經濟部商業發展署
Administration of Commerce, MOEA

經濟部商業發展署

零售業
個資法遵實務與資訊安全
說明會

資訊工業策進會
科技法律研究所、資安科技研究所

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

www.iii.org.tw

資訊工業策進會 Institute for Information Industry

大　綱

壹　個資法遵實務說明

- 法規架構
- 適用零售業安維辦法之條件
- 各類個資管理與保護措施實務

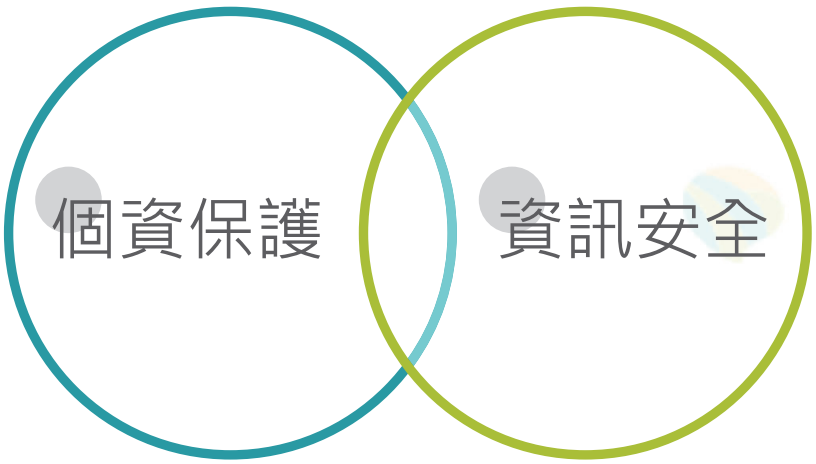
貳　如何採取合規之措施（零售業安維辦法第10條要求）

- 資安防護之個資法遵要求、依據與重點
- 資安措施執行建議

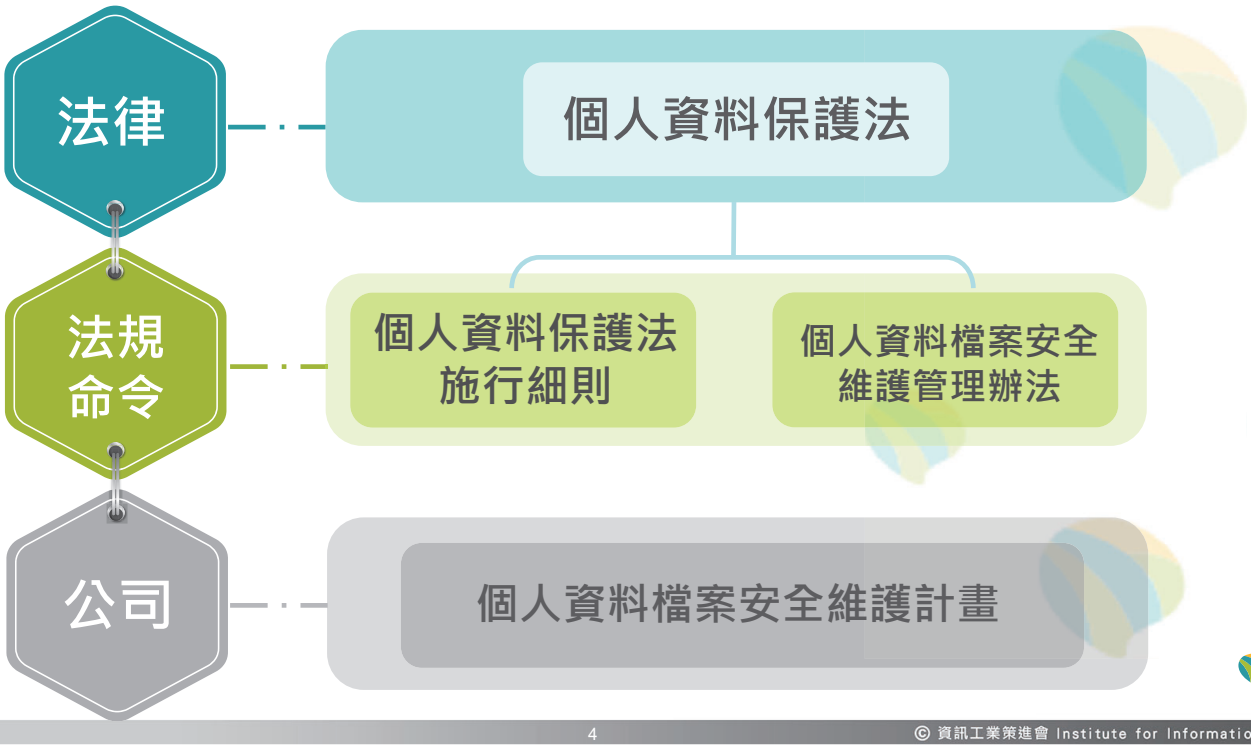
壹. 個資法遵實務說明

個資保護與資訊安全之關係

個人資料保護與資訊安全間，二者有**部分內容重疊**
現今數位化時代需**仰賴資訊安全，以落實個資保護**



個人資料保護法規架構



適當之安全措施

個人資料保護法第27條第1項

> 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

個資安全維護措施*：技術面及組織面

- 配置管理人員及相當資源
- 界定個人資料之範圍
- 個人資料之風險評估及管理機制
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序
- 資料安全管理及人員管理
- 認知宣導及教育訓練
- 設備安全管理
- 資料安全稽核機制
- 使用紀錄、軌跡資料及證據保存
- 個人資料安全維護之整體持續改善

*個人資料保護法施行細則第12條第2項

適用零售業個資安維辦法之條件

安全維護辦法第3條

> 本辦法所稱零售業（以下簡稱業者），指非其他中央目的事業主管機關主管之從事實體店面，或實體店面兼營網際網路方式銷售商品之零售，已辦理公司、有限合夥或商業設立登記，且資本額達新臺幣一千萬元以上，並有招募會員或可取得交易對象個人資料之業者，或受經濟部指定之公司、有限合夥或商業。但不包括應經特許、許可或受專門管理法令規範之行業。

1. 實體店面、實體兼營網路
2. 公司登記、商業登記、有限合夥登記
3. 資本額達NT 1,000萬以上(含)
4. 招募會員、交易對象個資

例：訂單（姓名、電話等）

個人資料之蒐集、處理及利用

蒐集

指以任何取得個人資料的方式。
- 直接蒐集、間接蒐集

處理

為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

利用

指將蒐集之個人資料為處理以外之使用。

1.制定安全維護計畫

安全維護辦法第6條

➢ 計畫範本與說明：
https://www.aoc.gov.tw/subclass/cont/145

• 業者應依本辦法規定訂定安全維護計畫，載明下列事項：

1. 個人資料蒐集、處理及利用之內部管理程序
2. 個人資料之範圍
3. 資料安全管理及人員管理
4. 認知宣導及教育訓練
5. 事故之預防、通報及應變機制
6. 設備安全管理
7. 資料安全稽核機制
8. 使用紀錄、軌跡資料及證據保存
9. 業務終止後，個人資料處理方法
10. 個人資料安全維護之整體持續改善方案

2.指定專責人員

安全維護辦法第5條

> 業者應指定安全維護計畫之專責人員，負責規劃、訂定、修正、執行安全維護計畫及其他相關事項，並定期向業者之代表人或經其授權之人員提出報告。

專責人員

- 至少指定一位員工作為個資專責人員 合法標準
- ➢ 業務有涉及個資的部門設有個資代表或負責人員
  適合業務較繁雜之公司
- ➢ 設立個資保護團隊/小組，組成包含公司管理階層與專責人員
  適合規模較大之公司

圖示來源：Flaticon.com

3.告知當事人事項(1/3)

安全維護辦法第8條第1項

> 業者蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，及符合前條第一項所定之類別及範圍。

告知事項 → 隱私權政策、聲明條款等

直接蒐集
個資法第8條

間接蒐集
個資法第9條

1. 非公務機關名稱
2. 蒐集之目的
3. 個人資料之類別
4. 個人資料利用之期間、地區、對象及方式
5. 當事人依第三條規定得行使之權利及方式
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響（僅直接蒐集）

3.告知當事人事項(2/3)

範本僅供參考

隱私權政策範本
（以加入會員且有提供網購為例）

○○股份有限公司（以下稱本公司）依據個人資料保護法第8條第1項規定，向您告知下列事項，敬請詳閱。

一、蒐集之目的：消費者服務與管理、行銷、消費習慣分析、網路購物、商品配送。

二、個人資料之類別：姓名、出生年月日、電子郵件、電話號碼、通訊地址。

三、個人資料利用之期間、地區、對象及方式：

（一）期間：即日起自本公司業務終止或您要求刪除個人資料。

（二）地區：中華民國境內。 → 若有國際傳輸之情形，應說明傳輸之地區。

（三）對象：○○股份有限公司（物流公司）、○○股份有限公司（資訊公司）。

（四）方式：以書面或電子之形式處理、利用。

3.告知當事人事項(3/3)

範本僅供參考

隱私權政策範本（續）

四、依據個人資料保護法第 3 條規定，您可以透過客服電話（0800-xxxxxx）、客服電子信箱（xxx@xxx.com.tw）或門市服務人員，向本公司行使下列權利：

（一）查詢或請求閱覽。

（二）請求製給複製本。

（三）請求補充或更正。

（四）請求停止蒐集、處理或利用。

（五）請求刪除。

五、您可以自由選擇是否要提供個人資料，若您不願意提供個人資料，則無法成為本公司會員亦無法於網站購買商品。

4.蒐集個資之注意事項

個資法第5條

> 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

蒐集個資常見問題

1. 蒐集過多個資，例如：會員是否要身分證字號？
2. 預先蒐集未來業務上可能會用到的個資
3. 未實際蒐集告知事項中提到的個資類別
4. 告知事項遺漏有蒐集的個資類別
5. 未在當事人提供個資前進行告知

5.盤點個人資料

安維辦法第7條第1項

> 應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。

個資盤點流程

1.以部門單位，釐清所有業務內容。

2.歸納出業務內容有涉及個資者。

➢ 建議進一步畫出作業流程圖

3.確認目前個資管理、保存等狀態。

4.製作並填寫個人資料盤點表。

5.每年至少一次重新盤點。

➢ 個人資料盤點表範本：
https://www.aoc.gov.tw/subclass/list/18

個人資料盤點表

- 個人資料檔案名稱
- 個人資料類型
- 個人資料項目
- 個人資料筆數
- 特定目的
- 法定情形
- 取得來源
- 保存方式與期限等

6.個資風險評估

個資法施行細則第12條第2項第3款

> 個人資料之風險評估及管理機制

風險評估方式

1.根據個資盤點結果，評估各項個資檔案風險。

➢ 評估各項個資發生事故所造成之影響程度（衝擊程度）及發生事故之可能性。

2.對評估出高風險的個資，採取因應措施，以降低風險。

3.每年至少一次重新評估。

➢ 個人資料風險評估表範本：
https://www.aoc.gov.tw/subclass/list/18

衝擊程度

- 個資敏感度
- 個資數量
- 對當事人的影響
- 對公司的影響

發生可能性

- 現行控管措施
- 過往發現缺失

7.刪除、銷毀個人資料

安全維護辦法第7條第2項

業者經定期檢視發現有非屬特定目的必要範圍內或特定目的消失、期限屆至而無保存必要之個人資料，應予刪除、銷毀、停止蒐集、處理、利用或其他適當之處置。

刪除、銷毀個資程序

1.透過定期盤點，發現無存必要之個資。

- 過度蒐集（非必要範圍內）、已無用途（特定目的消失）、保存期滿等

2.將個資刪除、銷毀或其他適當處理。

3.保存刪除和銷毀的紀錄。

8.當事人拒絕行銷

個資法第20條第2項（安維辦法第20條第2項）

當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

消費者經常投訴，已表達不願收到行銷訊息，仍然會收到。

未停止行銷常見原因

- 第一線人員未確實轉達消費者的需求。
- 未標記或未列入拒絕行銷名單。
- 系統已固定排程發送行銷訊息。

9.個資教育訓練

安維辦法第11條

業者訂定第六條第四款所定認知宣導及教育訓練計畫，應包括定期對所屬人員進行個人資料保護認知宣導與教育訓練，使其明瞭相關法令之規定、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及管理措施。

辦理時間

1. 新進人員入職實施教育訓練
2. 每年至少一次實施例行性教育訓練

訓練內容

1. 基礎個資法規（個資法、安維辦法）
2. 公司管理制度與規範
3. 人員職務範圍與注意事項

10.人員管理措施(1/2)

安全維護辦法第9條

業者訂定第六條第三款所定資料安全管理及人員管理之措施，應包括下列事項：

1. 權限設定

- 建立關於人員權限之管理規定，並讓人員可知道規定內容。
- 依據實際的業務需求，設定人員相對應的權限，避免接觸到與個人業務無關的個資。
- 定期（建議至少每月）確認人員權限的必要性及適當性，例如人員是否有職務異動或離職，但未調整權限。

➢ 經常有公司因疏失未刪除離職人員的權限，導致閒置帳號遭利用而個資外洩。

10.人員管理措施(2/2)

2. 業務負責人

- 檢視各部門的業務之性質，確認業務內容是否有涉及到個資。
- 有涉及到個資的業務，應有人員負責作業內容。

3. 保管與保密

例如：紙本、電腦、隨身碟等

- 要求人員妥善保管儲存個資的媒介物，例如應存放上鎖之置物櫃。
- 人員入職時簽署保密切結書，明確規範不能揭露任何業務上知悉之個資。

11.委託監督(1/2)

安全維護辦法第19條

業者委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第8條規定對受託人為適當之監督，並於委託契約或相關文件中，明確約定其內容。

契約約定及監督之內容

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
2. 受託者採取的安全措施。
3. 如有複委託，複委託之對象。
4. 受託者違反個資相關法規時，應向委託機關通知之事項及採行之補救措施。
5. 必須要委託機關同意方能執行之事項。（保留指示事項）
6. 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

11.委託監督(2/2)

委託監督檢核表（範本）

範本僅供參考

法律規範事項	檢核事項	查核結果
預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間	1.實際取得的個資內容	符合
	2.實際利用個資情形	不符合
	3.實際保存個資的時間	
個資保護安全維護措施	1.制定個資管理程序	
	2.個資盤點	
	3.風險評估	
	4.資訊安全措施	
	5.人員管理措施	
	……	
複委託	1.複委託的對象	
通知及補救措施	1.預擬通知方式	
……	……	

12.紀錄保存

安全維護辦法第15條第1項

業者訂定第六條第八款所定使用紀錄、軌跡資料及證據保存之措施，應包括下列事項：

- 留存個人資料使用紀錄
- 留存自動化機器設備之軌跡資料或其他相關之證據資料

建議保存項目 至少保存5年

個資使用紀錄

1. 客服
2. 消費習慣統計
3. 行銷

軌跡資料（Log）

1. 存取個資
2. 權限異動
3. 系統異常事件

13.事故之預防、通報及應變(1/2)

安全維護辦法第12條第1項

業者訂定第六條第五款所定事故之預防、通報及應變機制，應包括下列事項：

發生事故

應變措施

採取控制措施，防止事故或損害擴大

通知

1. 於得知事故起，72小時內通報主管機關
2. 查明事故及損害，通知當事人或其法定代理人

務必確保公司內部流程 可於72小時內完成

改善

查明事故根因，並訂定預防及改進措施

圖示來源：Flaticon.com

13.事故之預防、通報及應變(2/2)

個資事故通知範本

範本僅供參考

個資遭侵害之事實，例如：會員資料庫遭駭客入侵

親愛的顧客您好：

近期本公司因〇〇〇而發生個人資料外洩情事，導致您留存於本公司的個人資料（包含姓名、電話號碼、通訊地址等）受到影響。

本公司已採取〇〇〇、〇〇〇等措施，並已將本次事故相關資訊通報予主管機關。本公司未來會持續加強個資與資安的保護管理，以保障消費者的個資安全。

如果您對本次事故有任何疑問，請洽本公司客服專線（0800-000000）或電子信箱（xxx@xxx.com.tw）與我們聯絡。

14.資料安全稽核機制

安全維護辦法第14條第1項

- 應指定資料安全稽核之查核人員，定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向業者之代表人或經其授權之人員提出報告。
- 同條第3項：業者依第五條規定指定之專責人員與第一項規定之查核人員，不得為同一人。

查核人員

1. 查核公司內部執行個資管理與保護措施之結果。
2. 製作稽核結果報告。
3. 向公司代表人或高階管理層報告稽核結果。

➢ 各單位應修正稽核發現的缺失。

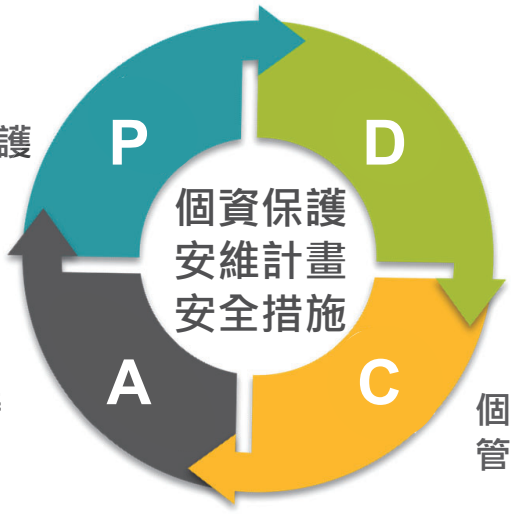
⚠ 查核人員與專責人員不得為同一人

圖示來源：Flaticon.com

15.持續改善

安全維護辦法第17條

業者訂定第六條第十款所定個人資料安全維護之整體持續改善方案，每年應參酌安全維護計畫執行狀況、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性；必要時應予修正。



Plan 計畫
規劃
個人資料保護與管理制度

Do 執行
實施
個人資料保護與管理制度

Check 評估
評估
個人資料保護與管理制度有效性

Act 改善
持續
監督與改善

罰則(1/4)

個人資料保護法第47條

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之。

裁罰並限期改正 | 處罰5萬-50萬，並限期改正，屆期未改正者，按次處罰

公司違反

- 無法定事由而蒐集、處理或利用特種個資
- 無法定事由而蒐集或處理一般個資
- 個資利用逾越特定目的
- 違反中央目的事業主管機關對國際傳輸之限制

罰則(2/4)

個人資料保護法第48條第1項

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰。

限期改正 | 先限期改正，屆期未改正者，按次處罰2萬-20萬

公司未落實

- 未於蒐集資料時，落實告知當事人事項，包含直接蒐集與間接蒐集
- 拒絕或未讓當事人依個資法第3條行使權利
- 發生個資安維案件時，未通知當事人
- 當事人表示拒絕行銷時，未立即停止行銷
- 首次行銷時，未提供當事人拒絕方式，或未支付所需費用

罰則(3/4)

個人資料保護法第48條第2項、第3項

非公務機關違反第27條第1項或未依第2項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法.....

裁罰並限期改正 | 處罰2萬-200萬，並限期改正，屆期未改正者，按次處罰

公司未執行
- 未採取適當之安全維護措施
- 未訂定個資安全維護計畫

屆期未改正者或情節重大者處罰金額為15萬-1500萬

罰則(4/4)

個人資料保護法

- 第49條：非公務機關無正當理由違反第22條第4項規定者.....
- 第50條：非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

其他裁罰事由

處罰2萬-20萬	規避、妨礙或拒絕主管機關進行行政檢查或行政調查
受與公司同一額度金額之處罰	公司之管理人、代表人或其他有代表權人，除非能證明已盡到防止義務

THANK YOU

數位轉型．軟體技術．資安產業．數位經濟

貳. 如何採取合規之措施（零售業安維辦法第10條要求）

如何採取合規之資安措施
(零售業個人資料檔案安全維護管理辦法第十條要求)

財團法人資訊工業策進會
資安科技研究所 張時鳴

大綱

- **資安防護之個資法遵要求、依據與重點**
  - 個人資料保護法及施行細則
  - 零售業個人資料檔案安全維護管理辦法
- **資安措施執行建議　(依據「零售業個人資料檔案安全維護管理辦法」第十條)**
  - 通訊系統帳號認證及驗證
  - 個資資料加密/遮罩
  - 安全企業網路架構與用途
  - 建立安全遠端連線及資料傳輸機制
  - 防火牆規則配置建議
  - 設備軟體更新與資安風險管控
  - 事故模擬演練
  - 如何防範及因應社交工程威脅(第十一條 教育訓練)

資安防護之個資法遵要求、依據與重點

個人資料保護法及施行細則

資安防護之個資法遵要求與依據

一、配置管理之人員及相當資源。

二、界定個人資料之範圍。

三、個人資料之風險評估及管理機制。

四、事故之預防、通報及應變機制。

五、個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善。

- 個人資料保護法第27條第1項
- 個人資料保護法施行細則第12條第2項第6、7、8、10款

目標與重點

- 資料安全管理及人員管理
  - 資料去識別化、存取管控、傳輸保護、技術面防護(設置防火牆、入侵偵測設備、定期惡意程式檢視等)
- 認知宣導及教育訓練
  - 非技術面防護(※建議包含社交工程)
- 設備安全管理
  - 定期檢查維護及更新設備
- 使用紀錄、軌跡資料及證據保存
  - 留存資訊設備、系統、資料庫等存取Log紀錄

零售業個人資料檔案安全維護管理辦法

零售業個人資料檔案安全維護管理辦法第十條

業者以資通安全管理法所稱資通系統直接或間接蒐集、處理或利用個人資料，應採取下列安全措施，並定期檢討改善

- 資通訊系統存有個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。
- 評估使用情境，採行個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。
- 確認蒐集、處理或利用個人資料之電腦、相關設備或系統具備必要之安全性，採取適當之安全機制，定期檢測並因應系統漏洞所造成之威脅。
- 與網路相聯之資通訊系統存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。

法規條文：https://law.moea.gov.tw/LawContent.aspx?id=GL001466

零售業個人資料檔案安全維護管理辦法第十條(續)

- 建置防火牆、電子郵件過濾機制或其他入侵偵測設備等防止外部網路入侵對策，並定期更新。
- 資通訊系統存有個人資料者，應設定異常存取資料行為之監控及定期演練因應機制。
- 處理個人資料之資通訊系統進行測試時，應避免使用真實個人資料；使用真實個人資料者，應訂定使用規範。
- 處理個人資料之資通訊系統有變更時，應確保其安全性未降低。
- 定期檢視處理個人資料之資通訊系統，檢查其使用狀況及存取個人資料之情形。

資安措施執行建議

依據「零售業個人資料檔案安全維護管理辦法」

資通訊系統帳號認證及驗證

資通訊系統帳號密碼驗證實施重點

資通訊系統中存有個人資料時，認證機制之設計與實施至關重要。以下是針對密碼複雜度設置的具體建議

最小密碼長度

- **密碼長度應該設為至少 12 至 16 個字符。越長的密碼越難被破解。**

字符組合

- 密碼應要求使用不同類型的字符組合
  - 至少包含一個大寫字母（A-Z）
  - 至少包含一個小寫字母（a-z）
  - 至少包含一個數字（0-9）
  - 至少包含一個特殊字符（如 !@#$%^&*()）

資通訊系統帳號密碼驗證實施重點(續)

避免使用常見密碼

- 系統應防止用戶設定常見的弱密碼（如 "password123"、"qwerty" 等）。可借助黑名單（blacklist）來阻止這些常見密碼。

過期策略

- 密碼應該定期過期（如每 90 天），並要求用戶重新設定密碼。這樣可以減少長期使用弱密碼的風險。

強制執行密碼歷程記錄

- 不得重複前 3 次密碼

多因素驗證 MFA 之種類與選擇

強化系統登入驗證安全，避免駭客攻擊及個資遭非法竊取

帳號、密碼驗證
(第一道驗證關卡)

簡訊、Email驗證碼等驗證
(第二道關卡)

成功登入
(兩道關卡均驗證成功)

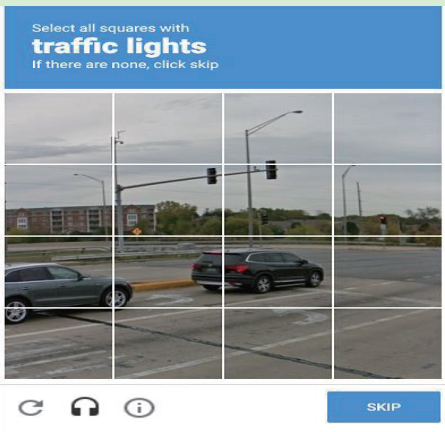
多因素驗證(Multi-Factor Authentication, MFA)是加強驗證強度的措施

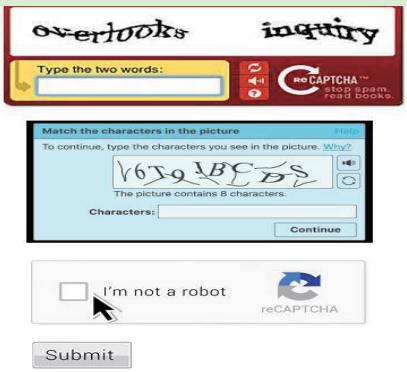
- 以**Email發出驗證碼**
- 經手機傳送**驗證碼**，可透過**APP或簡訊**。如經由簡訊發送，需要另電信系統服務費用
- 採用 **Google Authenticator APP**(Android, iOS)以提供掃描、驗證碼讀取。
- 亦可配合工商憑證、自然人憑證等卡片資料驗證或指紋、虹膜辨識等

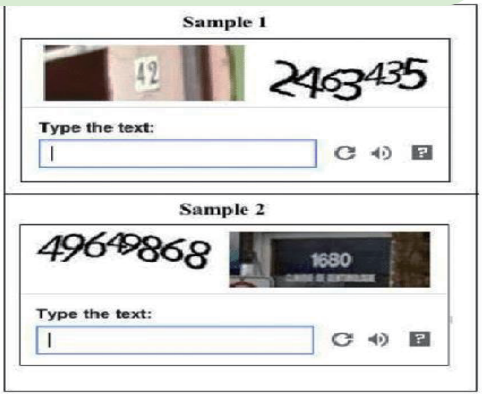
其他強化驗證措施方式-CAPTCHA

強化系統登入驗證安全，避免駭客攻擊及個資遭非法竊取

- 甚麼是**CAPTCHA**
  - 使用者嘗試登入、購買或造訪網站的機敏資訊時，**CAPTCHA 可作為驗證機制**。
  - CAPTCHA驗證包含字元、數字或物體的扭曲影像，可有效遏止機器人暴力嘗試破解登入。
  - 使用者**必須正確輸入字元或辨識影像中所描繪的物體才能繼續**。
  - 如果使用者的回答正確，且驗證其非機器人則允許存取；如果不正確，則可拒絕訪問或被要求再次嘗試。







採用OAuth 2.0(授權)+JWT強化API存取安全

何謂OAuth 2.0

OAuth 2.0本身是一個**授權框架**(不處理身份驗證)，用戶向授權伺服器授權第三方訪問其資源。**授權伺服器發放授權token**並使用此token來訪問伺服器上的資源。
OAuth 2.0的核心是在**處理授權問題**，且常與**JWT(用來處理身份驗證)**一起使用，**JWT是OAuth2.0流程中的一種token形**式。

個資資料加密/遮罩

方法一：採用加密機制

常見加解密方式比較

應評估採用安全加密演算法，兼顧個資資料傳輸效能與安全

加密演算法	簡述	常見演算法
對稱式加密	**加解密使用同一組密鑰**，運算快、需要雙方先安全的交換金鑰	◘ AES ◘ DES(加密金鑰的位元長度不足，已被暴力破解而淘汰。)
非對稱式加密	**加解密使用公私鑰**，運算慢、用途多	RSA

對稱與非對稱式加密方式優缺點探討

對稱式

- 優點：運算快。
- 缺點：雙方需**採用相同的金鑰**

非對稱式

- 優點：尚未有攻擊RSA演算法的方式可以破解 1024 bit 的金鑰(768 bits 已被破解)，建議**至少使用 2048 bit 的金鑰**。
- 缺點：效能欠佳。

※金鑰保存管理
應注意事項

加解密金鑰應妥善保存，**私鑰不得公開，應加密存放並限制存取權限**。定期更換金鑰，防止洩漏。可使用安全硬體或軟體管理，並**備份於安全環境**，以確保資料安全與完整性。

方法二：資料遮罩

資料遮罩處理方式

個資資料遮罩處理，使其無法直接、間接識別，達到個資法去識別化要求

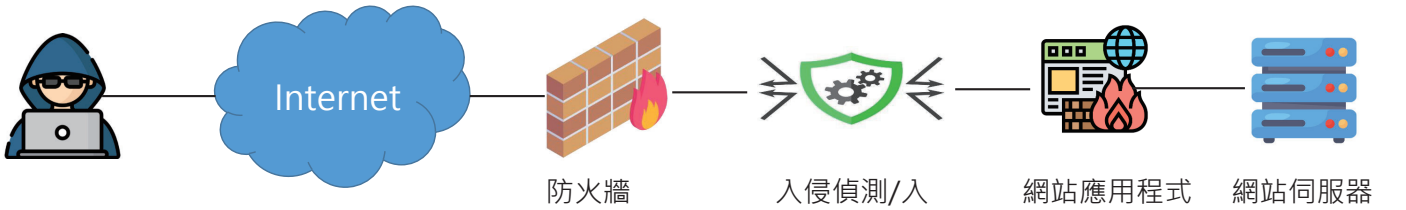
套用的演算法	原始資料	遮罩後資料	說明
虛構資料(Fictitious Data)	2562-2880	2562-*****	遮蔽後4個字元
亂數處理(Random Data)	Jeffrey Lee	David Chen	將資料亂數排列
日期增減(Date Aging)	12/21/2012	5/21/2009	日期提前3年7個月
數字更改(Numeric Alteration)	13856	15856	數字增加2000
語意處理(Semantic)	R113405505	F135869531	替換其他可驗證的身分證字號

安全企業網路架構與用途

資安防護「縱深防禦」安全措施與用途

縱深防禦透過多層安全措施，有效減少個資洩漏風險，強化個資保護。

縱深防禦(Defense in Depth)是結合多種不同的安全防禦機制來阻絕不同類型的駭客攻擊手法。即使其中一層無法順利攔阻，仍有其它輔助或備援方式接手攔阻，駭客必須逐一突破各項保護措施，才能成功入侵。

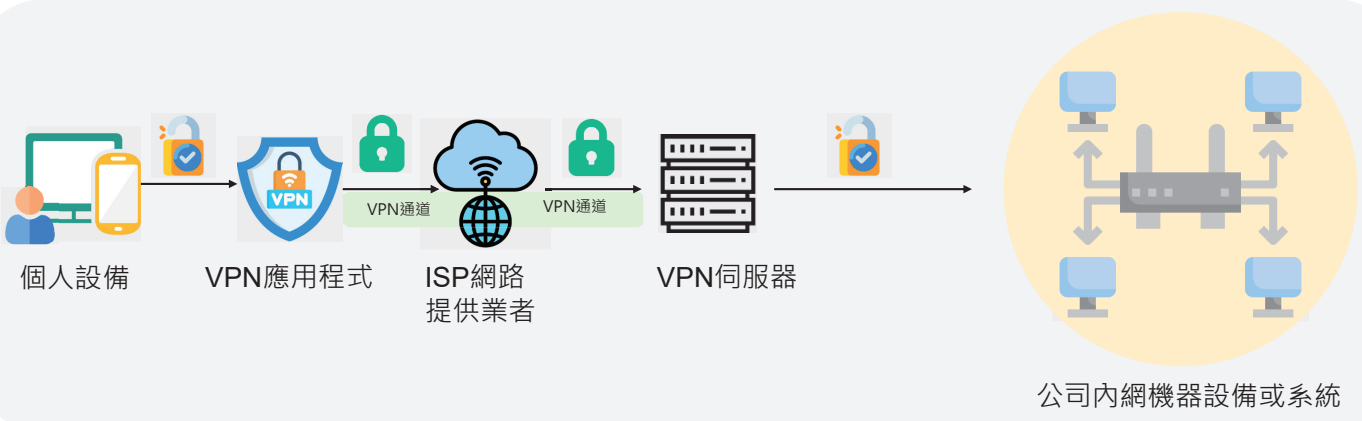


防火牆 (Firewall)	入侵偵測/入侵防禦 (IDS/IPS)	網站應用程式防火牆 (WAF)	網站伺服器 (Web Server)
針對連線來源(IP)及連線埠(Port)檢查是否符合連線政策	針對封包內容進行進一步特徵比對，以便即時發現惡意攻擊並加以阻擋	位於網頁瀏覽者與伺服器間，專責分析網路流量內容，主要防禦常見攻擊如SQL Injection、XSS攻擊	

採用VPN強化資安防護

採用VPN遠端安全存取公司資料，防止未經授權訪問，機敏資訊不外洩。

- VPN（虛擬私人網路）透過加密技術建立網路連線專屬通道，將資料從裝置傳送至遠端伺服器(VPN Server)，再由伺服器轉至目的地網站，這樣可以隱藏IP位置保護網路隱私。



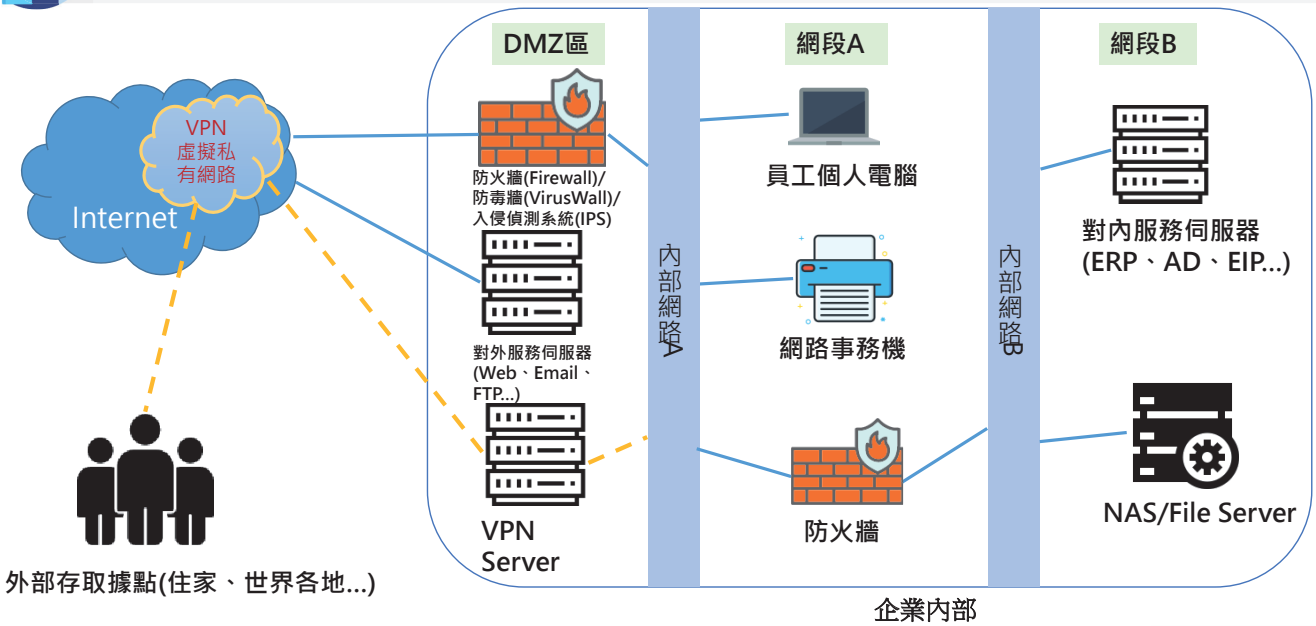
常見網路安全防禦技術

應評估及配置佈署適當網路安全防禦設備，避免駭客攻擊遭個資外洩

防禦類型	防禦設備	功能說明	用途需求
網路連線安全	防火牆(Firewall)	允許或禁止網路上之存取行為	限制/開放特定IP、Port等之資料存取行為
	入侵偵測系統(IDS) / 入侵防禦系統(IPS)	• IDS即時監控網路及系統事件，偵測入侵行為並示警 • IPS可進一步加以阻擋	偵測並阻止DDoS 攻擊等
	虛擬私人網路(VPN)	利用Tunneling、加密、身分驗證等技術，建立安全傳輸通道	透過網際網路(Internet)存取公司內部網路(Intranet)等
WEB安全	網路應用程式防火牆(WAF)	保護Web應用程式和資料	抵擋SQL Injection及XSS等常見網站攻擊行為

企業網路架構圖(網段區隔+VPN)

依設備存放地點與風險等級進行內部網段區隔+外部透過VPN存取，保障個資隱私安全，避免個資外洩



建立安全遠端連線及資料傳輸機制

遠端連線方式類型

遠端連線傳輸個資應採加密連線，確保個資資料傳輸安全

- **SSH**
  - shell介面，command模式
  - **連線通道經過加密**，使用 public 和 private key 的 Architecture 來做連線通道的加解密
- **telnet**
  - shell介面，command模式
  - **明文傳輸，沒有加密**的流程
- **遠端連線工具(例如：Microsoft遠端桌面工具)**
  - GUI介面
  - 可變更預設的遠端桌面安全**設定為加密連線**

記號標註為安全遠端連線方式

MS Windows遠端桌面工具連線安全性提升方式

建立加密連線，確保個資資料傳輸安全

防火牆規則配置建議

防火牆規則之組成

防火牆允許或禁止受保護網路之存取行為，避免遭受未經授權之非法存取

來源 IP 位址

- 來源 IP 位址可識別流量的來源。 組織可能會封鎖來自某些已知不正確的 IP 位址或 IP 範圍的流量。 或者，特定電腦或服務可能只能從允許列出的 IP 位址存取。

目的地 IP 位址

- 目的地 IP 位址指定流量的位置。 例如，公司可能會指定使用者無法瀏覽到已知為惡意或違反公司政策的特定網域。

協定類型

- 防火牆規則也可以指定流量是使用傳輸控制協定 (TCP)、用戶資料封包協定 (UDP)或 Internet 控制訊息協定 (ICMP)。 例如，組織通常會在網路外圍阻止 ICMP 流量。

連接埠範圍

- 防火牆規則使用TCP/UDP連接埠來指定允許或禁止的網路流量類型。 例如，允許入站 HTTPS 流量的防火牆規則將指定應允許到連接埠 443 的 TCP 流量進入網路。

防火牆規則配置應注意事項

採用嚴謹之防火牆規則配置並定期監控審查，避免潛在資安威脅

限制性規則（預設拒絕）與寬鬆規則（預設允許）

- 預設情況下，應將防火牆規則設定為預設拒絕所有存取。 然後建立例外規則，以建立更安全的網路環境，阻擋非法存取。

自訂防火牆規則

- 防火牆解決方案可能包含一組通用「適合所有人使用」之規則，但不符合組織的特定需求。 公司應該自訂這些規則，以提供升網路安全性。例如：特定伺服器應限制特定IP及Port之存取

記錄和監控防火牆規則

- 防火牆規則應確實記錄留存，並定期監控、盤查。 以幫助檢測潛在的安全威脅，並可以識別需要更加嚴格或寬鬆的不正確的防火牆規則。

設備軟體更新與資安風險管控

定期更新設備之目的與應包含內容

定期更新系統及設備安全漏洞修補程式，避免遭受駭客攻擊

建議經常檢查更新的軟韌體和系統

- 作業系統（Windows、macOS、Linux、Chrome OS ...）
- 瀏覽器（Chrome、Firefox、Safari、Edge ...）
- 安全防護軟體（防毒軟體、防火牆 ...）
- 辦公軟體（Microsoft Office、LibreOffice ...）
- 影音播放器（VLC、Windows Media Player ...）
- 操作軟體和韌體（智能裝置、物聯網設備 ...）

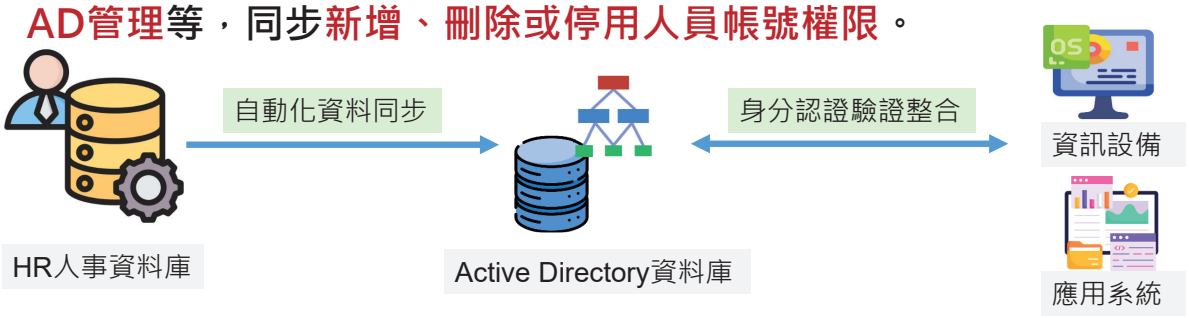
✓ 定期更新設備之目的

- 定期更新軟體和系統是為了**修補安全漏洞**、提供軟體新功能、提高與硬體兼容性、解決系統錯誤，是確保電腦保持安全、高效和功能完整的關鍵步驟。
- **忽略更新可能會使電腦或資訊設備變得容易受到威脅**，並且無法充分利用新的功能和技術。因此，建議經常檢查並安裝可用的更新。
- 可以**啟用自動更新**功能，並**定期手動檢查可用的更新**，包括操作系統、應用程式和硬體驅動程式。

強化設備系統帳號管制可採行之方式

自動化帳號權限管理機制，確保帳號與人員異動同步，避免個資外洩風險

- 考量與資料存取控制之「密碼的使用與保護」措施，採取相同策略實施管制，例如：將系統納入網域，並依使用者需求結合AD核予適當權限。
- 實施定期或不定期稽核，期使系統之帳號密碼管理處於正規管理模式，而非流於形式。
- 採用**自動化作業**，**人員異動**(新進或離職等)**結合HR人事資料、AD管理**等，同步**新增、刪除或停用人員帳號權限**。



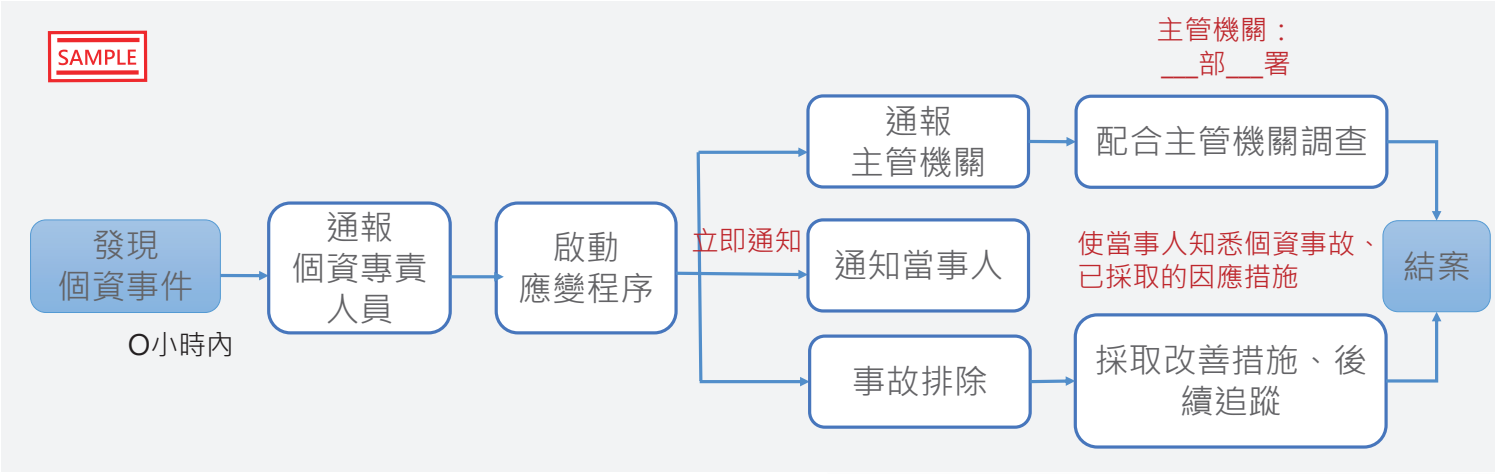
事故模擬演練

建立通報及應變程序

各單位應建立完整的事故通報流程 (建議含流程圖)，並涵蓋：

- 內部通報程序。
- 向主管機關通報程序。

建議將主管機關窗口及聯繫方式寫入文件



辦理演練

建議定期實際演練，強化組織應變能力，降低實務風險

演練目的與成效確認重點：

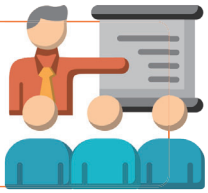
- ✓ 確認個資防護政策有效性
- ✓ 確認通報應變小組任務熟悉度
- ✓ 達成滾動精進防護政策

制 定

- 制定組織內部通報應變程序
- 制定程序各階段窗口清單

模 擬

- 定期以虛擬事故案件演練
- 記錄演練情形



檢 討

- 檢視演練紀錄與問題回饋，提出演練報告
- 依據結果優化通報流程與制度

帳號系統權限申請及盤查

系統帳號權限申請、審查及定期盤查

定期系統權限帳號清查盤點，保留紀錄，以供稽核及備查

校務行政系統權限申請表

申請日期：　　年　　月　　日 / 申請職員 ID：

說明

※ 不同的系統，功能與權限要求若相同，可填寫至同一張

※ 若申請暫時權限請將期限確實填寫或將「依審核單位判定」圈選

※ 流程說明：

勾選系統所有 申請人 → 申請單位主管 → 勾選系統之二級單位審核經辦 → 勾選系統之審核單位二級主管 → 勾選系統之審核單位一級主管 → 資訊中心經辦 → 資訊中心主任 → 依申請之核可系統進行權限開放 → 教單歸檔

※ 約一天工作天

系統名稱與審核單位

□ 教務 (一級單位審核：教務處)

二級單位審核 註冊課務組：□管理學籍 □抵免學分 □課程抵免 □管理成績 □管理畢業 □課程 □學群 □課程標準 □開課 □排課 □線上選課 □調查寒暑假 □課程介紹 □登記證照 □預警管理 □學生相關資料查詢(導師班查詢) □其他_____

□ 學務 (一級單位審核：學務處)

二級單位審核 生輔組：□缺曠 □懲罰 □換行 □減免 □班級幹部 □其他_____

諮輔中心：□導師設定 □學生諮商 □其他_____

軍訓室：□兵役 □其他_____

□ 總務 (一級單位審核：總務處)

二級單位審核 事務組：□管理請購 □管理採購 □管理廠商 □其他_____

保管組：□管理驗收 □管理財產／列管物品 □其他_____

□ 公用 (一級單位審核：資訊中心)

□公用項目設定(學生資訊系統、教職員資訊系統網頁公告功能) □其他_____

	功能	權限
1	查詢	□一般權限 □暫時權限(年 月 日至 年 月 日或依審核單位判定)
2	使用(異動、變更)	□一般權限 □暫時權限(年 月 日至 年 月 日或依審核單位判定)
3	審核	□一般權限 □暫時權限(年 月 日至 年 月 日或依審核單位判定)

申請原因：

申請人	申請單位主管	二級單位審核經辦	二級單位審核主管	一級單位審核主管

資訊中心經辦	資訊中心主任

權限開放日期：　　年　　月　　日（資訊中心填寫）

權限撤銷日期：　　年　　月　　日（資訊中心填寫）

※本表單由資訊中心留存

※如調職或離職，依人事發布令系統將自動撤銷其權限

系統權限申請及紀錄

文件編號	ISMS-D-007-03	系統使用者帳號清單	文件類別	限閱
版　次	V1.0		流水號	YYY-XXXX

應用系統名稱：　　清查或更新日期

權限權限列表：　R：讀取　A：新增　W：寫入　I：插入　D：刪除　ALL：全部權限

單位	姓名	帳號名稱	使用者群組/使用者權限	審查意見	審查後權限	備註

備註：1.如系統之資料表或報表已具備本表內同等資訊，得以當附件呈核。

2.作業系統、網路設備、資料庫及應用系統之使用者、管理者及專屬帳號皆須列出審查。

3.特殊帳號或權限應說明用途，共用帳號應說明使用範圍。

本系統是否已符合本公司密碼規定(長度 8 碼以上，且須包含英數字及特殊字元之組合、每半年強制更新)：□是　□否

承辦人：　　單位主管：

系統權限定期盤查及紀錄

如何防範及因應社交工程威脅(非技術面)

社交工程防範-收發電子郵件工具安全性設定

平時做好安全設定、強化資安意識，避免受社交工程侵害，造成資安事故

檢視寄件者及主旨

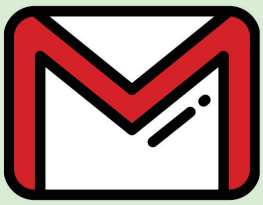
避免釣魚郵件，開啟信件前應檢視寄件人信箱、地址及主旨

郵件預覽關閉

關閉郵件自動預覽功能。不會自動開啟郵件，降低中毒的機率

取消自動回條

避免駭客蒐集有效的郵件信箱，防止信箱洩漏



強化郵件安全防護設定資安防護有保障

純文字模式開信

郵件中的網址均自動轉換為文字，圖片亦無法顯示，有效防範中毒狀況

阻擋 HTML 郵件中的圖片

若未阻擋，系統自動下載的圖片中可能含有惡意病毒、後門木馬程式

THANK YOU

數位轉型．軟體技術．資安產業．數位經濟