個資行政檢查作業準備與因應

教育機構驗證中心主導稽核員 黃攸德

大綱

- 個資行政檢查資料準備
- 教育部主管目的事業之個人資料檔案自我檢查表

個資行政檢查資料準備

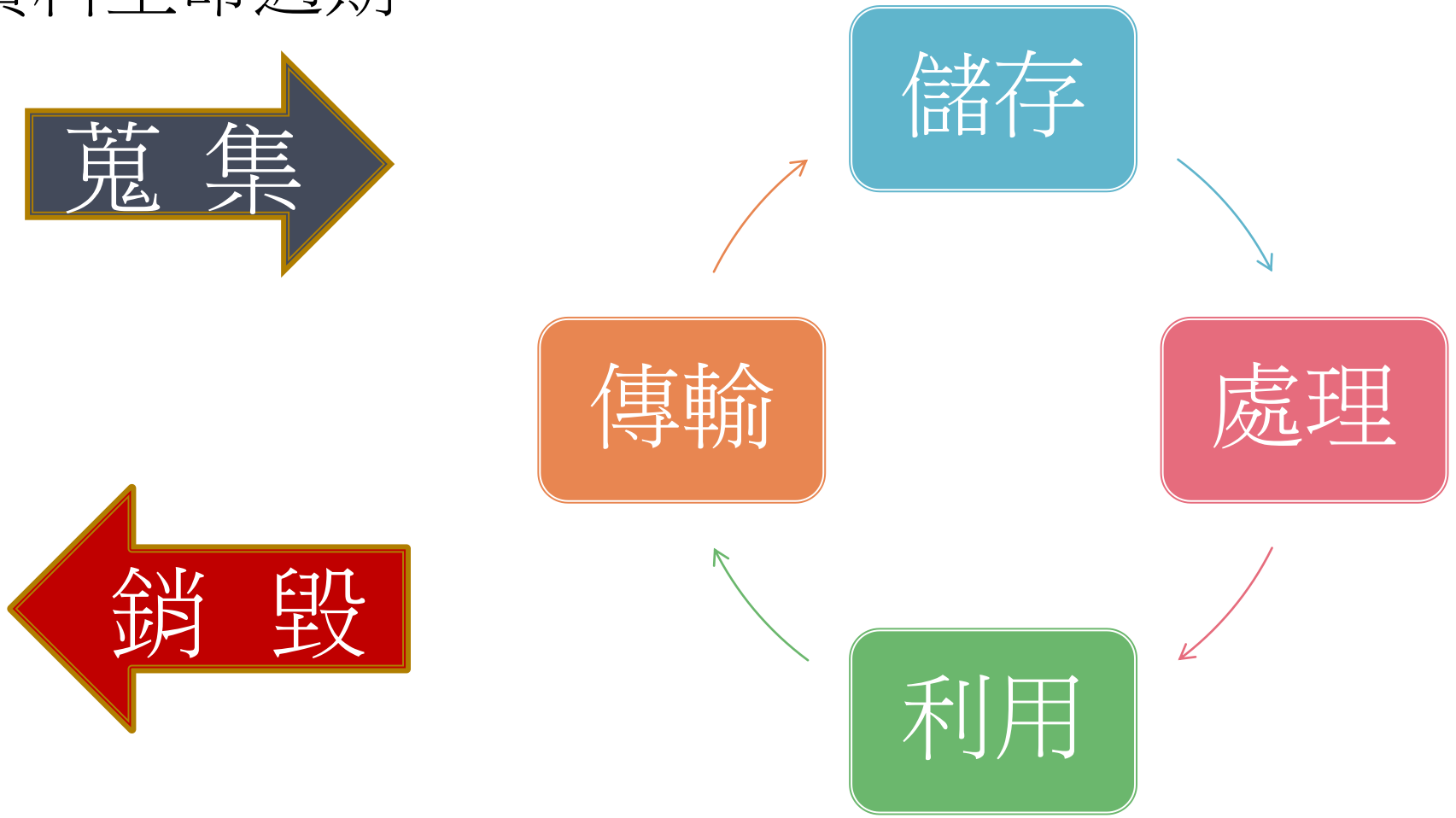
個資行政檢查目的

- 個人資料保護法第27條

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

個人資料保護範圍

- 個人資料生命週期



個資安全維護措施

- 個人資料保護法施行細則第12條

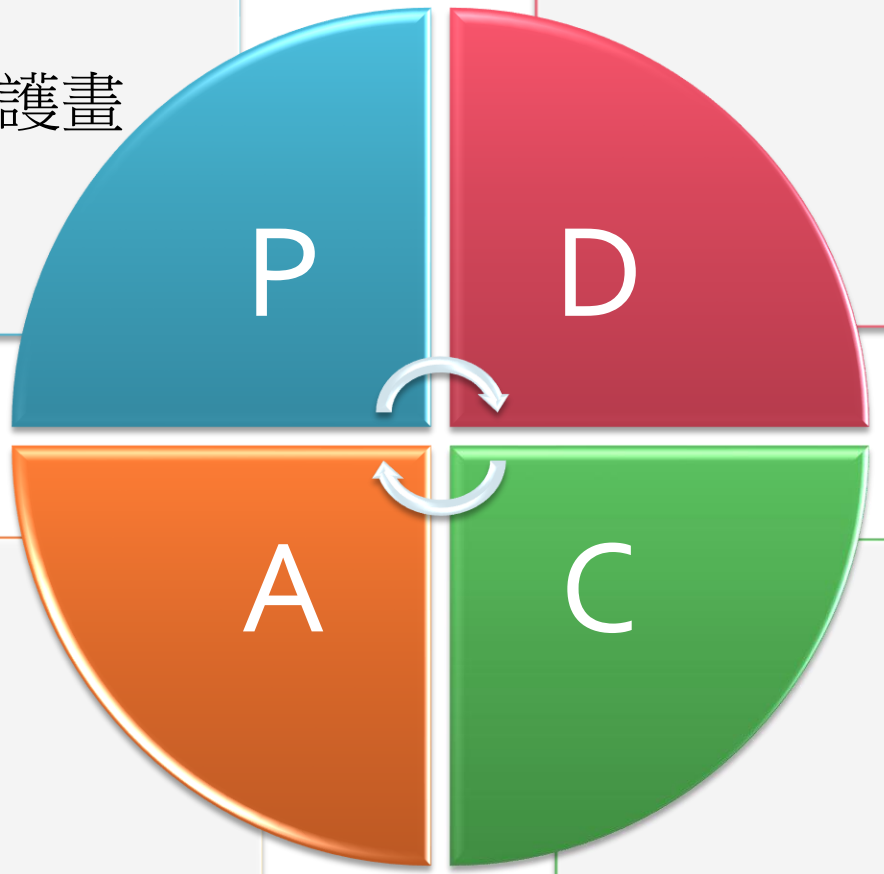
  前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

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。

維護個資安全作為

Plan 計畫
- 個人資料檔案安全維護畫
- 管理程序

Do 執行
- 人員、資料、設備管理
- 宣導與教育訓練
- 證據--表單紀錄



Action 行動
- 矯正改善
- 持續精進

Check 查核
- 內部查核
- 外部查核

佐證資料的準備(1)

- **佐證資料要與查檢項目的要求相符**
- **佐證資料內容完整清楚**(視資料量多寡，可節錄部分內容)
- **適度遮蔽個人資料**
- 建議依檢查項目建立佐證資料檢索表，也可增加補充說明

本次研習是依過去查檢經驗，建議檢附資料提供參考

因各委員經驗不同，查檢的方向可能略有不同

請依填表說明，儘可能準備提供

- 書面審查
  - 無補充說明機會
  - 儘可能準備提供

佐證資料的準備(2)

- 依自我檢查表填表說明，提供個資檢查表

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填對
			◯不適用(無明確法規要求)	
	3.3 依稽核人員評核結果檢討改進，並向管理人與稽核人員提出書面報告。	普中高	個人資料檔案安全維護計畫執行情形，定期或不定期稽核 ◯無 ◯有，檢附相關佐證資料 1、 稽核/查核日期:　　年　月　日 2、 專責人員或專責組織改善報告提出日期： 　　年　月　日 ◯不適用(無明確法規要求)	
	3.4 訂定個人資料保護管理政策。	高	訂定個人資料保護管理政策 ◯無 ◯有，檢附個人資料保護管理之政策公開紀錄 ◯ 不適用(無明確法規要求)	

3.3 依稽核人員評核結果檢討改進，並向管理人與稽核人員提出書面報告	• 請填寫稽核(查核)日期、並填寫改善報告提出日期(報告形式不限)。 **依經營業別提交所需之佐證資料：** **屬於私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、海外臺灣學校及大陸地區臺商學校、私立兒童課後照顧服務中心者** • 請檢附***稽核紀錄**、**稽核之不符合事項***追蹤改善紀錄**及***向管理人提出結果報告之紀錄**。 **屬於短期補習班者** 注意事項：查核人員與指定之專責人員不得為同一人。 • 請檢附***個人資料檔案安全維護計畫執行之檢查紀錄**及***向負責人提出結果報告之紀錄**。 相關名詞： • 管理人：由負責人擔任或指定人選，負責督導安全維護計畫訂定及執行。 • 代表人：在法律上有權代表公司的人，必須同時是負責人。 • 負責人：遵循法律掌管公司營運，並負責處理各種組織業務的人。 • 代表權人：被授予代表他人行使權力的人，其行動對被代表者具有法律效力。 補充說明： • 改善邏輯一致性：改善報告之日期需在稽核日期之後。佐證資料應呈現完整的「發現缺失 -> 進行改善 -> 追蹤結果」流程，不可僅檢附稽核表。 • 追蹤改善紀錄要點：若稽核結果為「合格／無缺失」，仍需檢附稽核紀錄，並於報告中註明「經查核各項要點均符合規範，將持續維持」。若有缺失，則必須針對該缺失提出具體改善措施與完成證明。 • 報告形式與內容：書面報告不限格式，但內容應包含：(1) 稽核時間、(2) 稽核發現（含優／缺點）、(3) 缺失改善對策、(4) 追蹤複查結果。

個資保護要求強度等級分數計算

- 評估構面及構面權重(填表說明P2)

評估構面	分數 / 權重	0	1	2	3
個資數量 A	1		1000 筆以下	一般個資 1001~50,000 筆 特種個資 1001~35,000 筆	一般個資 50,001 筆以上 特種個資 35,001 筆以上
外部利用 B	0.8	無外部利用情形	1000 筆內少量	一般個資 1001~50,000 筆 特種個資 1001~35,000 筆	一般個資 50,001 筆以上 特種個資 35,001 筆以上
國際傳輸 C	1.2	無國際傳輸	不涉及特殊類別敏感資訊 1000 筆內少量	一般個資 1001~50,000 筆 特種個資 1001~35,000 筆	一般個資 50,001 筆以上 特種個資 35,001 筆以上

要求強度總分=∑評估構面分數 x 構面權重

例 組織保有
一般個資總數 2000 筆
特種個資 60 筆
外部利用 100 筆以內
無國際傳輸

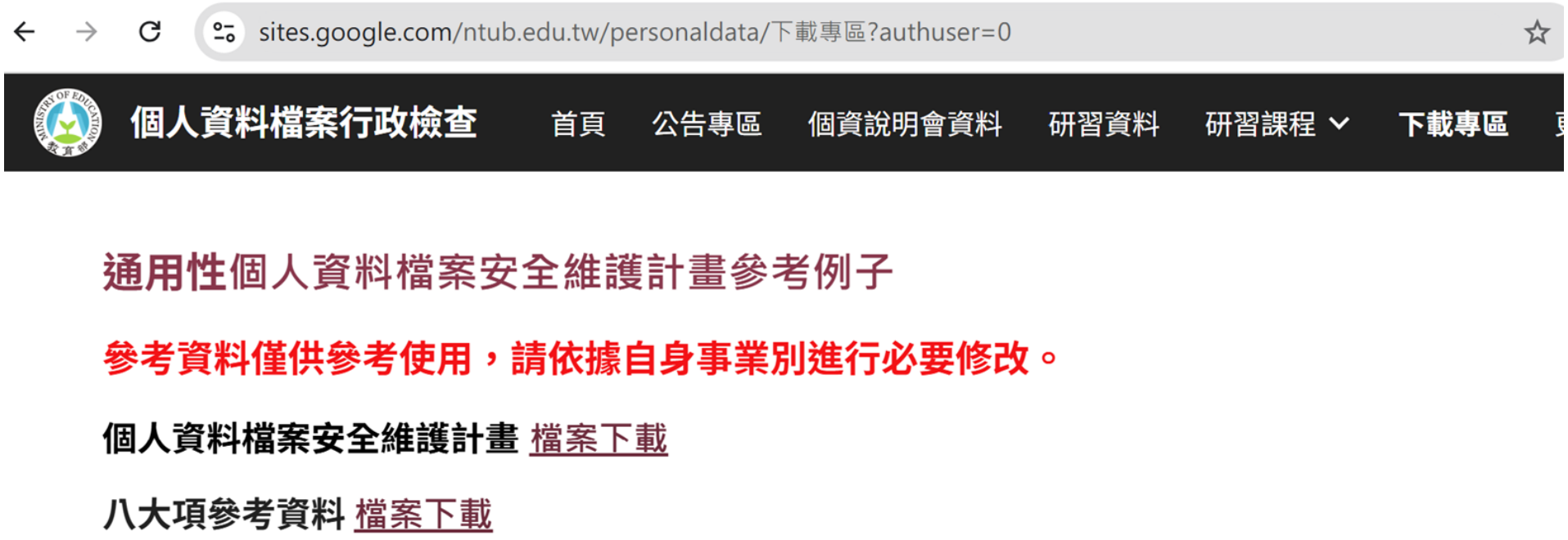
強度總分 = 2*1(A)+1*0.8(B)+0(C) =2.8

個資保護要求強度等級

要求強度等級	要求強度總分	說明
普	1~4	受檢單位擁有少量一般性個資及特種個資。
中	4.1~7	受檢單位擁有一定數量個資及特種個資，或有對外電子商務服務系統，或保有一定數量以上的特種個資之資通系統。
高	7.1~9	受檢單位擁有大量一般及特種個人資料(病歷、醫療、基因、性生活、健康檢查及犯罪前科)，有對外電子商務服務系統，或保有大量特種個資之資通系統。

重要參考資料

- 教育體系個資安維行政檢查計畫網站
  https://sites.google.com/ntub.edu.tw/personaldata/



重要參考資料

- 檢查表及本部各事業別安維辦法對應表
  https://docs.google.com/spreadsheets/d/1n2Di1dW-QfQupeGokkPgB3KjDFZe5Dor/edit?gid=1401677609#gid=1401677609

	A	B	C	D	E	F	G	H	I	J
1	查核重點	查核內容	紀錄文件	私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法	私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法	海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法	私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法	短期補習班個人資料檔案安全維護計畫實施辦法	運動彩券業個人資料檔案安全維護計畫實施辦法	個資法暨施行細則
2	1.個人資料檔案安全維護計畫	1.1訂定「個人資料檔案安全維護計畫」	請檢附所訂的個人資料檔案安全維護計畫（含業務終止後個人資料處理方法）。	第3條 依私立學校法核准設立之私立專科以上學校（以下簡稱學校）及依學術研究機構設立辦法核准設立之私立學術研究機構（以下簡稱機構）**應訂定個人資料檔案安全維護計畫**（以下簡稱安全維護計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第4條第1項 學校及幼兒園**應依本辦法規定訂定安全維護計畫**，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第4條 依海外臺灣學校設立及輔導辦法設立之海外臺灣學校及依大陸地區臺商學校設立及輔導辦法設立之大陸地區臺商學校(以下簡稱境外臺校)**應訂定個人資料檔案安全維護計畫**，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第4條 課照中心**應依本辦法規定，訂定安全維護計畫**，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第3條第1項 短期補習班（以下簡稱補習班）**應訂定個人資料檔案安全維護計畫**（以下簡稱計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第3條第1項 運動彩券業**應訂定個人資料檔案安全維護計畫**（以下簡稱計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	**(個資法授權主管機關訂)** 個資法第27條第2項規定中央目的事業主管機關得指定非公務機關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。
3	2.組織及運作管理情形	2.1指定專人或建立專責組織負責管理	請檢附**單位**個資管理組織圖、分工及相關辦法，並提出個資窗口所協助之各項個資保護工作事項，如：參與會議、盤點及風險評鑑工作、事件處理等。 **個資管理審查相關會議紀錄**	第5條 學校、機構**得指定或設管理單位，或指定專人**，負責個人資料檔案安全維護	第5條 學校及幼兒園**得指定或設管理單位，或指定專人**，負責個人資料檔案安全維護	第7條 境外臺校**得指定或設管理單位，或指定專人**，負責個人資料檔案安全維護	第7條 課照中心**應指定專責人員**，負責**規劃、訂定、修正、執行安全維護計畫及**	第6條 補習班**應指定專責人員**，負責**規劃、訂定、修正、執行計畫及**業務終止後個	第6條 運動彩券業**應指定專責人員**，負責**規劃、訂定、修正、執行計畫及**業務終止	**(個資法未要求照做)** 個資法施行細則第12條規定 得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則： 一、配置管理之人員及相當資源。
		3.1規劃、訂定、修正與執	請檢附所訂的個人資料檔案安全維護計畫（含業務終止後個人資	第5條 **訂定及執行安全維護**	第5條	第7條 **訂定及執行安全維護**				**(個資法授權主管機關訂)** 個資法第27條第2項規定中央目的事業主管機關得

査檢表填寫

壹、受檢查單位基本資料

		填表說明對應頁數
1.受檢查單位名稱	(非學校單位，請填報立案全名稱)	
2.填寫日期	_____年_____月_____日	1
3.經營業別	○ A ○ B ○ C ○ D ○ E ○ F ○ G ○ H ○ I ○ J	1
4. 具電子商務服務系統，或具有特種個資的資通系統之安全管理	○是○否	1
5.個資保護要求強度等級	個資數量分級：○ 1○ 2○ 3	2
	外部利用分級：○ 0○ 1○ 2○ 3	2
	國際傳輸分級：○ 0○ 1○ 2○ 3	2
	等級： ○普 ○中 ○高	2-3

經營業別

A：私立專科以上學校
B：私立兒童課後照顧服務中心
C：短期補習班
D：私立高級中學
E：私立國民中學
F：私立國民小學
G：私立幼兒園
H：海外臺灣學校
I：大陸地區臺商學校
J：其他

電子商務服務系統，或具有特種個資的資通系統

- 電子商務係指透過網際網路進行有關商品或服務之廣告、行銷、供應或訂購等各項商業交易活動。
- 系統若有可識別為特種個資之欄位，視同具有特種個資。(例如有欄位為"有身障手冊")
- 提供給家長即時觀看的監視系統，涉及「個人資料」或「特種個資」(如：幼兒的生理特徵/受傷狀況)，屬電子商務服務系統或具有特種個資的資通系統

特種個資

病歷、醫療、基因、性生活、健康檢查、犯罪前科

貳、受檢單位自我檢查項目

1、個人資料檔案安全維護計畫

1、個人資料檔案安全維護計畫	1.1 訂定「個人資料檔案安全維護計畫」	普中高	訂定個人資料檔案安全維護計畫(含業務終止後個人資料處理方法) ○是 ○否 ○不適用(無明確法規要求)	4

- 請檢附『**個人資料檔案安全維護計畫**』(含業務終止後個人資料處理方法)。

個人資料保護法第48條

第3項第3款

未依第五十一條之一第三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

第4項

非公務機關有前項各款情事之一，其情節重大者，由主管機關處新臺幣**十五萬元以上一千五百萬元以下罰鍰**，並令其限期改正，屆期未改正者，按次處罰。

個人資料檔案安全維護計畫相關檢查項

3.1 規劃、訂定、修正與執行所訂安維計畫**(管理人核准紀錄)**

4.3 依資料屬性訂定管理程序**(一般個資、特種個資)**

4.8 確認與維護保有個資之正確性

個資異動(當事人請求更正或補充)受理窗口，個資受理窗口人員名稱及職稱

5.1 使用者身分確認及保護機制(電子商務服務系統，或具有特種個資的資通系統)

6.1 對個資存取媒介物及環境(如機房、雲端)，採取環境管理措施**(中、高等級)**

(硬碟、固態硬碟、網路儲存裝置、USB、磁帶、磁碟、CD、DVD、藍光光碟等)

7.1 訂有業務終止之個資處置措施

事故通報與應變程序

8.1 訂定個資洩漏等事故發生或知悉起 72 小時內通報流程

8.2 訂定對個資洩漏等事故採應變措施以控制損害

8.3 訂定查明事故後以適當方式通知當事人之程序並告知已採取因應措施

8.4 研議預防機制

2、組織及運作管理情形

2.1 指定專人或建立專責組織負責管理	普中高	個資保護專人或專責組織 ○無 ○有，專責單位名稱或專責(職)人員_____ ○不適用(無明確法規要求)	5

- 普
  - 檢
- 中
  - 檢
- 高
  - 檢

置法規

3. 專責人員或專責組織任務

- 訂定、修訂個人資料檔案安全維護計畫 (管理人核可紀錄)
- 教育訓練 (簽到表(參與率)+教材)
- 內部稽核(稽核報告+改善事項追蹤紀錄)
- 個資保護成果報告(書面定期報告 或 會議紀錄+出席簽到表)
- 個人資料保護政策**(高)**

3. 專責人員或專責組織任務

3.1 規劃、訂定、修正與執行所訂安維計畫	普中高	規劃、訂定、修正與執行個人資料檔案安全維護計畫 ○有，檢附相關佐證資料 ○無 ○不適用(無明確法規要求)	6

- 檢附**個人資料檔案安全維護計畫** **管理人核准紀錄**

管理人：由負責人擔任或指定人選，負責督導安全維護計畫訂定及執行

- **在安全維護計畫內說明管理人是誰**

3.2定期報告紀錄.doc

3. 專責人員或專責組織任務

3.2 定期向管理人暨代表人或其他代表權人報告	普中高	專責人員定期向管理人暨代表人或其他代表權人報告個人資料檔案安全維護計畫執行情況 ○無 ○有，報告形式 □核准紀錄 □會議紀錄 □其他，_____	6

代表人：在法律上有權代表公司的人，必須同時是負責人

- 「定期」係指每年度至少應有一次報告紀錄
- **書面定期報告紀錄(含核准紀錄)或會議紀錄(含出席簽到表)**
  => 有明確記載定期報告**日期**且具有**管理人簽准(年月日)**
- 私立兒童課後照顧服務中心、短期補習班者
  - **定期報告紀錄**(不限形式)，需有報告對象簽核
    => 有明確記載定期報告**日期**且具有**負責人簽准(年月日)**

✓ 3.2定期報告紀錄.doc

3. 專責人員或專責組織任務

3.3 依稽核人員評核結果檢討改進，並向管理人與稽核人員提出書面報告	普中高	個人資料檔案安全維護計畫執行情形，定期或不定期稽核 ◯無 ◯有，檢附相關佐證資料 1、 稽核/查核日期:＿＿年＿月＿日＿＿ 2、 專責人員或專責組織改善報告提出日期： ＿＿年＿月＿日＿＿ ◯不適用(無明確法規要求)	7

查核人員與專責人員不得為同一人

- **稽核紀錄**、稽核之**不符合事項追蹤改善紀錄**及向**管理人**提出**結果報告**之紀錄(**管理人簽章(年月日)**)
  - **內容應包含**：(1) 稽核時間　(2) 稽核發現(含優／缺)　(3) 缺失改善對策 (4) 追蹤複查結果
- 短期補習班
  - 個人資料檔案安全維護計畫執行之**檢查紀錄**及向**負責人**提出**結果報告之紀錄(負責人簽章(年月日))**

✓ 3.3個人資料管理內部稽核查核表(空白)_v1.0.ods　　3.3持續改善措施單.docx

3. 專責人員或專責組織任務

3.4 訂定個人資料保護管理政策	高	訂定個人資料保護管理政策 ◯無 ◯有，檢附個人資料保護管理之政策公開紀錄 ◯不適用(無明確法規要求)	7

- 個資保護要求強度等級**高**之受檢單位
- **個人資料保護管理政策**公開之紀錄(如紙本或**電子的公告紀錄**)
- 各事業別之安維辦法無具體規範，本項可勾選不適用

✓ 3.4個人資料保護管理政策.docx

3. 專責人員或專責組織任務

3.5 定期對所屬人員進行宣導或專業教育訓練	普中高	提升個資保護意識護宣導或其他教育訓練執行情形 1、 近期宣導、教育訓練次數：_____ 2、 近期教育訓練日期：　　年　　月　　日 ○不適用(無明確法規要求)	7

- 「定期」係指每年度至少應有一次
- 課程內容須與個人資料保 護法相關

- 檢附人員定期教育訓練紀錄或宣導紀錄，如：**簽到表** (教育訓練執行**統計達成率**)、**教育訓練教材**、**課程時數認證證明**、宣傳單等
- 所屬人員：執行業務之過程必須**接觸個人資料之人員**，包括學校、機構之定期或不定期契約人員及派遣員工

4. 個人資料盤點、管理與紀錄

- 個資日常作業管理
  - 蒐集個資的告知(個資蒐集表單、網站個資蒐集畫面)
  - 不同資料屬性的管理(一般、特種個資)(安全維護計畫、管理程序)
  - 個資檔案盤點 (個資檔案盤點清冊)
  - 個資檔案風險評鑑(風險評估表+風險彙整表+風險改善計畫)
  - 個資蒐集利處理用符合特定目的(個資蒐集表單、網站個資蒐集畫面、稽核報告)
  - 確認與維護個資的正確性(安全維護計畫內的個資受理窗口)
  - 個資委外管理(委外契約 -> 個人資料委外監督及保護條款)
  - 首次利用個資行銷當事人確認作業(紙本、電子郵件、簡訊、網站公告)
  - 人員權限管理及保密義務(權限對照表+保密切結書)
  - 媒體/設備管理 (安全維護計畫、管理程序 +規定的表單紀錄)
  - 媒體/設備報廢或再利用的防護措施 (資料銷毀紀錄、硬體設備實體破壞紀錄)
  - 使用紀錄、軌跡資料及證據保存 (紙本調閱紀錄；系統存取、查詢、增修刪紀錄)

4. 個人資料盤點、管理與紀錄

4.1 定期盤點所保有個人資料並確認應遵守之法令	普中高	個人資料檔案盤點情形 近期個人資料檔案盤點日期：　年　月　日 個人資料檔案盤點欄位包含以下哪些內容(可複選)： □個人資料之類別 □特種個資 □蒐集方式 □保存期限 □銷毀方式 □處理方式 □利用方式 □控制措施 □其他，＿＿＿＿ ○不適用(無明確法規要求)	8

- 「定期」係指每年度至少應有一次
- 檢附 **個人資料檔案盤點清冊(含盤點日期)**

4. 個人資料盤點、管理與紀錄

4.2 風險分析及管控措施	普中高	分析評估風險，訂定適當之管控措施評估 1、 已核定可接受之風險值：○是○否 2、 負責人或管理人核定風險值時間： 年 月 日 ○不適用(無明確法規要求)	8

- 檢附經負責人、管理人核定之**風險評估文件資料**
- 風險評估文件完整性：檢附之文件需包含「風險識別」、「風險分析」(**個資檔案風險評估表**)，以及「風險評核」(**決定可接受風險值的紀錄**、超出可接受風險值之**風險處理計畫及核定時間**，都需有負責人、管理人之核可紀錄)

4. 個人資料盤點、管理與紀錄

4.3 依資料屬性訂定管理程序	普中高	資料蒐集、處理及利用管理程序規範 ○無 ○有，檢附相關佐證資料 ○不適用(無明確法規要求)	9

- 檢附同1.1項佐證資料(**個人資料檔案安全維護計畫**)，內容須包含依資料屬性訂定不同管理程序之章節
- 資料屬性：係指一般個人資料及特殊種類個人資料

4. 個人資料盤點、管理與紀錄

4.4 向當事人蒐集個資，或於利用非由當事人提供之個資前，盡告知義務	普中高	向當事人蒐集個資 或 利用非由當事人提供之個資前告知形式(可複選) ☐書面通知 ☐口頭告知 ☐網站公告 ☐個資收集表單 ☐隱私政策聲明 ☐簡訊通知 ☐其他，_____	9

- 勾選告知形式，並檢附對應的佐證資料

✓ 4.4向當事人蒐集個資告知事項.docx

告知當事人下列事項：
一、公務機關或非公務機關名稱。
二、蒐集之目的。
三、個人資料之類別。
四、個人資料利用之期間、地區、對象及方式。
五、當事人依第三條規定得行使之權利及方式。
六、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。

4. 個人資料盤點、管理與紀錄

4.5 檢視蒐集、處理個人資料是否符合個人資料保護法第十九條規定之目的及要件	普中高	適用個人資料保護法第十九條規定之目的及要件 ○無 ○有，檢附以下相關佐證資料(可複選) □安全維護計畫執行之檢查報告 □個資蒐集紙本表單 □個資蒐集系統畫面截圖	10

- 檢附如**安全維護計畫執行之檢查報告、個資蒐集紙本表單、個資蒐集系統畫面截圖**

紙本表單、個資蒐集系統畫面要有蒐集個資告知事項

✓ 4.5個人資料提供同意書.odt

個人資料保護法第十九條

- 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，**應有特定目的**，並符合下列情形之一者：

一、**法律明文規定**。

二、**與當事人有契約或類似契約之關係，且已採取適當之安全措施**。

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、**經當事人同意**。

六、為增進公共利益所必要。

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

八、對當事人權益無侵害。

4. 個人資料盤點、管理與紀錄

4.6 委託他人進行資料蒐集、處理或利用，進行適當監督	普中高	委託他人進行資料蒐集、處理或利用 ○無個資委外 ○有個資委外 1、 委外進行資料蒐集、處理或利用之監督情形近期對委外機構的檢核日期: 年 月 日 2、 委外監督事項應包含個資法施行細則第八條第2項規定： 一、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。 二、受託者就個資法施行細則第十二條第二項採取之措施。 三、有複委託者，其約定之受託者。 四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 五、委託機關如對受託者有保留指示者，其保留指示之事項。 六、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

- 檢附**委外監督紀錄(委外專案受託單位個人資料保護檢查表)**
  - 委外契約內要有**個人資料委外監督及保護條款**

✓ 4.6個人資料委外監督及保護條款.docx

✓ 4.6委外專案受託單位個人資料保護檢查表.ods

4. 個人資料盤點、管理與紀錄

4.7 首次利用個資行銷之當事人確認作業	普中高	○無首次利用 ○有首次利用(可複選) □電子郵件 □書面通知 □簡訊 □電話 □網站公告 □其他，__	12

- 有首次利用個資行銷，請勾選形式，並檢附首次利用個資行銷進行告知紀錄

  個資法第20條

  非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用

首次：第一次利用個資進行行銷活動，即第一次向用戶或客戶發送行銷材料或開始進行行銷活動之前，需要進行的告知作業紀錄

4. 個人資料盤點、管理與紀錄

4.8 確認與維護保有個資之正確性	普中高	為維護保有個資正確性的機制，應主動或依當事人之請求更正或補充之： 受檢單位個資受理窗口： 姓名：_____職稱：_____	12

- 檢附同 1.1 項佐證資料**個人資料檔案安全維護計畫 (要有個資受理窗口姓名、職稱)**
- 如有個資異動，請檢附紙本或電子紀錄

4. 個人資料盤點、管理與紀錄

4.9 針對所屬人員設定不同管理權限，並要求負保密義務	普中高	建立管理機制，設定所屬人員不同之權限 ○無（免附權限管控紀錄） ○有（請檢附權限管控紀錄） 是否有委外廠商/人員 ○無（請檢附所屬人員之保密切結書紀錄） ○有（請檢附所屬人員及委外廠商/人員之保密切結書紀錄） ○不適用(無明確法規要求)	13

保密切結書須涵蓋「所有」接觸個資之專職、兼職，以及工讀生

- 檢附所屬人員所簽訂之**保密切結書**。
- 如有委外，請檢附**委外廠商/人員保密切結書**。
- 如有依人員性質不同而設定對應之權限者，請檢附**權限管控紀錄**， 若勾選無則免附。
  - 公文系統之「帳號權限 設定畫面截圖」、「檔案室／保管箱領用登記表」或「鑰匙管理清冊」。

✓ 4.9保密切結書.docx　4.9應用系統存取權限清單.odt

4. 個人資料盤點、管理與紀錄

4.10 對存有個資之系統設備、媒介物等採取安全管理措施	普中高	系統設備、媒介物(含非電子類)及採取必要之防護措施 ○無 ○有，檢附相關防護措施佐證 ○不適用(無明確法規要求)	13

系統設備：包括桌上型電腦、筆記型電腦、伺服器等

媒介物：硬碟、網路儲存裝置、USB、磁帶、 磁碟、CD、DVD、藍光光碟等

- 私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園者
  - 檢附**媒介物)之防護措施程序**、與相對應之**作業紀**
- 私立兒童課後照顧 短期補習班者
  - 檢附**所屬人員保管個人資料之儲存媒介物之紀錄**，及**保管及保密義務之紀錄**

人員如何保存個人資料的存儲方式記錄(如：電腦每6個月更換密碼、檔案加密、紙本文件加鎖)

➢ 保密切結書

✓ 4.10實體環境管理規範.docx

4. 個人資料盤點、管理與紀錄

4.10 對存有個資之系統設備、媒介物等採取安全管理措施	普中高	系統設備、媒介物(含非電子類)及採取必要之防護措施 ○無 ○有，檢附相關防護措施佐證 ○不適用(無明確法規要求)	13

防護措施舉例

- 資料保存地點進出紀錄：記錄資料存儲地點的出入情況 ➤ 進出紀錄表
- 資料加密紀錄：記錄對資料進行加密的操作和方法。
  - ➤ 開啟檔案需輸入密碼之畫面截圖
- 災害恢復計畫：制定應對災害的恢復計劃，以保護資料安全 ➤ 計畫及演練紀錄
- 監控設備的使用情況：記錄監控設備的使用情況和操作記錄 ➤ 設備的log
- 及時檢測異常行為：監控系統，及時發現和應對異常行為，確保資 料安全。
  - ➤ log(資料的完整性、保存多久，log查檢紀錄

4. 個人資料盤點、管理與紀錄

4.11 存有個資之系統設備、媒介物報廢或轉作他用時，採取適當防護措施	普中高	系統設備、媒介物報廢或轉作他用時之防護措施 1. 紙本、電子資料及設備應訂有銷毀程序 ◯無 ◯有 ◯ 自行清除、處理 ◯ 由委外方清除、處理 清除單位：_____處理單位：_____ ◯不適用(無明確法規要求)	14

- 檢附**個資紙本、電子資料及設備之銷毀作業紀錄、硬體清除紀錄**(如格式化或物理破壞等資料銷毀紀錄)
- 若**勾選有**系統設備、媒介物報廢或轉作他用時之防護措施，紙本、電子資料及設備應訂有銷毀程序者，檢附**電子資料及設備之銷毀程序**
  - 銷毀程序完整性：檢附之銷毀程序書應明確區分不同媒介的處理 方式，如紙本用碎紙方式；電子檔案用格式化方式；硬體設備用消磁或實體破壞方式

✓ 4.11個人資料檔案銷毀申請表.odt

4. 個人資料盤點、管理與紀錄

4.12 留存所有個資使用紀錄、機關設備軌跡紀錄、相關證據紀錄	普中高	安全維護計畫各項程序及措施執行紀錄 ○無執行 ○有，檢附相關保留佐證 受檢單位目前個資保存期限：_____ ○不適用(無明確法規要求)	14

- 檢附留存之**個人資料使用紀錄**、可供證明**系統主機或儲放個人資料之主機軌跡紀錄檔畫面或其他相關資料**
  - 軌跡紀錄範疇：包含**系統登入紀錄、資料查詢紀錄、修改紀錄，以及匯出紀錄**；若**無電子系統**，則檢附**紙本檔案的「存取登記簿」或「調閱申請單」**。
  - 保存期限合規性：受檢單位須明確說明紀錄保存之年限，該年限應明訂於內部個資安維計畫中，且佐證資料需能證明歷史紀錄確實完整保存中。

    ※建議保存年限最少 **5 年**

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

- **防護管理措施**
  - 確認使用者身分及保護機制(帳號申請及異動紀錄及帳號定期盤點紀錄)
  - 個人資料顯示之隱碼機制(螢幕顯示個資畫面截圖或紙本輸出資料隱碼的照片)
  - 網際網路傳輸之安全加密機制(螢幕畫面截圖)
  - 個人資料檔案及資料庫之存取控制與保護監控措施
    (資料檔案及資料存取控制與保護監控畫面截圖或作業紀錄(log))
  - 防止外部網路入侵對策(網路架構圖(含設備資訊-防火牆))
  - 非法或異常使用行為之監控與因應機制(**中高等級**，log紀錄)
  - 定期演練及檢討改善(業務持續演練紀錄及演練後檢討紀錄)

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5.1 使用者身分確認及保護機制	普中高	使用者身分確認及保護機制 ○無，請說明理由_____ ○有，檢附相關佐證資料 ○不適用(無明確法規要求) ○不適用(不符合本項條件)	15

- 有採取使用者身分確認及保護機制，檢附同 1.1 項佐證資料(**個人資料檔案安全維護計畫**)，若勾選無保護機制者請說明理由

  安全維護計畫內要有

  => 帳號申請、建立、修改、啟用、停用及刪除之**程序**，執行**身分驗證管理**，如身分驗證資料不以明文傳輸、密碼複雜度或帳號鎖定機制等

  => 對外電子商務服務系統，具有帳號建立、啟用、修改、刪除的日誌紀錄

- 檢附紙本或電子**帳號申請及異動紀錄**及**帳號定期盤點紀錄**

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5.2 個人資料顯示之隱碼機制	普中高	系統輸出個資(如紙本列印、螢幕顯示)時，以適當隱碼遮罩處理) ◯無 ◯有，隱碼遮罩項目 ☐身份證字號 ☐姓名 ☐其他，_____ ◯不適用(無明確法規要求) ◯不適用(不符合本項條件)	16

- 檢附**螢幕截圖畫面**或是**紙本輸出資料的隱碼作為**
  - 隱碼遮罩：如遮罩身份證後四碼，如 A223456789 --> A22345****

✓ 5.2隱碼機制.docx

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5.3 網際網路傳輸之安全加密機制	普中高	網路傳輸加密機制 ○ 無傳輸加密 ○ 有傳輸加密，傳輸加密 ☐ SSL/TLS ☐ VPN

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5.4 個人資料檔案及資料庫之存取控制與保護監控措施	普中高	○存放個資之系統，資料庫存取控制與保護監控措施形式(可複選) □強化身份驗證 □存取紀錄 □權限管理 □安全訪問控制 □系統日誌 □資料庫加密 □定期漏洞掃描 □其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	17

- 檢附**資料檔案及資料存取控制與保護監控截圖畫面或作業紀錄(log)**

✓ 4.10實體環境管理規範.docx

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

- 個人資料檔案及資料庫之存取控制與保護監控措施
  - 強化身份驗證：實施身份驗證，確保僅授權用戶可以訪問資料庫 ➢ **資料庫登入畫面**
  - 存取紀錄：記錄資料庫的存取記錄，追蹤用戶對資料的操作和變更 ➢ **資料庫log**
  - 權限管理：設置資料庫用戶的權限，限制其對敏感資料的存取 ➢ **帳號權限清查紀錄**
  - 安全訪問控制：實施訪問控制策略，限制訪問資料庫的 IP 地址範圍或時間段。
    ➢ **防火牆規則**
  - 系統日誌：定期審查系統日誌，監控資料庫的存取和活動，檢測異常行為。
    ➢ **資料庫log**
  - 資料庫加密：對整個資料庫或特定欄位進行加密，以保護資料在儲 存和傳輸時的安全性 ➢ **欄位加密儲存畫面截圖**
  - 定期漏洞掃描：定期對資料庫進行漏洞掃描，及時發現並修補安全 漏洞。
    ➢ **弱點掃描報告，初測及複測**

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5.5 防止外部網路入侵對策	普中高	○有系統，防止外部網路入侵對策形式(可複選) □防火牆 □防毒 □入侵防護IPS / 入侵偵測IDS □內外網路區隔 □其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	18

- 檢附受檢單位**網路架構(含設備資訊)**
  - **防火牆**：監控和控制網路流量，阻止未經授權的訪問。
  - 防毒：掃描、檢測和清除電腦系統中的惡意軟體和病毒。
  - 入侵防護 IPS / 入侵偵測 IDS：監控網路流量，檢測和防止潛在的 入侵和攻擊。
  - **內外網路區隔**：分隔內部網路和外部網路，限制內部資源的外部訪問，提高安全性
  - **網路架構圖(有防火牆)、電腦防毒軟體畫面截圖**

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5.6 非法或異常使用行為之監控與因應機制	普中高	○有系統，監控作業形式(可複選) □LOG(日誌) □自動警示機制 □存取控制 □行為監控系統 □行為分析 □其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	18

- 檢附**監控紀錄**，或其他資料如行為監控分析紀錄
  - LOG(日誌)：記錄作業系統或應用程序或防火牆/入侵偵測或WEB 服務...等等運行時事件、錯誤和警告之檔案。
  - 自動警示機制：系統自動偵測異常情況，發出警示訊息以提醒操作者或管理者。
  - 存取控制：管理和限制使用者對資源或功能的存取權限，以確保資料安全。
  - 行為監控系統：追蹤使用者行為，監控系統內的活動，並檢測異常行為。
  - 行為分析：分析使用者行為模式，檢測異常或可疑活動，以提早發現安全風險。
- 因應機制之佐證：若發生異常，應檢附「**異常事件處理紀錄**」相關資料；若無異常，則建議檢附「**異常演練紀錄**」或「**定期監控分析報告**」

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

5.7 定期演練及檢討改善	普中高	定期演練情形 ○無 ○有，演練日期：　年　月　日 檢討日期：　年　月　日 ○不適用(無明確法規要求) ○不適用(不符合本項條件)	19

- 檢附**演練紀錄**(如資料毀損、個資外洩、外部網路入侵、非 法或異常使用行為、系統服務中斷、勒索軟體攻擊、垃圾郵件、釣魚攻擊、 社交工程攻擊、自然災害等情況)、**演練後檢討紀錄**。
  - 建議演練主題應對應「4.2 風險分析及管控措 施」中所列的高風險項目
  - 演練紀錄應呈現不同角色的分工，如：發現者、通報者、決策者、執行者
  - 演練後須檢附「檢討紀錄」，內容應誠實記錄**演練中發現的缺失**（如：人員通報過慢、備份還原時間過長），並提 出**對應的「改善措施」與「追蹤紀錄」**

✓ 5.7個資安全事件緊急應變計畫(演練).odt

6. 環境管理措施

6. 環境管理措施

6.1 對個資存取媒介物及環境(如機房、雲端)，採取環境管理措施	中高	個資存取媒介物及環境(如機房、雲端、媒介物保存櫃)管理措施 ◯無 ◯有，檢附相關資料 ◯不適用(無明確法規要求)	20

- 檢附同 1.1 項佐證資料 (**個人資料檔案安全維護計)**。
  - 等級 **中**：建議檢附如**存取記錄**(重要區域人員進出紀錄等方式)、**可攜式媒體申請管控紀錄、安全事件記錄、資料備份記錄**
  - 等級 **高**：**除等級中檢附之資料外**，併請**檢附**如**合規性文件**(如安全執照和標準遵循證書(資通環境安全相關第三方驗證證書))

✓ 6.1辦公室安全檢查表_v1.0.docx

6. 環境管理措施

6.1 對個資存取媒介物及環境(如機房、雲端)，採取環境管理措施	中高	個資存取媒介物及環境(如機房、雲端、媒介物保存櫃)管理措施 ◯無 ◯有，檢附相關資料 ◯不適用(無明確法規要求)	20

- 存取記錄：記錄存取系統或場所的人員和時間。
- 安全事件記錄：記錄發生的安全事件、日期和相關細節。
- 資料備份記錄：記錄資料備份的時間、方式和存儲位置。
- 設備維護記錄：記錄設備的維護歷史、維修情況和日期。
- 可攜式媒體申請管控紀錄：記錄申請使用可攜式媒體的用途、審批和使 用情況。
- 合規性文件：確保組織符合相關法規的文件，如安全執照和標準遵循證書(資通環境安全相關第三方驗證證書)。ISO27001 ISO27701

7. 業務終止之個資管理

7. 業務終止之個資管理

7.1 訂有業務終止之個資處置措施	普中高	業務終止之個資處置措施程序 ○無 ○有，檢附相關資料 ○不適用(無明確法規要求)	21

- 檢附同 1.1 項佐證資料 **(個人資料檔案安全維護計畫)**
- **屬於私立兒童課後照顧服務中心、短期補習班者**
  - 檢附**定期向負責人報告之紙本或線上紀錄**，若因無異動而未報告仍需提供 前次報告紀錄

7. 業務終止之個資管理

7.2 留存相關紀錄	普中高	○無業務中止 ○有， 請列舉本年度業務中止之個資檔案清冊： _____	21

- 如有業務中止，請列舉**本年度業務中止之個資檔案清冊**
  - 業務中止後之處置證明：針對中止業務所留下的個資，需註明處置方式並檢附紀錄，例如銷毀需檢附銷毀紀錄與照片；移交需檢附移交簽收清單等
  - 紀錄至少留存五年

8. 事故通報與應變程序

8. 事故通報與應變程序

- 訂定個資洩漏等事故發生或知悉起72 小時內通報流程
- 訂定對個資洩漏等事故採應變措施以控制損害
- 訂定查明事故後以適當方式通 知當事人之程序並告知已採取因應措施
- 研議預防機制

8.1事故通報紀錄表單.pdf

8. 事故通報與應變程序

8.1 訂定個資洩漏等事故發生或知悉起72小時內通報流程	普中高	1.訂定個人資料事故通報作業規範/應變機制 ◯無 ◯有，檢附相關資料 ◯不適用(無明確法規要求) 2.截至填報日期前本年度事故 ◯無事故發生 ◯曾有事故者，事故發生次數_____，最近一次事故通報日期:_____，檢附相關資料	22

- 檢附同 1.1 項佐證資料 (個人資料檔案安全維護計畫)
  - **無個資洩漏事故**者，請檢附**空白事故通報紀錄表單**，建議應進行單位模擬演練事故及通報模擬之作業。
  - **有個資洩漏事故者**，請填寫近期事故通報日期、年度事故發生次數並檢附**事故通報紀錄**

✓ 8.1事故通報紀錄表單.pdf

8. 事故通報與應變程序

- 通報對象之明確性：**流程應清楚列出內外部通報窗口。內部包含「個資保護專責人員」及「負責人」；外部則應列出主管機關**之 聯繫電話或線上通報系統網址。
- 空白表單之完整性：「**空白事故通報紀錄表單」內容應包含**：事 故發生時間、發現時間、影響人數、外洩個資類別、預計採取的 補救措施，以及應變通知方式。

8. 事故通報與應變程序

8.2 訂定對個資洩漏等事故採應變措施以控制損害	普中高	訂定個資洩漏等事故應變措施 ○無 ○有，檢附相關資料 ○不適用(無明確法規要求)	22

- 檢附同 1.1 項佐證資料(**個人資料檔案安全維護計畫**)

8. 事故通報與應變程序

8.3 訂定查明事故後以適當方式通知當事人之程序並告知已採取因應措施	普中高	訂定事故應變機制對通知當事人之程序及規範 ○無 ○有，檢附相關資料	22

- 檢附同 1.1 項佐證資料 (**個人資料檔案安全維護計畫**)
- **如有發生過事故，向當事人說明事件緣由及防護措施之通知紀錄**
  - Email、簡訊、網頁公告

8.4持續改善措施單.docx

8. 事故通報與應變程序

8.4 研議預防機制	普中高	應變機制之矯正預防程序 ○無事故發生 ○有事故者，事故案發日期：_____ 矯正預防紀錄最近日期：_____ ○不適用(無明確法規要求)	23

- 檢附同 1.1 項佐證資料(**個人資料檔案安全維護計畫**)
- 組織如**有發生事故**，檢附**矯正預防單(含預防機制說明)**
  - 8.4持續改善措施單.docx

9. 資安檢測

9. 資安檢測

- 系統弱點掃描
  - 主機、應用程式(網站)
- 滲透測試
- 資安健診
  - 網路架構檢視、網路惡意活動檢視(有線)、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、錄伺服器設定檢視、防火牆連線設定檢視、資料庫安全檢視
- APP檢測

9. 資安檢測

9.1 系統弱點掃描	普中高	如有自行開發或委外之資訊系統，若屬於服務型系統，請依下列事項： ◯無 ◯有處理個人資料之資訊系統 ◯未執行弱點掃描 ◯弱掃日期：_____ 弱掃執行人員/機構名:_____ 修補日期：_____	24

- 檢附 弱點掃描紀錄、修補紀錄
  => 主機、應用程式(網站)
  - 僅針對有處理個人資訊之資訊系統執行弱點掃描，**紀錄應有**日期及執行人員
  - 有中等級(含)以上風險**尚未修補完成**者，**需有預計改善方式及預計完成日期**
  - 修補完成後，建議**複測**，以**驗證修補成效**

9. 資安檢測

9.2 滲透測試	普中高	◯無 ◯有處理個人資料之資訊系統， ◯未執行滲透測試 ◯滲透測試日期：_____ 執行人員/機構名稱:_____	24

- 檢附**透測試紀錄**(具有**執行日期及執行人員/機構**)
  - 僅針對有處理個人資訊之資訊系統執行滲透測試

9. 資安檢測

9.3 資安健診	普中高	○無 ○資安健診日期：_____ 執行人員/機構名稱:_____ 資安健診項目(可複選) ☐網路架構檢視 ☐網路惡意活動檢視(有線) ☐使用者端電腦惡意活動檢視 ☐伺服器主機惡意活動檢視 ☐目錄伺服器設定檢視 ☐防火牆連線設定檢視 ☐資料庫安全檢視 ☐其他，_____	24

- 檢附**資安健診紀錄**(具有**日期及執行人員/機構**)

9. 資安檢測

9.4 APP檢測	普中高	如有自行開發或委外之APP，若為服務型使用，請依下列事項填寫： ◯無 ◯有APP，檢測紀錄日期：_____ 執行人員/機構名稱:_____	25

- 檢附**APP 檢測紀錄**(具有**日期及執行人員/機構**)

  檢測 單位須符合數位發展部數位產 業署推動行動應用App 基本資安 制度推動委員會所認可之「行動 應用App 資安認驗證制度認可實驗室

Q & A

謝謝您的聆聽