1 資安情資監控與應變作業程序

1.1 目的

確保企業資通系統的安全性，藉由監控、評估與應對資安威脅與事件，維持系統及資料完整性。

1.2 責任單位

資訊安全部門

1.3 執行頻率

- 惡意偵察或情蒐活動監控：**持續運行**
- 安全漏洞評估：**每季一次**

1.4 執行方法

1. 建立並持續運行監控系統，偵測與記錄任何惡意偵察或情蒐活動。
2. 每季執行資通系統安全漏洞評估，並記錄所有發現之漏洞。
3. 識別並記錄可能使安全控制措施無效或利用漏洞之方法（含技術與策略）。
4. 監控並收集惡意程式相關資訊，如惡意指令、中繼站位址及控制方式。

1.5 記錄保存方式

所有監控紀錄、安全評估報告及相關文件須保存至少 **五年**，由資訊安全部門統一管理。

---

2 資通安全情資辨識、收集與管理作業程序

2.1 目的

確保企業持續辨識、收集與管理資安情資，以提升系統防護能力並降低安全事件風險。

2.2 責任單位

資訊安全部門

2.3 執行頻率

- 情資收集與資料庫更新：**持續性作業**
- 資料庫定期審核：**每半年一次**
- 全面性審查與程序更新：**每年一次**

2.4 執行方法

1. 建立綜合資料庫，收集並維護下列情資：
    - 惡意偵察或情蒐活動資訊
    - 系統安全漏洞資訊
    - 使安全控制措施失效或利用漏洞之方法
    - 惡意程式資訊（指令、控制點、連線資訊等）
    - 資安事件造成之損害或潛在影響
    - 偵測、預防、因應或降低前述風險之措施資訊
    - 其他相關技術性資訊
2. 半年一次審核並更新資料庫，確保情資之及時性與準確性。
3. 每年依蒐集情資制定或更新應對方案，內容至少涵蓋：
    - 系統漏洞修補與惡意活動監控
    - 定期安全評估與滲透測試
    - 發現新漏洞或惡意程式時即時通報並處理
4. 定期培訓相關人員，確保具備識別與因應各類資安情資之能力。

2.5 記錄保存方式

情資收集、處理及應對方案文件保存至少 **五年**，由資訊安全部門存檔維護。

---

3 情資分析與應變作業程序

3.1 目的

及時辨識接收情資之可靠性與時效性，進行威脅弱點分析並採取預防或應變措施，以降低安全風險。

3.2 責任單位

資訊安全部門

3.3 執行頻率

- 接收新情資時：**立即啟動**
- 分析與應變措施制定：**48 小時內完成**

3.4 執行方法

1. 辨識情資來源可靠性與時效性（來源信譽度、更新速度、歷史準確性）。
2. 執行威脅與弱點分析：漏洞掃描、行為分析、威脅情報庫對比等。
3. 研判潛在風險並取得資安主管核准。
4. 依研判結果制定並實施預防或應變措施，例如：
    - 系統補丁更新
    - 存取控制調整
    - 員工安全教育
5. 指定人員監控執行效果並持續改進。

3.5 記錄保存方式

分析報告與應變措施記錄以電子方式保存至少 **三年**，由資訊安全部門管理。

---

4 資安事件應變作業程序

4.1 目的

確保企業有效識別與管理資安威脅，減少可能損害。

4.2 責任單位

資訊安全部門

4.3 執行頻率

持續進行

4.4 執行方法

1. 收集並分析惡意偵察或情蒐資訊（例：網路流量、異常訪問）。
2. 每季進行漏洞掃描並記錄結果。
3. 更新並記錄可能使安全控制失效之方法及風險應對策略。
4. 擷取並保存惡意程式資訊（指令、不明網域）。
5. 評估並記錄每次事件之損害或負面影響。
6. 針對已識別威脅或漏洞實施防範措施（防火牆規則、教育訓練等）。
7. 持續收集其他技術性資訊以保持警覺。

4.5 記錄保存方式

所有事件相關資料及活動記錄保存至少 **三年**，由資訊安全部門集中管理。

---

5 情資接收與安全維護作業程序

5.1 目的

確保所有接收情資獲得適當安全保護，防止外洩或未經授權存取與竄改。

5.2 責任單位

資訊安全管理部門

5.3 執行頻率

每次接收情資時

5.4 執行方法

1. 接收後立即分類，識別敏感資料及受法規保護資訊。
2. 採取安全維護措施：加密、存取控制、資料屏蔽等，確保機密性、完整性、可用性。
3. 設置自動化監控，偵測未經授權存取或資料竄改；異常時立即通報並處理。
4. 流程結束後將結果記錄於安全維護活動報告。

5.5 記錄保存方式

所有相關記錄保存至少 **三年**，由資訊安全管理部門保存與管理。

---

6 情資分享作業程序

6.1 目的

確保情資分享過程符合法規與公司政策，避免未經授權洩漏，並在符合主管機關要求下維持分享之靈活性。

6.2 責任單位

資訊安全管理部門（含法務部資安合規組對特定對象分享之審核）

6.3 執行頻率

每次情資分享前

6.4 執行方法

6.4.1 常規分享審查

1. 分享前審核內容，確認不含：
    - 個人、法人或團體營業秘密或經營資訊
    - 依法應保密或限制公開之資訊
2. 若資訊中包含不得分享內容，應拆分並僅分享不受限制部分。

6.4.2 法規例外處理

符合下列任一情形得分享，惟須留存書面記錄：

- 法規另有規定
- 公益或保護人民生命、身體、健康之必要
- 當事人同意

6.4.3 主管機關指定 / 同意模式

1. 需依主管機關指定方式操作；若無法依指定方式，分享前須取得書面同意。
2. 與未適用資通安全管理法之個人、法人或團體分享時，法務部資安合規組須先取得主管機關或中央目的事業主管機關書面同意。
3. 經核准後得以書面、傳真、電子郵件、資訊系統或其他經核准方式分享，並完整記錄分享內容與方式。

6.5 安全維護措施

1. 分享前詳盡分析與整合情資，並依敏感性進行遮蔽或匿名化。
2. 實施存取權控管及加密，防止未經授權存取與竄改。
3. 建立審計追蹤，確保分享流程可追溯。

6.6 記錄保存方式

所有審查、分析、分享與主管機關溝通之完整記錄保存至少 **五年**，由資訊安全管理部門（合規組）保存與管理。
