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。

文件編號	ISMS-1-001	機密等級	一般	日期	2021/05/31	版本	02

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。管理事項如下：

2.1 資訊安全政策。

2.2 資訊安全組織。

2.3 人力資源安全。

2.4 資產管理。

2.5 存取控制。

2.6 密碼學。

2.7 實體及環境安全。

2.8 運作安全。

2.9 通訊安全。

2.10系統獲取、開發及維護。

2.11供應者關係。

2.12資訊安全事故管理。

2.13營運持續管理之資訊安全層面。

2.14遵循性。

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。

4.1 資訊安全政策：(依附錄 A5~A18)

巨安長齡股份有限公司
資訊安全管理政策

4.1.1 依營運要求及相關法律與法規，提供資訊安全之管理指導方針及支持。

4.1.2 資訊安全政策由管理階層定義並核准，且對內部及相關外部傳達。

4.1.3 資訊安全政策應定期或發生重大變更時審查，以確保合宜、適切及有效性。

4.2 資訊安全之組織：

4.2.1 建立管理框架，以於組織內啟動及控制資訊安全之實作及運作。

4.2.2 確保遠距工作及使用行動裝置之安全。

4.3 人力資源安全：

4.3.1 確保員工及承包者瞭解其將承擔之責任，並適任其角色。

4.3.2 確保員工及承包者認知並履行其資訊安全責任。

4.3.3 將保護組織利益納入聘用變更或終止聘用過程之一部分。

4.4 資產管理：

4.4.1 識別組織之資產並定義適切之保護責任。

4.4.2 確保所有資產依其對組織之重要性，受到適切等級的保護。

4.4.3 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。

4.5 存取控制：

4.5.1 限制對資訊及資訊處理設施之存取。

4.5.2 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。

4.5.3 令使用者對保全其鑑別資訊負責。

4.5.4 防止系統及應用遭未經授權存取。

4.6 密碼學：

4.6.1 依照法規、客戶要求及資訊資產風險設置加密機制。

4.6.2 對加密使用金鑰進行取得、安裝、回收、備份及展期作業。

4.7 實體及環境安全：

4.7.1 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。

4.7.2 防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。

4.8 運作安全：

4.8.1 確保資訊處理設施之正確及安全操作。

4.8.2 確保資訊及資訊處理設施，以防範惡意軟體。

4.8.3 防範資料漏失。

4.8.4 紀錄事件即產生證據。

4.8.5 確保運作中系統之完整性。

4.8.6 防範對技術脆弱性之利用。

4.8.7 使稽核活動對運作中系統之衝擊降至最低。

4.9 通訊安全：

4.9.1 確保對網路及其支援之資訊處理設施中資訊之保護。

4.9.2 保護組織內及與任何外部個體所傳送資訊之安全。

4.10系統獲取、開發及維護：

4.10.1 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。

4.10.2 確保於資訊系統之開發生命週期內，設計及實作資訊安全。

4.10.3 確保測試用資料之保護。

4.11供應者關係：

4.11.1 確保對供應商者可存取之組織資產的保護。

4.11.2 維持資訊安全及服務交付之議定等級與供應者協議一致。

4.12資訊安全事故管理：

4.12.1 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。

4.13營運持續管理之資訊安全層面：

4.13.1 資訊安全持續應嵌入組織之營運持續管理系統中。

4.13.2 確保資訊處理設施之可用性。

4.14遵循性：

4.14.1 避免違反有關資訊安全相關之法律、法令、法規或契約義務，以及任何安全要求事項。

4.14.2 確保依組織的政策及程序，實作及運作資訊安全。

5. 資訊安全組織

5.1 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。

5.2 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。

5.3 資訊安全管理委員會之任務分配如下：

5.3.1 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。

5.3.2 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。

5.3.3 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。

5.3.4 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。

5.3.5 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。

6. 適用性聲明書

依據「ISO27001 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。

7. 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。

8. 實施

8.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

8.2 本政策經主任委員核定後實施，修訂時亦同。