

## 資安管理審查委員會&營業秘密委員會

隨著國際金融科技發展，企業面臨之資安風險日益增加，以及為保障同仁辛苦結晶，本公司分別於 2010 年及 2018 年成立「資安管理審查委員會」及「營業秘密委員會」。

### 資安管理審查委員會

每半年進行一次，由委員會成員參加，召開時間約在每年的 4 月及 10 月，負責審查與決議(1) 資訊安全政策、(2) 資訊安全政策目與控制措施之有效性、(3) 提供資訊安全所需的資源等，本公司有關資訊安全風險管理架構、資訊安全政策及具體管理方案，說明如下：

#### 1、政策與原則

- (1) 應考量相關法律規章及營運要求，進行資訊資產之資訊風險評估，確定資訊作業安全需求，建立標準作業程序，採取適當資訊安全管控措施，確保資訊資產安全。
- (2) 依人員職務及職能需求為基礎，建立評估或考核制度，並視實際需要辦理資訊安全教育訓練及宣導活動。
- (3) 資訊資產存取權限之賦予，應業務需求並考量最小權限、權責區隔及獨立性審查。
- (4) 建立資訊安全事故管理程序，以確保事故妥善回應、控制與處理，並訂定業務持續計畫並定期演練，以確保資訊系統或資訊服務持續運作。
- (5) 依據個人資料保護法與智慧財產法之相關規定，審慎處理及保護個人資料與智慧財產權。
- (6) 定期執行資訊安全稽核作業以確保資訊安全管理制度落實。
- (7) 違反本政策與資訊安全相關規範，依相關法規或本公司人事規定辦理。
- (8) 為確保本公司同仁皆知悉本公司資訊安全要求，另訂定「資訊安全宣言」告知本公司同仁遵悉。

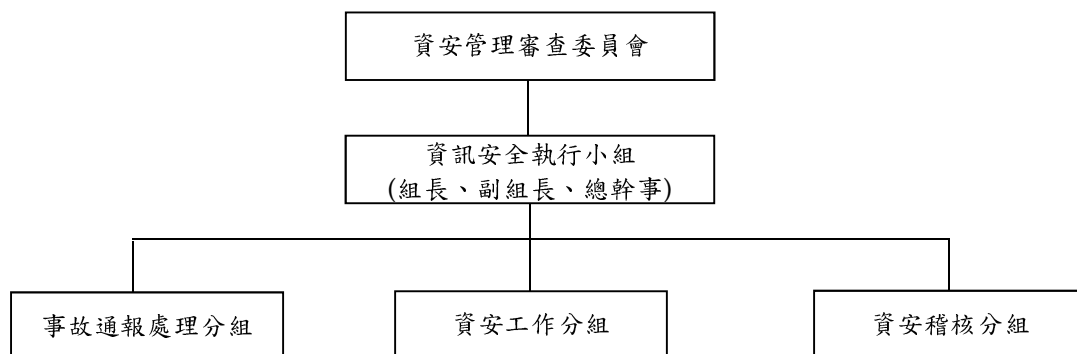
#### 資訊安全宣言

本公司資訊安全工作之最終目標在於：透過對人員、作業及資訊科技之管理，確保本公司關鍵業務資訊處理作業能有效運作，防範資訊處理作業過程中發生影響關鍵業務運作之資訊機密性、完整性及可用性之安全事故，支持公司成為全球光電製造中心之目標。

本公司之資訊安全工作係以系統化風險評估及風險管理為基礎，以管理及技術並重方式實施風險控制措施，並由同仁落實於日常工作中，共同努力以實現本公司下述之資訊安全目標：

- 關鍵業務之相關資訊保護完全符合公司要求與相關法令規範
- 關鍵業務與支援行政工作之資訊處理過程與結果要完全正確
- 資訊系統與資訊處理作業服務不間斷

## 2、組織架構



## 3、成員及工作職掌

### (1) 委員會成員

總經理、資訊中心副總、稽核主管、智權法務處處長、智權法務處法務部經理。

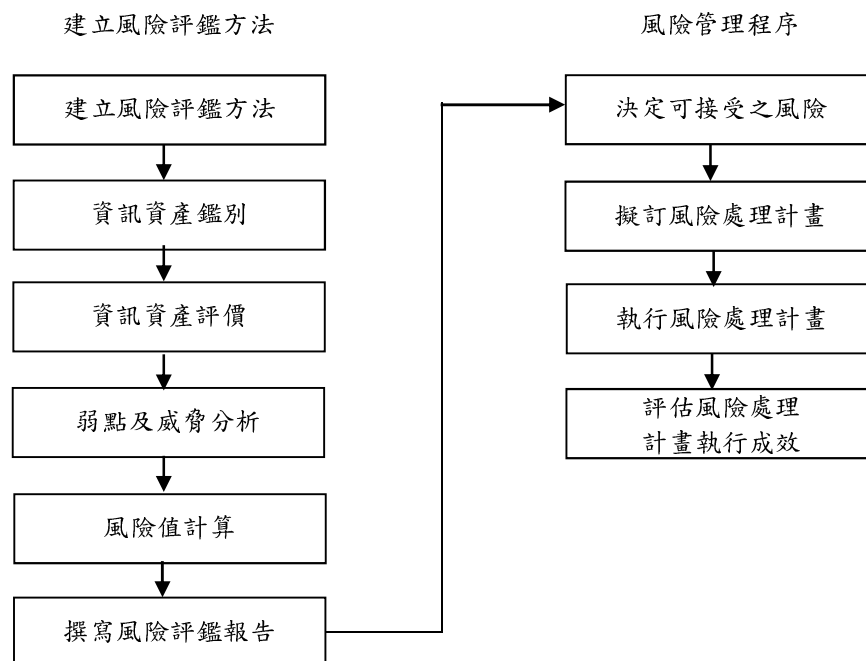
### (2) 執行小組成員

小組組長、副組長、總幹事

### (3) 工作職掌

職務/角色	工作職掌
資安管理審查委員會主席	<ul style="list-style-type: none"> <li>● 負責審查與決議本公司資訊安全管理相關事項。</li> <li>● 審查與核准資訊安全政策。</li> <li>● 審查資訊安全政策目標與控制措施之有效性。</li> <li>● 審查資訊安全所需的資源項目。</li> </ul>
資安管理審查委員會召集人	<ul style="list-style-type: none"> <li>● 負責審查與決議本公司資訊安全管理相關事項。</li> <li>● 審查與核准資訊安全政策。</li> <li>● 審查資訊安全政策目標與控制措施之有效性。</li> <li>● 審查資訊安全所需的資源項目。</li> <li>● 協調資訊安全相關工作。</li> <li>● 持續改善資訊安全管理制度。</li> </ul>
資安管理審查委員會委員	<ul style="list-style-type: none"> <li>● 負責審查與決議本公司資訊安全管理相關事項。</li> <li>● 審查與核准資訊安全政策。</li> <li>● 審查資訊安全政策目標與控制措施之有效性。</li> <li>● 審查資訊安全所需的資源項目。</li> </ul>
資安執行小組組長	<ul style="list-style-type: none"> <li>● 依據資訊安全特定角色職責遴選適當人員。</li> <li>● 維護資訊安全認知。</li> <li>● 協調資訊安全相關工作。</li> <li>● 確認資訊安全風險及實施風險處理。</li> <li>● 辦理資訊安全管理制度之獨立稽核。</li> <li>● 持續改善資訊安全管理制度。</li> </ul>
資安執行小組副組長	<ul style="list-style-type: none"> <li>● 協助組長依據資訊安全特定角色職責遴選適當人員。</li> <li>● 協助組長維護資訊安全認知。</li> <li>● 協助組長協調資訊安全相關工作。</li> <li>● 協助組長確認資訊安全風險及實施風險處理。</li> <li>● 協助組長辦理資訊安全管理制度之獨立稽核。</li> <li>● 協助組長持續改善資訊安全管理制度。</li> </ul>

#### 4、風險評鑑程序與風險管理流程



#### 5、風險評鑑時機與方法

##### (1) 風險評鑑時機

- 風險評鑑作業每半年執行乙次，並由資訊安全執行小組組長決定評鑑範圍。
- 如遇組織變更、作業流程變更、資訊資產異動或發生重大資訊安全事故等，得針對特定範圍內之資訊資產進行風險評鑑。

##### (2) 風險評鑑方法

- 資訊資產風險值是以資訊資產價值、資產弱點之脆弱度、面臨威脅發生機率及影響面所構成，並將資訊資產價值、弱點脆弱度及威脅發生機率，三項評分相乘，並依威脅對機密性、完整性、可用性產生之影響計算風險值。
- 資訊資產鑑別（識別清查），依據【資訊資產管理作業流程及程序】(PIS090003)執行所轄之資訊資產清查作業。
- 資訊資產評價（評估價值），由資訊資產擁有者針對資產之機密性、完整性、可用性，並考量組織特性與法令、法規要求進行評估。

#### 6、管理制度/內部稽核/定期呈報董事會/預防措施

##### (1) 稽核頻率

每半年辦理資訊安全內部稽核作業(可視實際情況整合於公司內部稽核活動實施)，並視需要採取針對資訊安全事故、資訊系統的重大變更等特定目的之不定期稽核。

##### (2) 稽核人員要求

為確保稽核過程的客觀性與獨立性，避免稽核自身工作。稽核人員需有資訊安全制度稽核經驗或曾參與資安稽核相關訓練(含公司內部訓練課程)。

### (3) 稽核計畫

- 應事前規劃並編製資訊安全稽核計畫，以作為執行稽核指導綱要，內容應包括：稽核依據、範圍、程序、人員、項目、預定時程等，由資安管理審查委員會召集人核准後執行。稽核計畫格式可參考資訊安全管理制度文件編號及撰寫格式標準。
- 資訊安全稽核若整合於公司內部稽核活動實施時，資安稽核計畫應於資安管理審查委員會召集人核准後，並提供稽核室納入公司內稽計畫中呈核並施行。

### (4) 呈報至董事會

有關電腦化資訊系統處理及資通安全檢查部分，已於 107 年 11 月 12 日呈報至董事會知悉，並針對缺失部份做出建議，後續追蹤已完成改善。

### (5) 預防措施

截至目前為止，公司尚無投保資安險，惟本公司對資安治理及強化防衛能力不餘遺力，尚無發現侵害供應商或客戶隱私權、機密資料外洩或系統被入侵等情事。

資安執行小組不定期進行業務持續演練及資安釣魚郵件演練等；演練系統發生異常時進行復原的程序，並定期進行稽核；遭釣魚同仁則需再次接受資安釣魚郵件的課程教育訓練及事後測驗，有效減少同仁遭至病毒攻擊、或資料遭到加密綁架、或橫向感染造成機密資料外洩、或系統遭到入侵癱瘓等。

## 營業秘密委員會

資安固然重要，也要保障公司之營業秘密及公司持有第三人之機密資料的安全，暨確保同仁工作成果、維持公司競爭力及避免公司重要資訊外洩，於民國 107 年 1 月 26 日組成「營業秘密委員會」。

### 1、組織架構

由總經理、資訊中心、稽核室、人資中心、智權法務處及支援中心等單位的最高主管組成，每個月定期召開一次月會。

### 2、保護範疇及權責

包括本公司及子公司所有尚未公開揭露、或被認定為秘密並具有敏感性或重要性之資訊、文件、檔案、配方、產品、樣品等機密資訊。針對違反營業秘密保護辦法之違規事件，均需由營業秘密委員會根據個案情節輕重，並決議相關懲處之方式。

### 3、實施教育訓練

- (1) 藉由定期發行之電子報，對公司全體同仁進行教育訓練以及法規宣導。
- (2) 不定期的安排相關專業人士/講師對特定員工進行教育訓練。