機密等級：一般

統一超商股份有限公司
資通安全管理政策

113 年 12 月 19 日訂定

第一條 目的

確保統一超商股份有限公司(以下簡稱本公司)所屬資訊資產-網路設備、電腦設備、應用系統、人員安全及委外廠商經由此一管理政策之管理，有效降低因人為疏失或天然災害等因素，導致之資訊資產不當使用、洩漏、竄改或破壞等風險，進而達到保護資通安全之目的，包含：

一、 機密性(Confidentiality)：確保只有獲得合法授權的使用者可以存取資訊。
二、 完整性(Integrity)：保障資訊與資訊處理方法的正確與完整性。
三、 可用性(Availability)：確保獲得授權的使用者於有需求時能適時存取資訊及相關資產。

透過本政策之管理，明確宣示本公司支持資安之目標，及使相關人員有所依循，並適切合乎本公司對資安之要求及相關法令之規範，以降低任何資安事件所帶來之衝擊，並持續運作及改善資通安全管理系統同時保障本公司與客戶之權益。

第二條 適用對象

本公司全體員工。

第三條 定義

無。

第四條 政策規範

一、 資通安全管理系統

1. 概述

本公司為展現貫徹資通安全管理的決心，確保公司內所有資訊與資訊系統獲得適當保護，參考 ISO/IEC 27001 標準之要求建立、記載、實施及

維護資通安全管理系統，並持續系統的有效性。

2. 運作機制

本公司參考 ISO/IEC 27001 標準，採用 Plan-Do-Check-Act（PDCA）之循環運作模式，建立與實施資通安全管理系統，並維繫其有效運作與持續改進。

(1) 規劃與建立(Plan)：依據本公司整體策略與目標，藉由成立資訊安全管理組織，控制潛在之威脅及漏洞，規劃風險評鑑、設計與建置控管機制，以建立資訊安全管理系統。

(2) 實施與運作(Do)：依據評估規劃之結果，建立或修正應有之管控機制。

(3) 監督與稽核(Check)：監督資訊安全管理系統各項作業之落實執行，並評估及稽核其有效性。

(4) 維護與改進(Act)：根據監督稽核之結果與建議，執行矯正措施，改善並執行應有之控管機制，以持續維護資訊安全管理系統之運作。

二、 管理責任

1. 應建立資安管理組織，負責推動、協調及督導下列資訊安全管理事項：

(1) 資安政策之擬定、審查、宣導及督導。

(2) 資安責任之分配及協調。

(3) 宣導符合各項資安目標、資安政策及法律規範下之責任，以及持續改進之需求。

(4) 充分提供資源以建立、實作、運作、監視、審查、維持與改進資安管理系統。

(5) 擬定接受風險與可接受風險等級的準則。

(6) 資安稽核計劃制定、資訊風險評估及不定期之資訊安全測試。

(7) 彙整資安管理系統管理審查議題與資料。

(8) 鑑別資安管理制度之內外部利害關係人，考量其對本公司之資安需求與期望，並決定內外部所需之溝通。

(9) 資安事件之檢討及監督，考量可能影響資安管理制度之內外部議題。

(10) 每年實施資安相關教育訓練與宣導，評估所提供資安教育訓練之有效性。

(11) 其他資安事項之核定。

2. 管理審查

本公司管理審查作業由資通安全執行處執行，管理階層應每年執行乙次管理審查以持續確保資安管理系統運作之適切、充足與有效，審查範圍包括資安管理系統改進方案與變更需求之評估，審查結果應予詳實記錄並妥善保存。

3. 資訊安全指標

本公司應建立資安指標評估資安的績效及資安管理制度之有效性，資安指標應至少包含量測之項目、方式、時間、頻率及負責人員等資訊，以確保資安指標量測之有效性。資安指標應與本公司資安政策作適當結合。

4. 資通安全內部稽核

應定期或不定期進行安全評估或稽核作業，以檢討控管目標、措施與程序是否合乎相關標準、法令規章或資訊安全需求，並依預期規劃有效執行與維持，以持續增進資安管理系統的有效性。

5. 資安管理系統之改善

(1) 持續改善

本公司應透過內外部稽核結果、資安事件分析、矯正措施及管理審查等機制，持續增進資安管理系統之有效性。

(2) 矯正措施

本公司應採取適當的控管措施，以減少資安管理系統建置與運作過程中所發現之不符合事項，並防止再度發生。矯正措施之作業程序如下：

- 識別各項不符合事項。
- 判定各項不符合之原因。
- 評估所需採取之措施，以確保各項不符合事項不再重複發生。
- 決定及實作所需之矯正措施。
- 記錄及審查所採取之矯正措施的有效性。

6. 文件管理系統

(1) 文件管制

本公司資安管理系統相關文件之管制方式，資安文件之管制、核發與變更均應依據本公司文件管制相關作業程序之規定辦理。

(2) 紀錄管制

本公司資安管理系統運作所產生之任何文件、表單及紀錄，應指定相關紀錄保存人員妥善保管，以利追蹤資安管理系統之執行狀況，維護系統有效運作。

7. 資安政策指導與覆核

本政策每年至少評估內容乙次，檢討覆核與修訂，以符合內外部利害關係團體的需求與期望，確保資安實務作業之有效性。

8. 實施規範與法令之遵循

本公司全體人員均須遵循此政策，違反者須依本公司相關規定予以處分，如涉有相關刑責或法律責任者，如營業秘密法、著作權法、個人資料保護法等，將衡酌情節追訴其法律責任。

三、 資訊安全管理原則

應建立但不限於，下方所條列之管理原則及控制措施：

1. 資訊安全組織
2. 人力資源安全
3. 資產管理
4. 存取控制
5. 密碼學

6. 實體及環境安全
7. 運作安全
8. 通訊安全
9. 系統獲取、開發及維護
10. 組態管理
11. 雲端服務管理
12. 供應商關係
13. 威脅情資管理
14. 資訊安全事故管理
15. 營運持續管理
16. 遵循性

第五條 參考文件

第六條 核准與修訂

本公司之資通安全管理政策經董事會核定後實施，修訂時亦同。