1.目的

為確保小川實業有限公司(以下簡稱本公司)所屬之資訊資產之機密性、完整性及可用性，並符合相關法令法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，以保障本公司之權益。

2.適用範圍

資訊安全管理涵蓋 13 項管理事項。避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、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 資訊安全政策制定及評估

2.2 組織的資訊安全職責與分工

2.3 人力資源安全與教育訓練

2.4 資訊資產管理

2.5 存取控制與密碼管理

2.6 實體與環境安全

2.7 作業安全管理

2.8 通訊安全管理

2.9 資訊系統取得、開發及維護

2.10 供應商安全管理

2.11 資訊安全事故管理

2.12 營運持續管理

2.13 遵循性（適法性）

3.依據

3.1ISO/IEC 27001:2013 (Information technology — Security techniques — Information security management systems — Requirements)

3.2ISO/IEC 27002:2013 (Information technology — Security techniques — Code of practice for information security management)

3.3 行政院及所屬各機關資訊安全管理要點

3.4 行政院及所屬各機關資訊安全管理規範

3.5 國家資通訊安全發展方案（106 年至 109 年）

3.6 建立我國資通訊基礎建設安全機制計畫

3.7 行政院國家資通安全會報之「各機關處理資通安全事件危機通報緊急應變作業注意事項」

3.8 行政院國家資通安全會報之「各政府機關(構)落實資安事件危機處理具體執行方案」

3.9 行政院國家資通安全會報之「各政府機關(構)資訊安全責任等級分級作業施行計畫」

3.10 行政院國家資通安全會報技術服務中心之「資通安全管理制度導入手冊」

3.11 行政院所屬各機關資訊業務委外服務作業參考原則

3.12 資通安全管理制度風險評估手冊

3.13 資通安全管理法

4.政策

為了促使本公司各項資訊安全管理制度能貫徹執行、有效運作、監督管理、持續進行，維護本公司重要資訊系統的機密性、完整性與可用性，特頒佈此一資訊安全政策，讓員工於日常工作時有一明確指導原則，保障本公司之權益，並期許全體同仁均能了解、實施與維持，達到本公司營運的目標。

4.1 強化資安訓練，提升資安認知

督導員工落實資訊安全工作，建立「資訊安全，人人有責」的觀念，每年持續進行適當的資訊安全訓練，以提高資訊安全意識。員工如有違反資訊安全相關規定，究其權責依人員獎懲相關規定

辦理。

4.2 落實資訊安全，確保持續營運

由本公司全體員工貫徹執行資訊安全管理制度，以保護資訊資產免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核 ISMS 制度的工作，確保營運持續，達到永續經營的目的。

5.資訊安全目標

本公司執行資訊安全管理制度需達成之資訊安全目標，詳如「I-2-02 資訊安全目標管理程序書」之相關規定。

6.資訊安全政策內容

6.1 本公司各項資訊安全管理規定必須遵守政府相關法規(如:刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等）之規定。

6.2 成立資訊安全管理組織負責資訊安全制度之建立及推動事宜。

6.3 定期實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

6.4 建立主機及網路使用之管理機制，以統籌分配、運用資源。

6.5 新設備建置前，須將風險、安全因素納入考量，防範危害系統安全之情況發生。

6.6 建立資訊機房實體及環境安全防護措施，並定期施以相關保養。

6.7 明確規範網路系統之使用權限，防止未經授權之存取動作。

6.8 訂定資訊安全管理系統內部稽核計畫，定期檢視本公司推行資訊安全管理系統範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正預防措施。

6.9 訂定營運持續管理規定並實際演練，確保本公司業務持續運作。

6.10 本公司所有人員負有維持資訊安全之責任,且應遵守相關之資訊

安全管理規範。

6.11 資訊安全管理系統文件應有明確之管理規範。

7. 管理階層責任

7.1. 管理階層承諾

為使資訊安全管理制度推動順利，管理階層應確實執行下列事項：

7.1.1. 建立資訊安全管理政策、資訊安全目標及計畫。

7.1.2. 成立資訊安全管理委員會，以明訂及文件化資訊安全之角色與責任。

7.1.3. 各單位主管應儘量藉由各種內部公開會議或集會時，向所有人員宣達符合資訊安全目標、法律及法規要求之重要性，以及持續改進之需求。

7.1.4. 提供充分資源，確保能建立、實施操作、監控審查及持續維持改進資訊安全管理制度。

7.1.5. 定期執行資訊安全管理制度之內部稽核作業。

7.1.6. 定期召開資訊安全管理制度之管理階層審查會議。

7.1.7. 決定風險評鑑後之可接受風險等級。

7.2. 資源管理

7.2.1. 資源提供

為確保資訊安全管理制度執行無礙，應決定並提供下列工作之必要資源：

7.2.1.1. 提供建置與維護資訊安全管理制度時所需的人力與資源設備。

7.2.1.2. 提供實施資訊安全管理制度時必要之協助。

7.2.1.3. 確定各項安全程序可配合營運需求。

7.2.1.4. 鑑別並提出法律與法規的要求以及於各項合約上之註明安全義務。

7.2.1.5. 正確應用所有實施的控制措施，以維持適當之安全。

7.2.1.6. 當需要時，進行審查並針對審查結果作適當因應。

7.2.1.7. 當必要時，改進資訊安全管理制度之作業流程，以確保其有效。

7.2.2. 訓練、認知及能力

為確保所有同仁皆有能力執行所要求之工作與符合各項安全要求，應藉由各種途徑取得協助同仁執行教育訓練，包括下列方式：

7.2.2.1. 提供各種能力訓練以滿足該需求。

7.2.2.2. 藉由意見（滿意度）調查、測驗、繳交心得報告及證書取得等方式，評估所提供訓練之有效性。

7.2.2.3. 確保同仁認知其所從事的活動之相關性及重要性，以及他們如何對安全目標之達成有所貢獻。

7.2.2.4. 應留下教育訓練、技能、經驗及評定資格等紀錄，紀錄保存之要求參閱第 7.4.3 節。

8. 資訊安全管理制度之管理階層審查

8.1. 概述

本公司資訊安全管理委員會至少每年召開一次會議，針對本公司現行之資訊安全管理制度進行審查，以確保相關程序的適用性、適切性及有效性皆符合本公司需求，並評估相關政策與目標的改進時機，或是其他的變更需求，且審查結果應留下相關文件與紀錄備查。

8.2. 審查輸入（管理審查之範圍）

管理階層審查至少應包含下列項目：

8.2.1.先前管理審查決議事項之跟催狀況。

8.2.2.有關可能影響 ISMS 的外部與內部問題之變更。

8.2.3. 資訊安全的績效回饋，包含下列趨向：

8.2.3.1. 不符合事項與矯正措施之執行狀況。

8.2.3.2. 監督與量測結果。

8.2.3.3. 內部稽核的結果。

8.2.3.4. 資訊安全目標的實現。

8.2.4. 利害相關團體的回饋。

8.2.5. 風險評鑑的結果與風險處理計畫的狀態。

8.2.6. 持續改進的機會。

8.3. 審查輸出

8.3.1. 管理審查的產出應包含和持續改進機會與資訊安全管理制度（ISMS）的變更需求有關之決定。

8.3.2.管理階層審查之產出建議包含但不限於下列事項之任何決策與措施：

8.3.2.1. ISMS 有效性之改進。

8.3.2.2. 風險評鑑與風險處理計畫之更新。

8.3.2.3. 影響資訊安全之程序與控制之必要時的修改，以回應可能衝擊 ISMS 之內部或外部事件，包括下列事項之變更：

8.3.2.3.1. 各項營運要求。

8.3.2.3.2. 各項安全要求。

8.3.2.3.3. 影響既有各項營運要求之營運過程。

8.3.2.3.4. 法律或法規各項要求。

8.3.2.3.5. 契約的各項義務。

8.3.2.3.6. 風險等級及/或風險接受準則。

8.3.2.4. 資源需求。

8.3.2.5. 控制措施的有效性如何量測之改進。

8.3.3. 組織應保存文件化資訊及管理審查結果的證據。

9. 審查

9.1. 本政策每年應至少評估檢討一次，以反映本公司資訊安全需求、

政府法令法規、外在網路環境變化及資安技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。

9.2. 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及合作廠商，以利共同遵守。

10. 實施

本政策經資訊安全長核准，於公告日施行，並以書面、電子或其他方式通知本公司所屬職員及與本公司連線作業之有關機關（構）、廠商，修正時亦同。