文件名稱：資訊安全管理政策

制定單位：資訊安全管理委員會

申請類別： □制定 ☑修訂 □廢止

NO	修訂日期	頁次	版本	修 訂 內 容 摘 要
1	2021/03/31		01	新制定。
2	2021/05/31		02	調整版本呈現的格式。
3	2024/03/15		03	配合 ISO／IEC 27001：2022 版本，調整資安政策。

文件編號	ISMS-1-001	機密等級	一般	日期	2024/04/10	版本	03

巨安長齡股份有限公司
資訊安全管理政策

1. 目的

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之業務持續運作環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

2. 適用範圍

資訊安全涵蓋 14 項管理事項，避免因人為疏失然災害等因素，導致資訊不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。

3. 定義

所謂資訊安全係將管理程序及安全防護技術應用於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體及經由列表機所列印之各式報表，以確保資訊蒐集、處理、傳送、儲存及流通之安全。

4. 本公司資訊安全政策

用心、細心、誠心，資訊安全永保安心。

5. 主題特定政策

5.1 存取控制：

5.1.1 限制對資訊及資訊處理設施之存取。

5.1.2 確保授權使用者得以存取，並避免系統及服務的未授權存取。

5.1.3 令使用者對保全其鑑別資訊負責。

5.1.4 防止系統及應用遭未經授權存取。

5.2 實體及環境安全：

5.2.1 防止組織資訊及資訊處理設施遭未經授權之實體存取、損害及干擾。

5.2.2 防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。

5.3 資產管理：

5.3.1 識別組織之資產並定義適切之保護責任。

5.3.2 確保所有資產依其對組織之重要性，受到適切等級的保護。

5.3.3 防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。

5.4 資料傳送：

5.4.1 確保資料傳送可追溯性及不可否認性 。

5.4.2 維持傳送作業之可靠性及可用性。

5.4.3 實體傳送使用破壞存跡或抗破壞之控制措施。

5.4.4 使用規定之電子傳輸媒體傳遞資料，不可因貪圖方便而任意使用非法與不當之傳輸媒體。

5.4.5 不得利用任何傳輸媒介透過資料傳遞、訊息傳送、發言或視訊等方式透露機密或敏感性資訊給其他組織或人員。

5.4.6 須依權責及工作需求核發適當權限，以管制相關文件之存取。

5.5 端點裝置之安全組態及處置：

5.5.1 對使用者端點裝置分發及回收。

5.5.2 對使用者端點裝置軟體安裝進行管控。

5.5.3 對使用者端點裝置進行安全性更新。

5.5.4 使用者端點裝置經登入程序使用。

5.5.5 防範惡意軟體對使用者端點裝置危害。

5.5.6 管制私人裝置使用。

5.6 網路安全：

5.6.1 網路使用者經授權後，只能在授權範圍內存取網路資源。

5.6.2 對使用網路系統的電腦連接線路，應適當加以控制，以減少未經授權之系統存取或電腦設施的風險。

5.6.3 設定網路區隔之規劃，應遵循內外網路實體區隔規定，並應禁止個人無線網路裝置破壞內外網路實體區隔之安全機制。

5.6.4 非經授權嚴禁使用無線網路及私有有線設備與網路介接。

5.7 資訊安全事故管理：

5.7.1 確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳達。

5.7.2 建全資訊安全事故通報體系。

5.8 資訊備份：

5.8.1 依照資訊之可用性及完整性需求，制定個資訊備份週期、方式及保存期限，並測試其有效性。

5.8.2 依照備份資料之機密性需求加以防護，避免衍生之其他資安事件。

5.9 密碼學：

5.9.1 依照法規、客戶要求及資訊資產風險設置加密機制。

5.9.2 管制金鑰產生、分派啟用、儲存、更新、廢止到封存和銷毀等作業。

5.10 資訊分類分級及處理：

5.10.1 資訊標示涵蓋所有格式的資訊及其他相關聯資產

5.10.2 使人員及其他關注方認知標示要求。

5.10.3 提供所有人員必要之認知方法，以確保正確標示資訊並進行相對應的處理。

5.11技術脆弱性管理：

5.11.1 定義並建立與技術脆弱性管理相關聯之角色及責任。

5.11.2 偵測其資訊資產是否存在脆弱性。

5.11.3 軟體更新管理過程，以確保對所有獲授權軟體，安裝最新經核可之修補程式及應用程式之更新套件。

5.11.4 使用適合所使用技術之弱點掃描工具,以識別脆弱性並查證脆弱性修補是否成功。

5.12安全開發政策：

5.12.1 確保資訊安全係跨越整個生命週期之整體資訊系統的一部分。此亦包括經由公共網路提供服務之資訊系統的要求事項。

5.12.2 當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。

5.12.3 在採購軟體時，視其安全需求，進行評估。

5.12.4 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

5.12.5 資訊系統應保護資料，防止洩漏或被竄改。

6. 資訊安全組織

6.1 資訊安全管理委員會由主任委員指派管理階層中的一員作為管理代表，負責資安各標準制度之建置、實施與維持，以統籌公司之管理制度、資源調度等事項之協調及研議。

6.2 建立「資訊安全組織成員表」，以確保任務明確之指派及 ISMS 有效之聯繫。

6.3 資訊安全管理委員會之任務分配如下：

6.3.1 主任委員：

- ISMS 管理制度之政策核准。
- ISMS 系統之目標的核准與確保審查框架的建立。
- ISMS 管理制度相關事務之資源取得、分配、協調與督導。

6.3.2 管理代表：

- 管理代表本身具有一切與資訊安全管理運作的監督權責，當資訊安全管理系統運作發生異常時賦有向高階管理階層直接提報權力，不受行政系統與外部影響。
- 協助召開管理審查會議、資訊安全會議，並報告有關本管理系統之運作狀況。
- 依照客戶需求之規定，負責要求建立、執行、維護符合資訊安全管理活動的書面化程序。
- 督導資訊安全事務之分配與協調，包含資訊安全管理認證單位之聯繫窗口。
- 協助高階管理階層提升全員對客戶資訊安全要求、法令法規的認知。

- 透過內部稽核活動成果，負責將資訊安全管理實施成效，向管理階層報告，以作為系統改善依據。
- 主持管理審查會議。
- ISMS 管理制度之政策的核准。
- ISMS 系統之目標的核准與確保審查框架的建立。

6.3.3 文管中心：

- 1. 統一對公司員工發佈本系統相關事項。
- 2. 宣達與執行本委員會決議事項。
- 3. 配合輔導顧問實施輔導工作。
- 4. 協同驗證機構辦理驗證工作。

6.3.4 推行委員：

- ISO 27001 資訊安全管理系統的推動、維持及改善。
- 負責資訊安全管理制度相關程序文件之審查。
- 負責資訊資產盤點、風險評估、風險處置、殘餘風險處理的策劃之全過程。
- 相關法令、法規遵循之界定與更新。
- 負責資訊安全之適用性聲明書之修訂。
- 出席資訊安全管理審查會議。

6.3.5 資訊安全執行小組：

- 緊急應變通報、災害復原系統的規劃。
- 負責持續營運計畫之制定、修訂與維護。
- 系統存取控制管理。
- 網路安全管理。
- 資訊系統監控與防毒。

7. 適用性聲明書

依據「ISO 27001 資訊安全管理系統-要求」要求產出「適用性聲明書」，以書面方式列舉資訊資產是否適用其標準所列之控制措施，及其不適用之原因。當組織架構、人員、設備、實體環境等變動時，資訊安全執行小組應重新定義控制措施之適用性。

8. 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本公司營運持續及資訊安全實務作業能力。

9. 實施

9.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

9.2 本政策經主任委員核定後實施，修訂時亦同。