宇達光學股份有限公司Unidar Technologies, Inc.

資訊安全政策

文件編號：ISMS-A-001

機密等級：一般

版　　次：1.1

發行日期：115.1.6

本文件歷次變更紀錄：

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	114.12.11		陳慧穎	初版，依據ISO 27001:2022
1.1	115.1.6		陳慧穎	頁首文件機密等級，由4級改為3級，並修正部分文字。

目　　錄

1. 目的

依據ISO 27001:2022標準，確保宇達光學股份有限公司Unidar Technologies, Inc.(以下簡稱本公司)所屬之資訊資產的機密性、完整性及可用性，並符合本地法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，特訂定本資訊安全政策（以下簡稱本政策）作為資訊安全管理之準則。

2. 適用範圍

為避免因人為疏失、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，對本公司造成各種可能之風險及危害，資訊安全政策範疇涵蓋四大控制措施領域，分別為「組織控制措施」、「人員控制措施」、「實體控制措施」及「技術控制措施」，由管理階層核准、發布及傳達予相關人員和相關關注方，視需要發展出各項主題政策，同時考量資訊安全管理系統範圍內之氣候變遷影響議題，包括組織之內外議題以及關注方對於氣候變遷提出的要求。

資訊安全控制措施主題，舉例如下：

1. 資訊安全組織及職責。
2. 資訊資產管理與風險評鑑。
3. 資訊存取控制及端點裝置之安全。

4. 實體及環境安全。

5. 營運持續。

6. 網路安全管理及連網安全。

7. 資訊安全事故管理。

8. 運作管理與資料備份。

9. 密碼技術及金鑰管理。

10. 技術脆弱性管理。

11. 系統(軟體)安全開發。

12. 人員安全與教育訓練。

3. 權責

3.1 本公司應成立資訊安全組織統籌資訊安全事項推動。

3.2 管理階層應積極參與資訊安全管理制度，提供對資訊安全管理制度之支持。

3.3 本公司全體人員、委外服務廠商與訪客等皆應遵守本政策。

3.4 本公司全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

3.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任

或依本公司之相關規定進行議處。

4. 定義

ISMS(Information Security Management System)資訊安全管理系統，遵循ISO 27001:2022標準，以系統化方法對資訊安全風險進行分析及控管，以確保資訊系統及相關作業之機密性、完整性與可用性。

5. 目標

5.1 為維護本公司資訊資產之機密性、完整性與可用性，建立安全及可信賴之資訊作業環境。並保障使用者資料隱私之安全，期由本公司全體同仁共同努力，以達成下列目標：

5.1.1 保護本公司業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

5.1.2 保護本公司業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

5.1.3 建立本公司業務營運持續計畫，以確保本公司業務服務之持續運作。

5.1.4 確保本公司業務服務執行須符合相關法令或法規之要求。

5.2 公司規劃、實作及控制資訊安全要求事項所需過程之相關準則，並實作控管措施，以「ISMS-D-011適用性聲明書」作為文件化資訊紀錄，

對控制所規劃之變更，需審查非預期變更之後果，必要時採取行動以減輕任何負面效果，藉此確保與資訊安全管理系統相關的外部提供的過程、產品或服務受到控制。當公司確定需要對資訊安全管理系統變更時，應以規劃的方式執行變更。

5.3 本政策至少應每年評估一次，以反映相關法令、技術及業務等最新發展現況。

5.4 本公司應考量內、外部議題及利害相關者要求，定訂適當之資訊安全管理制度實施範圍，經由管理階層審核、確認後實行。

5.5 資訊安全管理制度實施範圍應定期或不定期視內、外部環境之變更，如：法令法規之要求、組織異動、資安事件發生、管理制度落實狀況等因素，於管理審查會議進行檢視調整。

5.6 關於本公司資訊安全管理制度落實情形，經有效性量測確認資訊安全管理制度已達資訊安全政策目標。本政策經資訊安全委員會召集人核定後實施，得以書面、電子或其他方式通知同仁、與本公司連線作業之有關機關（構）及提供資訊服務之廠商，修正時亦同。

6. 參考文件

ISO國際組織所頒佈之27001規範，2022年版本。

7. 相關表單

ISMS-D-011適用性聲明書。