力麗科技股份有限公司

資訊安全政策

機密等級：■一般 □敏感 □機密

編　　號：ISMS1I002
版　　本：01
核准日期：2020/08/03

文件名稱：資訊安全政策
文件編號：ISMS1I002
制定日期：2020/07/15
申請類別：■制定　□修訂　□廢止

No.	修訂日期	頁次	修訂內容摘要
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

1. 目的

1.1. 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

2.1. 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：

2.1.1. 資訊安全政策制定及評估。
2.1.2. 資訊安全公司職責與分工。
2.1.3. 人力資源安全。
2.1.4. 資訊資產管理。
2.1.5. 存取控制管理。
2.1.6. 密碼學管理
2.1.7. 實體及環境安全管理。
2.1.8. 運作安全。
2.1.9. 通訊安全。
2.1.10. 系統獲取、開發及維護。
2.1.11. 供應者關係。
2.1.12. 資訊安全事故管理
2.1.13. 資訊安全的營運持續管理
2.1.14. 遵循性

3. 定義

3.1. 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

4.1. 保護內部文件等資訊資產之機密性、完整性與可用性；對外提供之資料庫應用，則確保其安全穩定及高效率之資訊服務。

5. 控制措施政策：

5.1. 資訊安全政策：(依附錄 A5~A18)

5.1.1. 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。

5.1.2. 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。

5.1.3. 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。

5.2. 資訊安全之組織：

5.2.1. 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。

5.2.2. 確保遠距工作及使用行動裝置之安全。

5.3. 人力資源安全：

5.3.1. 確保員工及承包者瞭解其將承擔之責任，並適任其腳色。

5.3.2. 確保員工及承包者認知並履行其資訊安全責任。

5.3.3. 將保護組織利益納入聘用變更或終止聘用過程之一部分。

5.4. 資產管理：

5.4.1. 識別組織之資產並定義適切之保護責任。

5.4.2. 確保所有資產依其對組織之重要性，受到適切等級的保護。

5.4.3. 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。

5.5. 存取控制：

5.5.1. 限制對資訊及資訊處理設施之存取。

5.5.2. 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。

5.5.3. 令使用者對保全其鑑別資訊負責。

5.5.4. 防止系統及應用遭未經授權存取。

5.6. 密碼學管理：

5.6.1. 密碼建立採用 6 個字元以上，並包括英文及數字。

5.6.2. 使用者不應在工作上使用與個人帳號相關的密碼，並至少 6 個月更換一次。

5.6.3. 密碼禁止與任何人分享，包括 同事與上司。。

5.6.4. 防止系統及應用遭未經授權存取。

5.7. 實體及環境安全：

5.7.1. 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。

5.7.2. 防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。

5.8. 運作安全：

5.8.1. 確保資訊處理設施之正確及安全操作。

5.8.2. 確保資訊及資訊處理設施，以防範惡意軟體。

5.8.3. 防範資料漏失。

5.8.4. 紀錄事件即產生證據。

5.8.5. 確保運作中系統之完整性。

5.8.6. 防範對技術脆弱性之利用。

5.8.7. 使稽核活動對運作中系統之衝擊降至最低。

5.9. 通訊安全：

5.9.1. 確保對網路及其支援之資訊處理設施中資訊之保護。

5.9.2. 保護組織內及與任何外部個體所傳送資訊之安全。

5.10. 系統獲取、開發及維護：

5.10.1. 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。

5.10.2. 確保於資訊系統之開發生命週期內，設計及實作資訊安全。

5.10.3. 確保測試用資料之保護。

5.11. 供應者關係：

5.11.1. 確保對供應商者可存取之組織資產的保護。

5.11.2. 維持資訊安全及服務交付之議定等級與供應者協議一致。

5.12. 資訊安全事故管理：

5.12.1. 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。

5.13. 營運持續管理之資訊安全層面：

5.13.1. 資訊安全持續應嵌入組織之營運持續管理系統中。

5.13.2. 確保資訊處理設施之可用性。

5.14. 遵循性：

5.14.1. 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。

5.14.2. 確保依組織的政策及程序，實作及運作資訊安全。

6. 資訊安全責任

6.1. 資訊安全管理委員會應建立及審查本政策。

6.2. 資訊安全管理者透過適當的標準和程序以實施本政策。

6.3. 所有人員與合約供應商均須依照程序以維護資訊安全政策。

6.4. 所有人員有責任報告安全事件，和任何已鑑別出的弱點。

6.5. 任何蓄意違反資訊安全的行為將受到相關規範或法律行動。

7. 資訊安全目標

7.1. 執行資訊安全管理需達成之資訊安全目標，包含以下範圍，並於「資訊全景分析與風險評估管理程序」訂定具體項目進行統計。

7.1.1. 資安政策審查

7.1.2. 行動裝置所導致之風險

7.1.3. 資安組織人員受訓

7.1.4. 資訊資產清冊更新

7.1.5. 離職/退休人員帳號管理

7.1.6. 實體設備保養

7.1.7. 病毒監控

7.1.8. 對外網路連線

7.1.9. 資料安全

7.1.10. 系統測試

7.1.11. 委外資訊服務廠商資安管理
7.1.12. 資安事件避免重複發生
7.1.13. 資安事件對公司營運持續影響
7.1.14. 本公司之業務活動合法執行

8. 適用性聲明書

8.1. 依據「ISO 27001 資訊安全管理系統-要求」要求制定「資訊安全管理系統-適用性聲明書」，確認資訊安全管理各項控制措施，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，ISMS 資安委員會將重新定義控制措施之適用性。

9. 審查

9.1. 本政策依據「資訊安全管理審查程序」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。

10. 實施

10.1. 資訊安全政策經管理審查會議核定後，發佈各單位實施，修訂時亦同。