編號	查核項目	需改善機構(代碼)	檢附資料說明(修正意見)
1	1.1 是否指定專人或專責單位，負責辦理個人資料保護管理政策之研議、認知宣導與教育訓練、資料與設備安全管理、稽核等工作事項？	T3、T21	明列專責單位名稱/人員
2	1.2 是否有個人資料管理人員組織配置？並依分工執行？	T3、T5、T10、T12、T18、T19、T21	檢附管理人員分工表
3	1.3 是否有個人資料保護管理政策？是否公告公司人員周知？	T2、T3、T4、T5、T7、T10、T14、T16、T17、T21	檢附個資保護管理相關規範/周知佐證
4	1.4 就個人資料之蒐集、處理及利用是否有相關程序規定？是否公告公司人員周知？	T2、T3、T4、T5、T7、T10、T14、T16、T17、T21	檢附個資蒐集、處理及利用相關程序/周知佐證
5	1.5 是否進行個人資料盤點並備有清冊？盤點之方式為何？結果之正確性？	T1、T2、T4、T5、T8、T9、T10、T13、T14、T18、T19、T21	說明盤點方式 /檢附盤點清冊
6	2.1 是否進行個人資料風險評估並進行相應處理？風險評估之方式？結果之正確性？	T1、T2、T3、T5、T7、T8、T10、T13、T14、T16、T19、T21	檢附個資風險評估規定 /風險評估表單
7	2.2 是否訂定風險處理計畫，並根據該計畫導入控制措施，以降低風險？	T1、T8、T14、T21	檢附風險處理計畫
8	3.1 針對個人資料事故是否有可行之應變機制？	T3、T8、T19、T21	明列應變機制相關規定
9	3.2 發生個人資料事故時，是否適時以適當方式通知當事人相關事故事實、因應措施及諮詢服務專線等？	T1、T2、T3、T5、T7、T8、T11、T12、T13、T19、T20、T21	明列通知方式、因應措施及諮詢服務專線
10	3.3 是否訂有檢討預防機制，避免類似事故再次發生？	T3、T8、T19、T21	檢附預防機制規定

編號	查核項目	需改善機構(代碼)	檢附資料說明(修正意見)
11	3.4 發現個人資料事故時，是否於 72 小時內填具通報紀錄表，通報所在地之直轄市、縣（市）政府，並副知中央目的事業主管機關？	T5、T7、T8、T10、T13、T19、T21	檢附私立職業訓練通報紀錄表
12	4.1 有無蒐集、處理或利用特種個人資料？如有，其蒐集、處理、利用及其他相關規定是否已遵守？	T2、T6、T9、T10、T17	檢附個資使用同意書
13	4.2 是否進行告知？如否，有無法定免告知事由？告知之時點與方式是否合法、適當？	T2、T5、T6、T8、T9、T10、T17、T21	檢附個資使用同意書
14	4.3 蒐集、處理或利用個人資料是否具備並符合特定目的及特定情形？是否遵守其他依法令應遵守之事項？	T2、T6、T8、T9、T10、T17、T21	檢附個資使用同意書
15	4.4 是否有特定目的外利用？如有，是否有合法事由？	T6、T10	應敘明是否有特定目的外之利用
16	4.5 是否進行行銷？行銷是否符合特定目的？如進行行銷，是否提供當事人拒絕行銷之管道？是否於當事人拒絕行銷時，停止行銷？	T6、T10	應敘明是否進行行銷並檢附相關拒絕行銷管道之佐證
17	4.6 如何決定是否委外？委外時如何選任受託人？與受託人間是否就個人資料保護法要求事項簽訂合約或設計監督規劃？	T6、T8	應敘明是否委外，並檢附相關作證
18	4.7 是否進行個人資料國際傳輸？是否於傳輸前檢視有無中央目的事業主管機關依個人資料保護法第 21 條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域？	T6、T7、T8、T12	應敘明適用/不適用原因，如有國際傳輸，應檢附外部傳送相關規定及告知傳輸目的之佐證

編號	查核項目	需改善機構(代碼)	檢附資料說明(修正意見)
19	4.8 對資料接收方預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式是否有監督機制？是否監督資料接收方有提供當事人行使個人資料保護法第 3 條所定權利等相關事項之機制？	T5、T6、T7、T8	如不適用應敘明清楚，如適用應檢附相關佐證及監督機制
20	4.9 是否提供當事人權利行使管道？是否於法定期限內回復當事人？如展延回復，是否依法定要式為之？拒絕當事人時是否有合法事由？	T4、T5、T7、T8、T9、T10、T21	應敘明適用/不適用原因及提供權利行使管道佐證
21	4.10 是否主動更正或補充當事人之個人資料？	T6、T8、T18	應敘明不適用原因
22	4.11 是否曾（合法）提供資料予第三人？如提供內容有誤或不備之資料如何通知更正？	T6	應敘明不適用原因
23	4.12 特定目的消失或期限屆至時，是否刪除、銷毀、停止蒐集、處理、利用個人資料？如否，有無法定事由？	T2、T5、T10、T13、T14、T15、T18	應檢附相關保密切結書或銷毀紀錄表之佐證
24	4.13 業務終止時是否對個人資料進行妥善、合法之安排？	T1、T2、T5、T8、T10、T14、T15、T18、T21	應敘明相關規定，並檢附銷毀紀錄表之佐證
25	4.14 是否定期檢視個人資料管理之狀況並持續改善？	T1、T2、T4、T5、T7、T8、T10、T14、T15、T18、T19、T20、T21	應檢附盤點清冊相關佐證
26	4.15 委託關係終止或解除時，是否確認受託者返還個人資料之載體，及刪除履行契約以儲存方式而持有之個人資料？	T2、T5、T10、T13、T15	應檢附相關切結書佐證

編號	查核項目	需改善機構(代碼)	檢附資料說明(修正意見)
27	5.1.1 是否訂定適用之資訊安全注意事項並公告周知？	T1、T10、T20	應提供公告佐證
28	5.1.2 運用電腦或自動化機器相關設備，是否訂定使用可攜式設備或儲存媒介物之規範？	T2、T4、T8、T14、T17、T19、T20、T21	應訂定使用規範
29	5.1.3 保有之個人資料內容，是否採取適當之加密或遮蔽機制？	T2、T3、T4、T5、T9、T14、T17、T21	應提供遮蔽/加密畫面
30	5.1.4 傳輸個人資料檔案時，是否採取安全加密機制？是否確認資料收取者之正確性？	T2、T3、T4、T9、T21	應提供相關佐證畫面
31	5.1.5 依據保有資料之重要性，評估有備份必要時，予以備份，是否比照原件加密？儲存備份資料之媒介物，是否以適當方式保管？是否定期進行備份資料之還原測試，以確保有效性？	T1、T2、T3、T4、T5、T7、T8、T9、T10、T14、T16、T19、T20、T21	應提供近期還原測試紀錄
32	5.1.6 儲存個人資料之媒介物於報廢或轉作其他用途時，以物理或其他方式是否確實破壞或刪除媒介物中所儲存之資料？	T2、T3、T4、T5、T8、T9、T10、T14、T20、T21	應提供近期報廢紀錄
33	5.1.7 是否妥善保存管理機制及加密機制中所運用之密碼？	T14	應敘明相關規範及佐證
34	5.2.1 是否確認蒐集、處理及利用個人資料之各相關業務流程之負責人員？	T3、T21	明列專責單位名稱/人員
35	5.2.2 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工，是否有妥適分工與分散權責？是否定期確認權限內容之適當性及必要性？	T3、T5、T10、T12、T18、T19、T21	應檢附檢附管理人員分工說明書

編號	查核項目	需改善機構(代碼)	檢附資料說明(修正意見)
36	5.2.3 被賦予敏感資訊存取權之所有員工，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？	T1、T5、T10、T19	應檢附個資管理人員保密協議書/切結書
37	5.2.4 員工離職時，是否取消其識別碼？是否依規定繳回其通行證(卡)及相關證件？	T2、T3、T4、T5、T7、T8、T9、T10、T14、T19、T20、T21	應提供員工離職程序表或其佐證
38	5.2.5 員工離職時，是否依規定繳回其使用或保管之個人資料？	T2、T3、T4、T5、T7、T8、T9、T10、T14、T19、T20、T21	應提供員工交接表或其作證
39	5.3.1 依據作業內容不同、作業環境及個人資料之種類與數量，實施必要之門禁管理？	T2、T4、T5、T17、T21	應提供運用相關佐證
40	5.3.2 是否以適當方式或場所保管個人資料之儲存媒介物？	T4、T5、T14	應提供運用相關佐證
41	5.3.3 針對不同作業環境，是否加強天然災害及其他意外災害之防護，並建置必要之防災設備？	T2、T3、T4、T5、T19、T20、T21	應提供運用相關佐證
42	5.4.1 是否於電腦、自動化處理設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別及控管？	T3、T5	應提供截圖佐證
43	5.4.2 認證機制使用之帳號及密碼，是否具備一定之複雜度，並定期更換密碼？	T3、T5	應提供截圖佐證
44	5.4.3 是否於電腦、自動化處理設備或系統上設定警示與相關反應機制，以對不正常之存取進行適當之反應及處理？	T3、T20	應提供截圖佐證

編號	查核項目	需改善機構(代碼)	檢附資料說明(修正意見)
45	5.4.4 個資存取權限之數量及範圍，是否依作業必要予以設定？是否禁止共用帳戶和密碼？	T3、T5	應提供運用佐證
46	5.4.5 是否採用防火牆或入侵偵測等設備，避免儲存個人資料之系統遭受無權限之存取？	T2、T3、T4、T5、T14、T17、T19、T21	應提供運用佐證
47	5.4.6 使用能存取個人資料之應用程式時，是否確認使用者具備使用權限？	T3、T14、T19、T20、T21	應提供運用佐證
48	5.4.7 是否定期測試權限認證機制之有效性？	T1、T2、T3、T4、T5、T7、T9、T10、T14、T17、T19、T20、T21	應提供運用佐證
49	5.4.8 是否定期檢視個人資料之存取權限設定？	T1、T2、T3、T4、T5、T7、T9、T10、T14、T17、T19、T20、T21	應提供運用佐證
50	5.4.9 是否於處理個人資料之電腦系統中安裝防毒、防駭軟體？是否定期更新病毒碼？	T4、T5、T9	應提供運用佐證
51	5.4.10 對於電腦作業系統及相關應用程式之漏洞，是否定期安裝修補程式？	T4、T5	應提供運用佐證
52	5.4.11 對於具備存取權限之電腦或自動化處理設備，是否禁止安裝檔案分享軟體？	T1、T20、T21	應提供運用佐證
53	5.4.12 測試處理個人資料之資訊系統時，是否不使用真實個人資料？有使用真實個人資料之情形 時，是否明確規定使用程序？	T1、T3、T7、T17、T19、T20	應提供測試畫面紀錄
54	5.4.13 處理個人資料之資訊系統有變更時，是否確認其安全性並未降低？	T1、T3、T17、T19、T20	應提供測試畫面紀錄

編號	查核項目	需改善機構(代碼)	檢附資料說明(修正意見)
55	5.4.14 是否定期檢查處理個人資料資訊系統之使用狀況，及個人資料存取情形？	T1、T2、T3、T4、T5、T7、T8、T9、T10、T14、T15、T16、T17、T19、T20	應提供檢查紀錄
56	6.1 管理階層是否有要求員工，依照公司訂定之政策及程序施行安全事宜？	-	-
57	6.2 是否對所有員工提供個人資料保護認知宣導及教育訓練？	T2、T5、T8、T10、T14、T16、T17、T18、T19、T21	應提供教育訓練或宣導佐證
58	7.1 是否保存「因應事故發生所採取之行為、受託者執行委託人要求之事項、提供當事人行使之權利、個人資料之維護及修正、所屬人員權限之異動、所屬人員違反權限之行為、備份及還原之測試、個人資料之交付及傳輸、個人資料之刪除、銷毀或移轉、存取個人資料者之資訊、定期檢查處理個人資料之資訊、教育訓練、計畫稽核及改善措施之執行紀錄」5 年？	T1、T2、T3、T4、T5、T6、T7、T8、T10、T13、T14、T16、T19、T20、T21	應提供個資保護管理運作紀錄或稽核紀錄或年度資訊安全報告等佐證