

資訊安全政策

1. 目標：

確保企業持續營運、降低企業資訊安全風險至可接受水準，防範資訊資產遭受各種資訊安全威脅。管理作業準則必須符合促使資訊作業達到機密性(Confidential)、完整性(Integrity)、與可用性(Availability)的特性。

2. 範圍：

資訊資全管制範圍包含茂林光電集團(Global Lighting Technologies Inc.)所屬的相關企業，所有與資訊相關的作業皆是本政策所規範。

資訊安全作業包含：資訊硬體、應用軟體/系統、網路設備與作業、資訊傳遞、資訊資產保全、資訊教育訓練與其他與資訊有關者。

3 組織與職掌：

- 3.1 資訊安全委員會：由集團營運長擔任召集人，定期集會，進行資訊安全計畫審核、批准與資訊安全績效之確認，每年定期向董事會報告資安治理狀況。
- 3.2 資訊安全執行人：由資訊安全委員會指派，負責統合各關係企業之資訊安全作業執行。
- 3.3 執行小組：由資訊安全執行人依據資訊安全計畫需要，徵求關係企業相關負責人員組成，負責各單位資訊安全作業之執行與協調。
- 3.4 資訊部：負責資訊軟硬體、資料保護、安全作業的實際執行。資訊部門主管必須確保擁有足夠的資源與人力，以執行資訊安全作業。
- 3.5 稽核：由公司稽核人員依據稽核原則，定期或不定期進行資訊安全稽核，並將稽核結過提報資訊安全委員會與資訊安全執行人，作為資訊安全改進之依據。

4 資料分類與分級：

- 4.1 依據資訊管理政策與相關作業規範，訂定資訊資料分級與分類。
- 4.2 依據所訂出的資料層級，進行不同層級資料的安全保護流程。

5 使用者帳號與權限管理：

- 5.1 對於資訊持有、資訊系統使用都必須經過申請，經過所屬主管與相關主管核准。
- 5.2 對於申請之使用者帳號與權限，必須配合工作內容與職務授權。
- 5.3 資訊帳號、權限申請與異動必須符合權限作業規範。達到資訊保密的要求。

6 網路通訊安全管理：

- 6.1 除系統管理者之外，嚴禁任何使用者存取或變更網路設備之設定。
- 6.2 原則上鎖定所有網路通訊 port，視業務需要個別開放。任何開放都必須經過適當的申請核准作業。
- 6.3 通訊網路必要的防護設備，如防火牆，防毒裝置等設施必須保持運作，每日點檢後登記於檢查日誌表。
- 6.4 網路通訊上任何異常狀態，必須被記錄，追蹤。並依據資安的緊急、風險程度進行處理。

7 應用系統安全管理：

- 7.1 應用系統的原始程式必須依規定存放於應用程式伺服器。並保持對應的備份檔案。
- 7.2 應用系統的使用必須依據系統資料分類分級，進行權限管控。
- 7.3 應用系統必須有正式環境與測試環境。根據作業需求分別訂定不同的權限。
- 7.4 應用系統的程式上線、修改和維護必須經過完整的驗證測試程序。以確保作業的完整與資料的正確性。

8 資訊安全教育：

- 8.1 資訊安全執行人與各資訊單位，必須利用各種機會宣導資訊安全之概念，以確保集團人員了解資安的重要與公司資安政策。
- 8.2 必須針對公司新進人員，進行資訊安全教育。對公司之資訊作業規定、資訊安全要求，新進人員必須有所瞭解。

9 資料備份與系統備援管理：

- 9.1 資訊資料必須依照資訊分類與分級，進行相對應的資料備份保全作業。
- 9.2 重要資訊設備必須有必要的備援系統，以保持系統的運作。
- 9.3 備份資料的保存必須特別注意其儲運，保存的環境條件，以確保資料保存。
- 9.4 年度必須至少進行一次資料備份與回存驗證作業，並留下完整的驗證文件，並進行後續追蹤改進作業。

10 緊急資訊安全事故處理與災害復原：

- 10.1 資訊安全執行人為資安事故的負責人。資安事故發生時，應由在場人員通知資訊安全執行人。如若連絡不上，應即聯絡工作代理人或同級主管。
- 10.2 資訊安全執行人獲得通知，應衡量資安狀況啟動資安緊急作業。必要時應即刻提報最高主管，取得資源協助。

- 10.3 資安事故後應將事故提報資訊安全委員會。提報內容應包括資安事件狀況、緊急應變處理方式、處理人員、處理結果、事故原因分析、長期解決方案等。
- 10.4 緊急資訊安全事故必須依照相關作業規範執行。
- 10.5 資訊安全執行人必須預估可能的資安傷害，並擬定相對應的作業方式，以降低可能的災害損失。
- 10.6 資訊安全執行人必須動員相關單位，定期根據資安災害計畫進行演練，並檢討可能的改進方案，執行必要的改進。

11 資訊安全的內部稽核：

- 11.1 資安稽核分為三個層次：作業單位自我稽核、資訊安全執行人定期稽核，與稽核人所進行之稽核。
- 11.2 集團內各資訊單位必須依據資訊稽核作業規範，進行自我稽核，並依據稽核結果提報改進措施。
- 11.3 資訊安全執行人定期針對整體資訊安全與各資訊單位進行稽核，並提報缺失與改進方
- 11.4 稽核人員定期或不定期進行資安作業稽核。

12 修改：

- 12.1 本政策經過提報審核後生效。任何補充、修訂，由資訊安全執行人提報資訊安全委員會核准後生效。