資訊安全教育訓練範本

1. 公司資安政策與規範

- **內容**：介紹公司的資安政策、守則及相關規範，確保員工了解並遵守。
- **目的**：建立統一的資安標準，防止資訊洩漏和不當使用。

2. 資安基礎知識

- **內容**：涵蓋資訊安全的基本概念，如機密性、完整性、可用性（CIA 三元組）。
- **目的**：讓員工理解資安的重要性及基本原則。

3. 資安風險與管理

- **內容**：介紹常見的資安風險、風險評估方法及管理策略。
- **目的**：提高員工的風險意識，學會識別和應對潛在威脅。

4. 安全操作指南

- **內容**：具體的安全操作流程，如資料存取、設備使用及網路連接。
- **目的**：確保日常操作中遵循安全規範，減少人為錯誤。

5. 密碼管理與認證

- **內容**：強調強密碼的重要性、多因素認證的使用及密碼管理工具的介紹。
- **目的**：加強帳戶安全，防止未授權存取。

6. 資訊保護與隱私

- **內容**：介紹個人資料保護法規（如 GDPR）、資料分類及處理方式。
- **目的**：確保員工在處理敏感資訊時遵循法律和公司規定。

7. 網路安全

- **內容**：涵蓋防火牆、入侵偵測系統（IDS）、虛擬私人網路（VPN）等技術。
- **目的**：保護公司網路免受外部攻擊和未經授權的存取。

8. 電子郵件與釣魚攻擊防範

- **內容**：識別釣魚郵件的特徵、防範措施及應對方法。
- **目的**：減少員工因釣魚攻擊而洩漏敏感資訊的風險。

9. 行動裝置安全

- **內容**：行動裝置的安全使用指南，如裝置加密、遠端擦除及應用程式管理。
- **目的**：保護員工使用行動裝置時的資訊安全。

10. 事故應變與報告流程

- **內容**：介紹資安事件的應變計劃、報告流程及責任分工。
- **目的**：確保在發生資安事件時能迅速有效地應對，減少損失。

附加資源

- **互動式訓練模組**：透過案例分析和模擬演練，提升員工的實務操作能力。
- **資安手冊**：詳細記錄各項資安政策和操作指南，供員工隨時查閱。
- **定期測驗與評估**：檢視員工對資安知識的掌握程度，並持續改進培訓內容。