹤事項 ■ 資安室工作說明 ■ 資訊安全政策審查 ■ 可接受風險值檢視 ■ 近期 Fortinet 近期 Fortinet Fortinet 發佈資安漏洞警訊，設備更新或評估採取因應措施 ■ 公司電腦 Windows Update 更新狀況說明 ■ 弱掃與滲透檢測後續進行 ◆ 112 年第 3 次資訊安全會議 (112/11/27)，重點討論議題： ■ 前次會議決議事項之處理狀況 ■ ISO 27001 驗證前管理審查議題(資訊安全管理系統內、外部議題的變更、關注方之回饋、資訊安全績效回饋、風險評鑑結果及風險處理計畫狀態、持續改善之機會) ◆ 113 年度資訊安全啟始會議 (113/01/10) ■ 專案管理及執行時程說明 ■ 重點工作說明及待配合事項 ■ 教育訓練規劃 ◆ 113 年第 1 次資訊安全會議 (113/04/30)，重點討論議題： ■ 外稽事項 1 個次要缺失+4 個觀察事項+3 個改善契機

<table>
<tr><td></td><td>
■ ISO27001 驗證改版
■ 資訊安全通識教育線上學習
■ 資安宣導文宣
■ 導入 EDR 現況
■ 尋找遠端連線軟體測試(應由使用者點選同意後，工程師方可連線處理作業)
■ 設定 AD GPO(待資安室彙整後提供)
■ 離職員工電腦整機流程
■ WSUS 修補派送討論
■ 使用者電腦應用程式白名單機制
■ 建立 file Server 後，限制 USB 使用
■ 對外網站弱掃與滲透測試，後續改善追蹤中
◆ 113 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
■ 內部查核範圍及時程說明
■ 稽查定義與認知
■ 稽查流程說明
■ 資安常見稽查問題
■ 個資常見稽查問題
◆ 113 年第 2 次資訊安全會議 (113/07/19)，重點討論議題：
■ SentinelOne 安裝後現況說明
■ 各部門自行採購授權軟體之管理（請資訊服務部說明）
■ AD policy 設定與管理
■ File Server 整理與權限管理、限制 USB 使用測試
■ 2024.08.27(9:30-17:00)資訊中心作業查核
</td></tr>
<tr><td>教育訓練</td><td>
<table>
<tr><td>課程名稱</td><td>日期</td><td>上課人數</td></tr>
<tr><td>資訊安全通識教育訓練</td><td>112/12/21-</td><td>2497</td></tr>
</table>
</td></tr>
</table>

		113/03/20	
	關係企業之個資保護準備事項說明會	112/12/25	21
	113 年度資安暨個資盤點及風險評鑑課程(一)	113/01/24	24
	113 年度資安暨個資盤點及風險評鑑課程(中部)	113/02/16	16
	113 年度資安暨個資盤點及風險評鑑課程(二)	113/02/27	42
	關係企業之資訊資產盤點說明會	113/03/08	25
	113 年度資安暨個資盤點及風險評鑑課程(南部)	113/03/11	18
	社交工程演練教育訓練	113/05/31- 113/07/31	380
	113 年度高階主管【資訊安全暨個資保護】課程	113/06/18、 113/06/19	108
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
112/8/10-113/8/13	0	6	17	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 級事件則多為分享器設備遭揭露安全漏洞，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(112/8/10-113/8/13)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，目前證書之有效期為 111 年 1 月 3 日至 114 年 1 月 3 日。

Certificate TW16/00020

The management system of

Taiwan SECOM Co., Ltd.

6F, NO. 139, Cheng Chou Road,
Taipei 103, Taiwan, R.O.C.

has been assessed and certified as meeting the requirements of

ISO/IEC 27001: 2013

For the following activities

The scope of registration appears on page 2 of this certificate.

This certificate is valid from 03 January 2022 until 03 January 2025 and remains valid subject to satisfactory surveillance audits.
Recertification audit due a minimum of 60 days before the expiration date.
Issue 3. Certified since 03 January 2016

This is a multi-site certification.
Additional site details are listed on subsequent pages.

Authorised by

SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

21HC 27001 2013 0421 M2

Page 1 of 2

Taiwan SECOM Co., Ltd.

ISO/IEC 27001: 2013

Issue 3

Detailed scope

Taiwan SECOM Co., Ltd.
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 1.5.

Computer room of SECOM
This site acts as a main server room

Additional facilities

Computer room of SECOM
3F, No.111, Ln. 76, Ruiguang Rd., Neihu Dist., Taipei City 114, Taiwan, R.O.C.

UKAS MANAGEMENT SYSTEMS
0005

Certificate TW16/00020

The management system of

Taiwan SECOM Co., Ltd.

6F, NO. 139, Cheng Chou Road,
Taipei 103, Taiwan, R.O.C.

has been assessed and certified as meeting the requirements of

ISO/IEC 27001: 2013

For the following activities

The scope of registration appears on page 2 of this certificate.

This certificate is valid from 03 January 2022 until 03 January 2025 and remains valid subject to satisfactory surveillance audits.
Recertification audit due a minimum of 60 days before the expiration date.
Issue 3. Certified since 03 January 2016

This is a multi-site certification.
Additional site details are listed on subsequent pages.

Authorised by

SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

21HC 27001 2013 0421 M2

Page 1 of 2

Certificate TW16/00020, continued

Taiwan SECOM Co., Ltd.

ISO/IEC 27001: 2013

Issue 3

Detailed scope

Taiwan SECOM Co., Ltd.
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 1.5.

Computer room of SECOM
This site acts as a main server room

Additional facilities

Computer room of SECOM
3F, No.111, Ln. 76, Ruiguang Rd., Neihu Dist., Taipei City 114, Taiwan, R.O.C.

UKAS MANAGEMENT SYSTEMS
0005