大同技術學院

委訓機關個人資料管理規定

大同技術學院

中華民國104年3月31日

目　次

壹、製作依據

一、本程序書制定之法律依據

(一) 個人資料保護法 99 年 5 月 26 日總統公告版本

(二) 個人資料保護法施行細則，法務部於 101 年 9 月 26 日公告之修正版本。(法令字第 10103107360 號)

二、 程序書制定參考

(一) 法務部公務機關保護執行程序暨管考手冊

(二) 研考會個人資料保護參考指引 101 年

貳、製作目的

本程序書在規範委訓單位(包括彙管單位、辦訓單位等)，供委訓單位進行委訓作業之個人資料管理作業，以符合本校對委訓單位之管理要求。

本程序應管理範圍，應至少包括

一、與本校委託業務有關之所有資料，包括

(一)紙本

(二)電子檔案

(三)相關網站、系統等資料檔案

(四)備份檔案

二、與處理本校委託業務有關之系統，包括

(一)伺服器或檔案主機系統

(二)網站系統

(三)處理學員資料、電子檔案之個人電腦或主機

三、與處理本校作業有關之人員

(一)正職人員

(二)約聘僱人員，包括工讀生

(三)其他委託或合作單位之人員(接觸本校資料者)

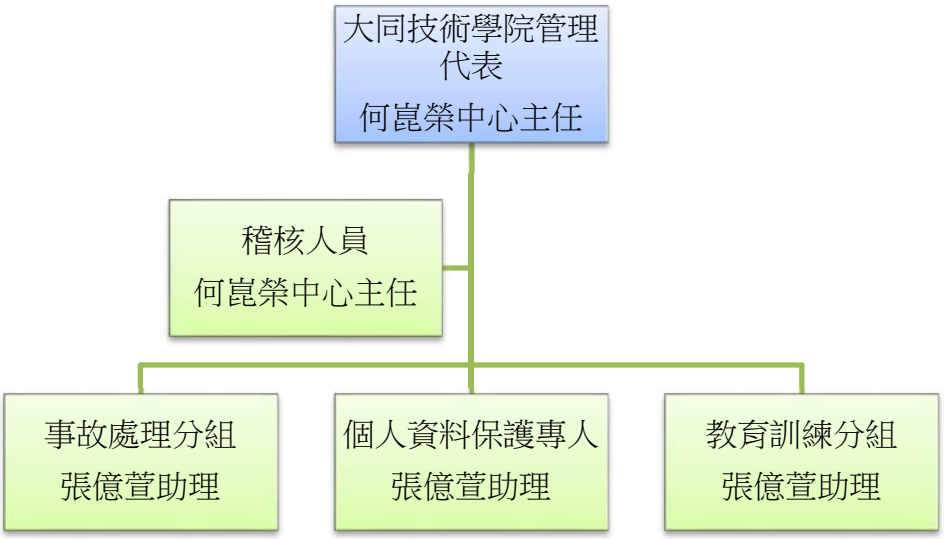
參、個人資料保護管理政策及組織

一、制定依據

大同技術學院承辦勞動力發展署之訓練作業，依據及依個人資料保護法、個人資料保護法施行細則及勞動力發展署對於委外單位之個資保護要求，制訂本個人資料保護管理政策(以下簡稱本政策)。

二、管理組織

本校於組織內設立個人資料保護執行小組負責推動個資保護管理事宜，本管理組織結構如下表:



(一) 組織管理代表

1.本校何崑榮中心主任為本校個人資料保護小組之管理代表

2.提供充分人力及資源確保個人資料保護管理組織之運作

3.核准個資保護管理政策及相關個資管理程序及辦法

4.確認個人資料安全內部稽核結果及改善結果

(二)個資保護專人

1.設個資保護專人一人，由管理代表任命。目前由本校張億萱助理擔

任。

2.負責個人資料之例行作業之管理及執行，其作業包括

(1)維護相關個資管理程序及辦法

(2)進行年度之個人資料風險評估及風險管理

(3)維持本校資料安全及設備之安全

(4)執行勞動力發展署所規定之資訊安全要求

(5)接受當事人權利行使作業申請

(6)負責與勞動力發展署之監督回報作業

(7)持續改善本校之個人資料管理流程

(8)協助事故處理分組與教育訓練分組

(9)內部個人資料法律問題諮詢窗口

(10)與勞動力發展署溝通個人資料保護事宜

(三)稽核人員

本校稽核人員，負責查核本校人員及業務執行是否符合本管理規定及勞動力發展署之各項規定。(由於其職務需求之獨立性，稽核人員並不得與個資專人相同)

1.負責本校個人資料保護管理制度之內部稽核作業

2.接受管理代表委任進行稽核結果之執行確認及結案

3.擬定稽核計畫

4.任命執行稽核人員(如必須)

5.對執行稽核人員進行教育訓練

6. 管理及稽核人員及稽核執行

7. 於稽核結果產出後向管理代表報告稽核結果

(四)教育訓練分組

1.教育訓練分組由本校組織代表進行任命，目前由張億萱助理擔任

2.每年依據個人資料保護法、勞動力發展署之要求、以及本校之安全保護需求擬定教育訓練計畫

3.負責執行個人資料保護教育訓練

4.評估教育訓練成效

(五)事故管理分組

1.事故管理分組由本校組織代表進行任命，目前由張億萱助理擔任

2.負責個資事故之預防、應變及處理作業

3.與資訊部門協同處理個資事件

4.依規定進行事故之通報，包括對勞動力發展署以及其他政府規定之通報

5.查明個資事故之發生原因並向個資專人及管理代表報告

6.進行個人資料事故後對於受影響民眾之通知

三、政策之制訂與管理

(一)政策之制定

本校之政策制定由個資保護專人擬定，經由管理代表核定，公布後實施。

(二)政策之執行

本政策於管理代表核定後公布實施，所有校內與個人資料保護相關之作業，均應遵循本政策。

本政策之執行由個資保護專人進行規劃，並由各單位協助政策之推行。

個資保護專人應定期進行對於政策遵循的查核，以確保政策之執行成效。

(三)政策修改與調整

個資保護專人應於每年或於個人資料保護法相關法規有重大變化後審視及修訂本政策，以確保本政策之適用性。

四、政策內容

為確保本校之業務執行，使本校業務資訊管理作業符合個人資料保護法之規定，確保學員之隱私及相關權益，訂定此個人資料保護管理政策，本校所有人員於執行個人資料保護相關業務時應遵循此政策。

(一)個人資料之保護應兼顧保護學員隱私、滿意及本校業務之順利推行。

(二)本校所有業務及資料處理僅於合於法令、勞動力發展署相關規範要求及本政策規範下執行。

(三)個人資料之蒐集、處理、利用僅在本校及受委託執行業務之特定目的範圍內進行，超出特定目的外的利用應遵循個資法之相關規定。

(四)資訊系統及作業流程應確保個人資料之正確性，並符合資訊安全要求之機密性、完整性及可用性。

(五)資訊系統及作業流程設計應儘可能確保可歸責性及保存合宜之軌跡資料及使用紀錄。

(六)應適當公開個人資料之蒐集、處理及利用過程，使當事人知悉本校之作業及個人資料之保護方式。

(七)本校所有作業應於法定執掌之必要範圍內蒐集、處理個人資料。

(八)本校個人資料之保存應符合法律及本校業務需求之期間，並確保個資的保存達到法定要求之最小期限。

(九)個人資料交付或傳輸予本校以外之組織或個人，應究其合目的性及合法性，並考量資訊傳輸之安全性後始得交付。

肆、個人資料蒐集、處理及利用管理程序

一、招生管理

本校依據勞動力發展署各項規定進行對外招訓作業，招生人員應遵守

(一)職訓補助或勞動力發展署核定本校執行之課程(以下稱勞動力發展署委訓課程)，包括以下作業，均為勞動力發展署依據其職權之委外作業，本校於執行下列業務時，視同勞動力發展署，應遵守個資法公務組織之規定、勞動力發展署之各項規定及本管理規定辦理。本校辦理勞動力發展署委託之訓練項目包括:

1.執行小型企業人力提升計畫之各項課程

2.青年就業站之各項電腦課程

(二)於所有招生之文件，包括文宣品、廣告、網站、電子文件(包括檔案、電子郵件)、電子訊息(簡訊、其他類電子傳訊工具)等說明，應清楚說明本校之課程與勞動力發展署之委託關係。

(三)所有委訓課程之個人資料管理作業，其蒐集主體均為勞動力發展署，本校受勞動力發展署或彙管單位之委託及依據其規定進行對於該參訓學員資料之蒐集、處理、利用，但非為該個人資料之擁有者。

(四)所有委訓課程之個人資料之歸屬權屬於勞動力發展署，本校所有人員(包括正職、約聘雇、工讀生或兼任講師、訓練員)，均不得於勞動力發展署委託範圍外處理或利用該個資。

二、報名管理

本校於執行勞動力發展署委訓課程之報名作業應注意以下事項:

(一)所有表單，均應以合宜之方式說明或提示勞動力發展署為資料之蒐集者，本校為委訓單位或受委託執行本業務之組織。

(二)所有報名作業，均依據勞動力發展署所規範之欄位進行蒐集，非規範之欄位，本校一律不予蒐集。

(三)本校因業務執行之因素如需蒐集勞動力發展署規範以外之參訓學員個人資料項目，應事先以書面方式取得勞動力發展署承辦人員之同意。

(四)報名作業留存之各項紀錄，包括書面紙本、電子檔案、網頁紀錄(包括可能之 Log)均需妥善保管，並列入本校年度個人資料盤點作業。

(五)報名作業如為委託或與其他單位共同辦理(不計入勞動力發展署統一辦理之報名管道)，應注意於報名作業結束後該資料是否留存於委託或共同辦理單位，如該單位需要留存勞動力發展署委訓課程之資料，應依據本管理規定之委外管理程序辦理。

(六)本校如需於勞動力發展署委訓課程參訓學員報名作業中進行本校之蒐集作業，應另外以明確告知之方式使參訓學員理解本校為該蒐集作業之蒐集主體，並依據個人資料保護法之規定(包括告知或得同意等規定)進行蒐集，不得與勞動力發展署委訓課程之報名流程混淆，本校之蒐集部分，不得作為參加勞動力發展署委訓課程之必要條件。

三、系統及學員資料管理

本校依據勞動力發展署之報名作業規定，需將資料於學員報名後，鍵入勞動力發展署指定之電腦系統，由勞動力發展署進行後續之資料處理作業，有關學員資料管理應注意事項包括:

(一)現場作業

1.所有現場之紙本作業、電子檔案以及各類可能留存參訓學員資料之各式媒體，均應妥善保存，避免未授權之存取。

2.現場櫃台處理報名作業，應注意相關紙本或電子檔案，系統螢幕畫面於作業中被其他人員窺視或竊取之可能。

(二)紙本及實體儲存媒體之保護

1.相關資料紙本及儲存媒體，於作業完成後，均應依據本校規定，存放於安全區域或上鎖以確保該等資料之保護。

2.於報名作業產出之學員資料影印本或作廢但含有學員資料之紙本，應以碎紙方式或其他可以去除紙本上之學員資料進行該紙本之處理，本校嚴禁將含有學員個人資料之紙本逕行回收再利用或廢紙回收。

3.作業中產出之學員報表紙本，於確定其不再使用或無保存之目的後，應碎紙方式進行銷毀，確保不產出額外之風險。

4.運用於課程管理或學員管理之紙本或電子檔案，於確定其不再使用或無保存之目的後，應碎紙方式進行銷毀，確保不產出額外之風險。

(三)電子檔案及系統使用

1.學員資料電子檔案不得存放於未設定密碼(未有存取控制)之公共空間。

2.處理學員報名作業之電腦，應設定螢幕保護程式及保護密碼，本校螢幕保護程式啟動之時間為 10 分鐘。

3.因作業處理產出之學員資料報表電子檔案，於確定其不再使用或無保存之目的後，應予以刪除，確保不產出額外之風險。

4.勞動力發展署相關系統之帳號，應避免共用帳號，以確保資料存取之授權及可歸責性，如因作業需要或系統限制需要共用帳號密碼，應以其他管制配套，確保該共用作業於核准及監視管制下進行。

(四)存取控制:

1.對於參訓學員資料之存取控制，應以業務所必須進行權限分配，未授權之人員，不應取得紙本或電子資料之存取權限。

2.學員資料電子資料檔案應記錄存取人員、存取時間。

3.本校每半年進行學員資料系統之系統存取權限，確保存取權限之開放均符合人員之業務需求。

(五)使用電子郵件及傳送訊息

1.個人資料之電子形式傳遞，應予加密或亂數化處理後傳送。

2.所有學員資料透過電子郵件或其他傳訊工具進行傳遞，應最少以 Winzip 等工具進行通行碼(password)的保護，密碼並應以另一封郵件或訊息傳遞。

(六)個人資料實體形式封裝應由本校承辦人員封裝於傳遞信封內，外觀上不得標示其他足以顯示個人資料內容之註記。

(七)個人資料於各類傳遞前應記錄相關傳遞細節以供日後查閱。

四、學員資料利用管理

勞動力發展署委託本校辦理之委訓課程，其學員資料係屬於勞動力發展署,本校僅得於勞動力發展署委託之範圍處理或利用委訓課程學員資料。本校人員應遵使以下利用管控事項:

(一)本校僅於合於個人資料保護法以及勞動力發展署之規範下利用學員資料。

(二)於進行各項利用前，應確認該利用符合勞動力發展署之委託範圍、勞動力發展署之特定目的。

(三)如有超出勞動力發展署之委託範圍、勞動力發展署之特定目的以外之利用，應事先以書面方式取得勞動力發展署承辦人員之同意。如該利用為臨時個案，應至少以口頭或電子郵件方式取得勞動力發展署承辦人員之同意後辦理。

(四)超出勞動力發展署及彙管單位以外之單位對本校提出學員資料存取或調閱，應事先以書面方式取得勞動力發展署承辦人員之同意後辦理。大量資料之要求，應會同本校個資保護專員一同辦理。本作業流程中之同意及交付之證明應留下紀錄。

(五)本校利用勞動力發展署之學員資料，僅於勞動力發展署相關之訓練資訊，非本校自行以學校名義蒐集或與勞動力發展署共同蒐集者，不得利用於其他非勞動力發展署訓練課程之訊息派送或行銷。

(六)本校利用勞動力發展署之學員資料於行銷勞動力發展署之其他課程，如當事人邀要求停止利用或停止行銷，應立即停止利用該資料於行銷目的。

(七)學員參訓個人資料、軌跡資料及蒐集相關告知及同意證據，如無其他法令限制，應至少保存五年，以確保相關證據於個資法損害賠償請求權時效內均能完整提出。

五、個人資料銷毀管理

(一)個人資料之銷毀應以無法回復資料原貌為原則，擁有或管理單位銷毀時應留銷毀紀錄並通知本校個資保護專人備查。

(二)送至本校以外銷毀之實體形式資料，須派專人參與運送並全程監督銷毀過程且應留存銷毀紀錄並副知本校個資保護專人備查。

伍、定期回報保護管理狀況

本校承辦勞動力發展署相關作業，依據勞動力發展署之規定，應進行個人資料管理之狀況定期回報

一、應回報項目

本校應回報項目包括

(一)執行小型企業人力提升計畫

回報相關保護管理狀況時間: 本年度七月、及十二月

(二)執行失業者職業訓練

回報相關保護管理狀況時間: 本年度六月、及十二月

(三)回報負責人

本校指定之回報負責人由本校個資專人偕同相關單位依上述狀況進行。

(四)回報方式

依據勞動力發展署規定，本校應於內部稽核作業後，依規定將內部稽核作業結果繳交給勞動力發展署窗口或指定之彙管單位，進行個人資料保護管理之回報作業。

陸、個人資料保護人員管理

一、人員適用範圍

本校於執行勞動力發展署相關專案人員均為本管理規定之管理範圍

(一)本校正職人員

(二)本校約聘雇人員或工讀生

(三)本校之專職或兼職講師、訓練人員

(四)其他與本校合作或接受本校委託而接觸勞動力發展署相關專案或學員資料者

二、人員安全規定

本校適用本規定之人員應遵守

1.簽訂本校保密切結書

2.依據勞動力發展署或彙管單位要求進行保密切結之簽署

3.閱讀並遵守本校「個人資料保護管理規定」

4.遵守本校資訊安全相關規定及作業規範

5.接受本校人員個人資料訓練作業

6.接受本校指派進行個人資料保護相關之工作

三、特殊人員之安全規定

本校人員如因業務需求需要接觸大量個人資料(例如資料庫等)，因其職務涉及風險較大，本校因應相關保護要求得執行

1.人員背景查核(包括前雇主工作狀況之查核)

2.人員安全查核(例如犯罪前科等資料查核)

四、人員安全管理規定

為確保本校之人員安全及人員管理之有效性，本校實施以下措施

1.依據人員業務不同，設定人員之系統存取權限，並管控人員對於資料之接觸情形，及定期審查、確認人員存取資料之權限正確性及必要性。

2.人員應依據其職務，妥善保管與職務相關或被指派保管責任之資產、媒體及資料。

3.人員離職或職務調動時，應辦理保管個人資料、學校資產之交接，本校應於該人員離職或調動後取消或調整該人員系統之存取權限。

柒、資訊安全基本要求

本校之資料安全管理措施要求共分為四大類安全措施，個資保護專人應進行公司內之資料安全管理措施之推行，並視需求回報管理代表執行狀況及資源需求

一、資料安全防護措施

(一)蒐集作業安全防護措施

1.紙本蒐集方式: 以紙本方式進行個人資料之蒐集，應進行以下之防護措施

A.紙本應進行紀錄管制，視紀錄之重要性，透過編號及安全等級標示(密級、內部使用、公開，公開等級可以不標示)，含有個人資料之紀錄應至少標示為內部使用

B.蒐集之紙本應進行紀錄管制，除進行對於該資料歸屬之卷宗進行機密等級標示，並應進行實體存取之防護(例如鎖於櫃子內)

C.須依據個人資料盤點結果中識別之保存年限要求進行保存，確保資料的可再使用性及可讀性

2.媒體蒐集方式: 透過媒體(CD/DVD/TAPE 等)接收個人資料檔案需進行以下防護

A.如媒體數量超過三項，或為經常性(如按月蒐集)蒐集者，應建立清冊進行數量管制

B.媒體應進行紀錄管制並進行機密等級標示

C.媒體應進行實體存取之防護

D.媒體資料輸入資訊系統後，應視其需求進行保存，如不須保存該媒體，應進行媒體報廢作業進行銷毀

3.網站蒐集方式: 透過本校網站進行個人資料之蒐集時，應進行以下防護措施

A.確保輸入之網頁具有 SSL (Secured Socket Layer)等安全措施(或其他對等之安全措施)，確保該蒐集作業簿不會在傳輸過程遭未授權存取、側錄或擷取

B.網頁所產出之資料檔案應注意其安全防護，該資料檔案不應置放外部可存取之目錄

C.網頁程式或網站系統所保存之暫存檔(Server Log, Server Cache 檔)應定期刪除或確認存放於伺服器內未遭未授權之存取，並確認暫存檔中可能留存的個人資料之保護狀態

(二)處理作業安全防護措施

1.處理設備之實體安全

請參考本文件第十一章、設備安全管理

2.處理設備之邏輯安全及網路安全

請參考本文件第十一章、設備安全管理

3.資料儲存設備之安全

請參考本文件第十一章、設備安全管理

4.資料正確性檢查

A.應用系統或網站系統，應於蒐集個人資料後，進行對於資料正確性的檢查，例如查核筆數、設定資料正確檢查碼(Parity Check)等方式進行正確性檢查。

B.重要個人資料之輸入作業，應於輸入作業完成後，進行資料

正確性之複核作業。

C.資料於傳輸或接受後，應進行資料正確性之檢查，確保傳輸 / 接受前後之資料正確性。

5.刪除作業(依據當事人權利要求)

個人資料保護法所規範之刪除，應使個人資料於個人資料檔案中消失，因此，資料的刪除作業應確保

A.該資料於個人資料檔案中消失，包括備份之資料

B.以去識別化進行刪除時，應注意該資料不應於去識別後得以其他方式重新組建其具識別性之欄位

C.刪除作業應確保於暫存檔案、原始紙本、原始資料檔案或媒體之資料也同時被刪除

(三)利用作業安全防護措施

1.資料利用之安全防護控管

資料之利用除須依本文件利用管理程序進行申請外，並應於核准該利用時檢核其利用過程之安全性

2.資料傳輸至其他單位之控管

(1)紙本傳輸

A.如必須應透過人員親自交付

B.透過公文傳遞者，應視情形進行密件標示處理

C.需透過郵遞業者傳遞紙本時，應以掛號方式寄出，並應進行該紙本資料密封作業，必要時得以保密膠帶進行保護。

(2)電子傳輸

A.應避免以未有安全防護之電子傳輸方式進行個人資料之傳輸

B.以電子傳輸個人資料，至少應以 Winzip 等壓縮軟體進行密碼保護，並以分開的傳遞方式遞送該密碼

C.視需求得以加密(Encryption)方式進行資料加密，以確保檔案之機密性

D.傳輸前，應確認接收端之收件人、位置、主機等資訊，確保不在傳輸過程中遭攔截或竊取

E.大量資料電子傳輸或經常性資料電子傳輸應進行申請，由執行小組確認其安全性後始得進行

二、資料存取安全措施

包含個人資料處理之資訊系統或資料庫其存取控制應包括

(一)帳號唯一性原則

1.所有帳號應為唯一性，如非必須，不得多人共用帳號

2.帳號共用應事先經過單位主管及資訊系統負責人之同意，並於適當安全配套(如增加其可歸責性措施)後使得進行

3.嚴禁帳號之借用，以避免破壞帳號使用之可歸責性

(二)帳號核發、變更及刪除方式

1.帳號之核發，應經過申請核准，並記錄其使用人員及使用期間

2.帳號之啟用及通行碼(password)發放，應有安全防護，以避免遭他人未授權使用

3.帳號之變更應經過事先之申請審核，並留存相關紀錄

4.帳號於人員離職或變更職務後應進行刪除之作業，如需保留一定的

期限，應事先經過單位主管及資訊系統主管之核准

(三)帳號通行碼(password)原則

1.處理個人資料之資訊系統其通行碼應至少為 8 碼

2.處理個人資料之資訊系統其通行碼應至少每 180 天更換一次

3.視需求進行通行碼複雜度(Complexity)之要求

(四)軌跡資料保存

1.申請及變更資料

A.所有個人資料蒐集、處理、利用之申請作業與變更作業應留存適當之軌跡資料

B.帳號之申請作業紀錄(電子紀錄及紙本紀錄)應至少保留 5 年

C.使用者(民眾)申請之存取帳號作業紀錄，如無其他法律規定保留期限，應至少保留 5 年

2.存取紀錄

A.個人資料之存取紀錄，應留存其存取紀錄，重要個資檔案或個人資料主檔資料庫之存取紀錄建議保留五年

(五)定期審查存取權限

有關個人資料之資訊系統或資料庫系統存取權限，應至少每半年進行一次存取權限之審查(可併同於個人資料安全稽核作業中進行)

三、資料存放安全措施

(一)紙本資料

1.紙本資料除進行實體存取之安全管控外，大量紙本保存時應注意該紙本事後檢索、取回(retrieve)之可能性及作業方式，以因應當事人

進行刪除之請求

2.紙本之存放應注意防潮及防火，避免意外毀損紙本個資

3.紙本存放之倉庫，應注意其安全性，如與其他物品共置於一室內，應透過監視(Surveillance)防護措施，或其他安全管制制度(例如人員陪同)進行其存取控制防護

(二)電子資料(存放於電腦或伺服器)

1.存放於個人電腦者

(1)電子(檔案、資料庫等)型態之個資存放於個人電腦，應注意該電腦至少應裝設防毒軟體，並嚴禁使用 P2P 等高風險軟體

(2)電子型態之個人資料存放於個人電腦，應確保僅存放最少之需求資料，以避免過多資料存放之風險

(3)稽核人員應於個人資料安全稽核時進行個人電腦之檢核，確保個人電腦未存放非業務需求之個人資料檔案

(4)經常性存放個資於個人電腦者，應事先進行申請，由該部門主管及該資料業管單位進行審核，並確保該電腦有足夠安全防護

(5)必要時個資存放於個人電腦者，應進行資料之加密，以降低資料遭竊取、遺失之風險

2.存放於電腦伺服器者

(1)檔案伺服器等應避嚴禁以未有存取控制之方式進行檔案共享

(2)檔案伺服器之存取權限應視需求開放，並應定期檢視其存取權限之設定

(3)檔案伺服器之管理者權限應控制其必要數量，避免過多的管理者權限可存取非業務相關之資料檔案

(4)存放於檔案伺服器中之檔案，應視需求定期進行檢視，確保其存放之安全防護需求

(5)視需求高重要或大量個人資料存放之檔案應進行加密作業，以避免個資洩漏、遺失之風險

(6)檔案伺服器應留存相關存取紀錄，並由管理人員定期檢視是否有異常之存取行為

(三)資料儲存媒體

1.可移除式媒體

(1)可移除式硬碟機:未經核准不應使用可移除式硬碟機進行個人資料之複製或備份

(2)USB 磁碟: 未經核准不應使用 USB 磁碟進行客戶資料之複製或儲存作業

2.磁帶媒體(Tape, CD, DVD…)

儲存個人資料檔案之媒體應對媒體管制、保護作業進行控管

四、資料備份安全措施

(一)備份作業之規劃

1.訂定備份規定

應訂定備份規定，並依規定進行個人資料檔案之備份作業，包括備份的明細、頻率、方法以及存放媒體形式及存放位置規定等

2.訂定備份計畫或清單

備份管理人員或系統管理人員應依據備份規定進行該資訊系統或檔案之備份作業，並產出備份計畫或清單，透過人工或工具進行備份並留存紀錄

3.評估及訂定備份的安全防護需求

對於備份後的備份檔案應視其存放之媒體種類、存放之位置、系統、既有之安全防護評估並擬定備份檔案之安全防護需求，並依據該需求進行防護措施的實施，並將結果紀錄於備份計畫或清單表格內

4.評估及訂定備份的測試需求

針對備份計畫或清單內之備份結果，應評估該備份資料之重要性及其還原需求之頻率、可能性進行評估後產出備份測試之需求

(二)備份作業執行及記錄

於備份計畫或清冊內記錄

1.記錄備份之執行狀況

2.記錄備份之儲存位置及保護措施

3.記錄備份之目的、使用方式

(三)備份作業之監督及測試作業

1.定期審查備份作業之正確性

2.定期執行備份資料之盤點作業

盤點備份資料須注意備份檔案可能存放在以下媒體：

(1)TAPE

(2)CD

(3)DVD

(4)存放於媒體或虛擬主機(Virtualized Server) 上(Ghost、Image 檔案)

(5)伺服器、儲存設備內之檔案

A.檔案伺服器內

B.NAS / SAN 或其他網路儲存設備內

C.遠端主機、遠端儲存設備、網路儲存設備等

D.可移除式媒體上

a.可移除式硬碟

b.USB 儲存設備

E.資料庫主機之 Mirror (鏡像)主機、備份資料庫主機等

3.備份媒體之測試

(1)依據測試需求擬定測試計畫

(2)於測試執行後將測試結果記錄於備份計畫或清冊內

捌、個人資料之風險評估及管理機制

一、個人資料盤點作業

(一)受委託蒐集及自行蒐集之個人資料

本校於進行個人資料盤點作業前，應區分本校之資料係為勞動力發展署所委託之作業蒐集，或是因本校自有作業之需求而蒐集，由於受勞動力發展署委託之業務，係公務機關執行法定職務所蒐集，因此該等資料之風險評估應以公務機關法律規定評定之。

本規定之個人資料盤點作業應以受勞動力發展署委託所蒐集之資料為主，包括勞動力發展署僅補助部分金額之專案資料、或本校與勞動力發展署共同蒐集之資料均適用

(二)個人資料分類分級

本校之個人資料依照其屬性、種類、數量、格式及保存方式進行分級

1. 屬性

(1)特種個資: 個資法第 6 條(目前暫緩實施)所規範之個資包括: 病歷[1]、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。此類個資為特種個資，本校僅於以下狀況始得蒐集，且蒐集時必須依據個資法規定實施適當安全維護措施：

A.法律明文規定

B.公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施

[1] 病歷雖於 99 年 5 月 26 日所公布之版本未納入個資法第 6 條，但已於個資法修訂草案中將該項目列入特種個資。

C.當事人自行公開或其他已合法公開之個人資料

D.公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料

E.前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之

(2)一般個人資料: 依據個資法第 2 條所規定，個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

2.種類

依據本校之個人資料特性，將本校之個人資料種類區分為：

(1)學員個資: 因本校接受勞動力發展署委託訓練業務蒐集、處理、利用之學員個人資料，包括特種或一般個資

(2)廠商個資: 與勞動力發展署委託訓練業務有關之廠商因與本校有業務(採購、承包....)往來或承接本校委外業務而交付之廠商(廠商包括其他公務單位)員工或個人之聯絡資訊，此類個資可能為本校直接向當事人蒐集或廠商間接交付之各類資料，包括個人聯絡資訊、個人財務資訊等等(範疇不包含法人之資訊)

(3)員工個資: 包括本校人事單位依法蒐集之正職人員、約聘僱人員、工讀生或正職、兼職等之講師個人資料

(4)其他個資: 無法歸類於前三種個人資料之種類。

3.筆數

依據本校之作業特性將個人資料之數量進行分級：

(1)大量個資: 個資數量介於 1 萬- 10 萬筆

(2)小量個資: 個資數量介於 1,000 筆-1 萬筆

(3)微量個資: 個資數量小於 1,000 筆

4.格式

本校之個人資料可歸類為以下格式，但注意部分個人資料於處理過程中包含多種個資格式：

(1)書面/紙本格式: 包括一般書表、單據、手寫稿...等

(2)電子文件格式: 包括網頁、及 e-mail、電子公文等被視為電子文書之書面。

(3)檔案格式: 包括各種電子檔格式、備份檔案或暫存檔、郵件附件等，與電子書面格式之不同為此類檔案主要利用方式為檔案，通常用於傳遞或保存。

(4)資料庫格式: 存放於資料庫主機內之資料。(資料庫之備份檔案屬於檔案格式)

5.保存方式

依據個人資料的存放及保存方式，本公司個人資料之保存可分為：

保存方式	書面/紙本	電子文件	檔案	資料庫
高安全保存	編號、上鎖	高強度存取管制	加密保護、存取控制	高強度存取控制，限制連結
中安全保存	編號管理、集中存放	普通存取管制	加上通行碼保護，存取控制	強度存取控制、未限制連結
低安全保存	未有管理或上鎖	無存取管制	無保護、存取控制	共用帳號、一般系統均可連結

二、風險評估作業

本校個人資料之風險評估作業步驟：

(一)由各部門個資管理專人盤點後進行風險評估作業。

(二)風險評估作業，依據本章第一點之分類方式進行對於個人資料檔案之風險評估作業。(風險評估之作業表單如附件六、個人資料盤點暨風險管理計畫表)

1.衝擊性評估表：

衝擊性	評估標準
低	微量個人資料(<1000)且不含高風險個人資料內容 僅姓名及聯絡方式(電話、email、地址) 從合法公開資訊取得
中	小量個人資料(1000~1 萬筆)且不含高風險個人資料資訊
高	大量個人資料(1 萬筆以上)或含完整個人資料或高風險個人資料資訊

2.高風險個人資料資訊：

(1) 病歷、醫療、基因、健康檢查、性生活及犯罪前科等資訊(個人資料保護法第 6 條) 。

(2) 含身份證字號或護照號碼、銀行帳號、財務資訊(法人帳號資訊非為個人資料) 。

(3) 完整個人資料(profile)：例如完整人事資料、完整之監理申請資料。

3.風險分級表

衝擊性 / 保存方式	低	中	高
高安全保存	低風險	低風險	低風險
中安全保存	低風險	中風險	高風險
低安全保存	低風險	高風險	高風險

(三)風險評估作業評估結果為：

(1)高風險者，應提出風險處理計畫/辦法進行改善作業。

(2)中度風險者，應評估是否有可改善的方式提出改善建議，若無改善方法應持續關注其安全性。

(3)低風險者，可以免為進行改善或風險處理計畫。

三、風險管理作業

由前段風險評估作業所評定之個人資料風險，應包括以下作業：

(一)風險評估作業執行：

1.執行負責：由個資專人負責彙整本校資訊資產進行盤點及風險評估作業

2.風險處理計畫：由個資專人進行相關風險評估及風險處理計畫之彙整。

3.風險處理計畫核定及風險接受：由管理代表進行計畫之審查及剩餘風險之接受。

(二)風險改善及處理

1.風險評估作業評估結果為高風險者，應提出風險處理計畫/辦法，並由單位主管進行核准該風險處理計畫能將該資產之風險有效控制至低或中度風險。

2.風險評估結果為中度風險者，應視可改善的方式提出改善建議。由個資專人進行評估其可行性。

3.低風險者，可以免為進行改善或風險處理計畫。

4.各單位之風險評估結果應交由個資專人進行本公司之風險評估彙整，並由管理代表進行本校之風險處理計畫之核定，確保所有個資風險均有改善措施或處理計畫。

(三)風險可接受等級：本校之風險可接受等級為中等風險。

(四)風險處理計畫，其中應包括風險處理計畫說明，執行人員，預計完成日期及所需資源，處理後的風險預估值，所有高風險值應控制至低或中風險。

(五)風險改善管控作業，應由管理代表核准相關計畫後，由個資專人進行後續控管作業，確保所有改善及風險處理計畫均已依原計畫有效完成控制個人資料之風險。

(六)整體風險評估結果與風險處理計畫應於風險評估作業完成後，由個資專人向管理代表進行報告。

(七)風險管理表單：如附件六、個人資料盤點暨風險管理計畫表。

玖、事故之預防、通報及應變機制

本校承接勞動力發展署之訓練作業，應進行各項事故預防作業及降低事故衝擊之措施。如本校於資安或個資事故發生時，將先行判定該事故相關之個資是否為與勞動力發展署所委託相關之專案學員個資。

一、事故預防

本校為避免事故之發生，訂定本程序書，並依據程序執行以下管控措施以預防個人資料事故：

(一)個人資料管理組織與政策

(二)個人資料蒐集、處理、利用管理，包括招生、報名、資料處理及資料利用管理

(三)定期回報保護管理狀況

(四)資訊安全基本要求

(五)個人資料風險評估及風險管理

(六)事故預防、通報及應變機制

(七)認知宣導及教育訓練

(八)設備安全

(九)資料安全自評及內稽管理

(十)抱怨及當事人權利行使管理

本校內部稽核人員，應針對本校「個人資料管理規定」進行每年兩次之內部稽核作業，並產出內部稽核報告，確保本校均依據該規定及勞動力發展署之規定做到個資事故之預防作業。

二、個人資料事故處理流程

(一)疑似期：與此階段查證引起個人資料事件之原因並做成相關報告。

1.本校各業務單位應由個資專人查證引起個人資料事故之原因並做成相關報告，呈報管理代表。

2.疑似期之調查結果，應由個資專人於查證結果確認後，以適當方式通知當事人或通報事故之單位。

3.相關個人資料事故之通報及查證後之通知應留下相關紀錄以供事後查證作業。

4.除可確認該疑似事故非為本校導致，應於適當的時間點，由個資專人或事故分組通知勞動力發展署聯絡人。

(二)個人資料事故處理期

如確認事故發生原因為本校之責任，應儘速處理個人資料事故

1.由本校個資專人或事故處理分組進行對勞動力發展署聯絡人之通知，並留下正式紀錄，包括勞動力發展署對本校之後續事故處理指示。

2.本校個資專人分析案由並提出相關處理方式，提交管理代表進行處理方式之決議，並留下相關決議紀錄。

3.由本校個資專人蒐集相關證據並與本校內部或外部法律專業人員或本校委外律師討論可能之法律責任。

4.由事故處理分組及發生事故單位個資就事故之範圍擬定事故通知之當事人及相關單位之方式及內容。

5.如事故涉及跨一個單位以上時，應由個資專人為單一聯絡窗口，整合各單位之事故處理結果及通知當事人。

6.由本校個資專人邀集本校相關單位及本校委外律師(如適用)與當事

人召開事故協調會避免事件擴大。

(三)事故擴大期

如該事故已無法於事故處理期中進行處理，事故已導向範圍擴大或延伸至法律訴訟階段為事故擴大期，本期之控管重點應為控制事故之擴大及其衝擊。

1.由本校個人資專人及委外律師(如適用)組成事故說明小組向外說明，其對外發言部分得由管理代表指定，並應同時要求本校相關同仁不得自行針對此事故進行發言。

2.由本校事故管理分組及委外律師共同擬定訴訟策略。

(四)司法訴訟

1.由本校個資專人及委外律師(如適用)共同擬定訴訟策略。

2.本校個資專人及委外律師(如適用)就訴訟策略進行訴訟。

3.本校事故管理分組及委外律師尋求事故和解之可能性。

三、個人資料事故通報管理

本校於發生事故後應依本規定進行個人資料事故通報：

(一)內部通報流程

本校所有人員發現疑似資安或個資事故現象，應立即通報個資專人或事故處理分組人員。

(二)外部通報流程

學員或客戶如果透過本校抱怨管道向事故處理分組通報相關疑似個資事故，於判定為疑似事故時應立即通知個資專人。

(三)事故後通報勞動力發展署

本校個資專人，應於本校違反個資法、相關法令、勞動力發展署規定及本校管理規定或發生個資事故之時、事故處理及事故處理完成後，以適當方式進行對勞動力發展署之書面通報，包括：

1.發生事故之緣由

2.後續之處理狀況

3.補救措施及其執行狀況

4.可能對勞動力發展署之影響

(四)事故之紀錄與處理

事故處理小組接收到相關通報，應記錄事故通報內容，並依本章之事故處理程序進行處理。

四、個人資料之事故懲處管理

1.個資專人查明相關人員疏失之責任歸屬後(如疏失人員為個資專人時，由管理代表進行調查人員之指派)，視情節之輕重為適當之處置

2.事故懲處後應以適當方式通知勞動力發展署或彙管單位。

壹拾、認知宣導及教育訓練

一、訓練需求評估

(一)執行人員

本校之個人資料安全教育訓練由教育訓練分組執行管控。

(二)執行時間

個資專人最遲應於每年十二月產出次年之教育訓練計畫，並由管理代表審核後，由教育訓練分組執行。產出格式如附件七、全年教育訓練計畫書

(三)評估內容

評估內容依參考:

1.法規變化

2.勞動力發展署管理機關提出之教育訓練需求

3.人員個資保護知識需求

4.年度個人資料事故發生原因等

5.配合資安教育訓練

二、訓練計畫

教育訓練分組於每年十二月產出次年之教育訓練計畫，並由管理代表審核後，由教育訓練分組執行。

年度之訓練計畫應至少包括:

(一)針對全體人員之個資法認知訓練至少三小時

1.個人資料案例說明，說明目前市場相關的案例或個資法相關判決案例，以強化人員對於個資法之遵循知識

2.個資相關法律、法規之更新畫變化說明，以及影響本校之營運作業方式。

(二)個資專人及內部稽核人員訓練至少各 3 小時，個資專人及內部稽核人員應進行年度之專業訓練，包括

1.個人資料法律訓練

2.個資專人管理訓練

3.稽核人員專業訓練

三、訓練執行

由教育訓練分組委由本校內部人員或聘請外部講師或參加外部課程進行訓練。

四、訓練結果維持

訓練之結果或訓練成效之評估應予以留存，並於每年個人資料保護管理審查會議中提出成效報告。記錄表單如附件十、個別部門教育訓練計畫、執行紀錄

五、成效評估與計畫修正

於每年之成效報告後，應提出隔年之教育訓練計畫之修正，如有重大差異或成效缺失，應提出矯正預防計畫，確保教育訓練之成效管理。

壹拾壹、設備安全管理

個資法要求對於個人資料處理設備進行安全的管控，本校對於設備安全管理之程序分為

一、個資處理設備清查

進行對於本校內部個資處理設備之清查作業，透過清查進行對於設備的識別，確保所有與個人資料蒐集、處理、利用作業相關之設備均於此過程中被清查出，以便後續進一步的評估設備所需要的安全要求。

(一)個人資料輸入處理設備

1.辦公輸入設備: 掃描器、傳真機、影印機等用來處理紙本資料個資蒐集設備。

2.個人資料輸入管道:包括網站設備、IVR 互動語音回應系統、CTI 電腦語音整合系統及電話等可能用來接收或處理蒐集個人資料之設備。

(二)個人資料處理設備

1.個人電腦設備: 包括人員使用之個人電腦設備、筆記型電腦、手持式電腦設備等資料處理設備

2.檔案伺服器: 儲存檔案的公共檔案主機，包括各類、各種技術刑事的檔案集中儲存設備均屬。

3.資料庫主機設備: 主要以資料庫形式(包括各種不同資料庫，例如 SQL Server, My SQL, Access Databse, LDAP …)存放個人資料的設備均屬。

4.通訊設備: 例如傳真機，答錄機，影印機等通訊設備，因目前科技進步，該等設備內均有設置儲存裝置(例如硬碟機)，以加速或增加該設備的功能，因而可能因為民眾傳真進本校或本校人員影印相關含個

人資料之紙本而在該等設備中留存部分個人資料(此類設備維護廠商通常可以檢視或存取該儲存裝置)。

5.其他資料處裡設備: 例如各式側錄主機(例如 email 側錄設備，網訊息路側錄設備、電話語音側錄設備)，各類 Log 紀錄蒐集及分析設備。

6.資料儲存設備

(1)備份空間、伺服器(包括異機備份、SAN 或 NAS 網路儲存設備)。

(2)備份媒體、盤帶、光碟(CD, DVD)等之儲存設備。

二、設備安全需求評估

對於處理個人資料設備於清查後應進行對於該等設備安全需求的評估作業，包括以下之評估:

(一)設備實體安全防護

評估設備是否需要適當的實體安全控管，例如:

(1)是否需要實體存取預防措施: 例如上鎖、加上密碼控管、專人看管、或其他實體保護。

(2)如設備數量較多，應評估是否進行數量的盤點及控管，確保該等設備無遭竊之可能。

(二)設備邏輯及網路安全防護措施需求

如果設備可以接上網路、通訊網路等邏輯(非實體)通路時，應注意對於此類網路安全的需求評估:

1.設備之網路安全措施

2.評估設備是否需要適當的網路安全措施,例如進行適度的網路區隔，進行相關的 NAT (Network Address Translation) 以確保 IP 位置不

被外部人員所知悉，安裝防火牆設備或設定連線端條件(固定 IP、 回撥、特殊路由等)。

3.資料傳輸安全防護措施

評估此類設備在傳輸資料時，是否需要進行額外的資料保護，例如傳輸加密、安全通道、VPN 等強化傳輸安全之防護措施。

(三)資料安全防護措施

如果設備具備存放或短暫存放資料的能力，應評估此類設備是否需要進行資料安全的防護包括:

(1)資料機密性的保護需求: 評估資料是否需要進行機密性的保護，例如加密機制、設置存取控制、通行碼管制、進行資料遮罩等。

評估該等設備是否需要在送修、維修前應移除資料或以其他方式控制不被維護廠商未授權存取。

(2)評估該設備是否需要進行資料完整性的保護，例如避免震動、電流不穩、資料傳輸後複核等保護。

(3)資料可用性的保護需求: 該等設備是否需要進行備分，不斷電保護及其他確保資料可用性之防護需求。

(四)設備存取權限之管制需求

(五)如果設備可以讓多人進行存取，應評估如何進行存取權限的控管保護，包括評估：

(1)帳號申請作業需求，應具備帳號申請作業，確保開放該設備存取之過程經過相關人員核准。

(2)帳號存取權限安全措施: 例如帳號長度控管，通行碼更換頻率，通行碼複雜度及通行碼的交付安全保護。

(3)帳號審查作業需求: 評估是否進行定期的帳號權限審查，以確保該設備之存取權限開放均為正確。

(4)其他防止未授權存取的安全保護需求: 例如進行 OTP (One Time Password), 雙因認證等強化存取控制的作法，螢幕保護控制、Session Time Out 等對於存取控管的安全防護。

三、設備安全防護措施執行與監督

於設備之安全防護措施需求評估完成後，應於清查的表單中產出對應的安全防護需求統計，並依該需求進執行計畫，各單位專人應該進行對於該執行計畫的推行及監督，確保所有評估出之需求均於計畫的時程、需求資源的條件下被完成，如因故不能依原規劃進行防護措施，也應將結果及後續補強或改善方式向個資專人報告後結案。

(一)擬定執行計畫: 個資專人偕同本校資訊人員、總務人員等擬定防護措施執行計畫，並呈報管理代表核准後實施。

(二)設備安全防護之執行: 由個資專人協同資訊人員、總務單位等進行對於設備安全防護措施之檢查，未達需求者應提出執行計畫進行改善，於單位完成防護措施執行後，應記錄結果並呈報管理代表。

(三)稽核人員於每年進行內部稽核時進行對於設備安全維護作業之檢查，不符合需求者應提出稽核發現，並追蹤至改善完畢。

壹拾貳、資料安全自評及稽核機制

一、稽核人員

本校之個人資料安全稽核由管理代表指派之稽核人員進行。

二、稽核管理

(一)依據勞動力發展署之規定，本校每年至少應執行兩次稽核，本校於每年五月及十一月進行內部稽核作業。

(二)本校之個人資料保護管理內部稽核工作之執行者不限於本校個資保護執行稽核人員之人員，可以委由外部具備專業資格之人士進行，但不論由內部或外部人士執行,稽核人員必須具備獨立性及客觀性，內部稽核人員不能稽核本身之工作。

(三)稽核工作必須對稽核過程所查核事項的事實加以記錄，以顯示其稽核軌跡作為稽核發現之佐證。

(四)稽核所發現之缺失及觀察事項與建議，應由稽核人員及被稽核單位就是否屬實取得一致之見解，被稽核單位應對稽核所見加以檢討並尋求改善，稽核結果及改善行動執行情況應交付本校個資專人。

三、稽核準則

(一)個人資料保護法

(二)個人資料保護法施行細則。

(三)勞動力發展署對個資保護管理相關作業規定。

(四)本校個人資料保護管理規定及各單位作業內容。

四、稽核計劃

1.稽核人員於每年規定之稽核作業時程前一個月前產出該次稽核計畫，並告知內部、外部(如適用)受稽核單位指派稽核人員及規畫預定執行

時間。

2.稽核計畫之制定須考慮過去稽核之結果決定稽核範圍及查核重點。

3.計畫內容必須涵蓋指派之稽核人員，稽核範圍及查核重點，人員工作分派及時間分配，人員獨立性審查結果，稽核計畫經個資專人或管理代表審議通過，並通知受稽核單位或流程。

五、稽核範圍

(一)須包含本管理規定之各項需求程序之執行結果

(二)個人資料保護告知事項及同意內容 (個資法第 8 條及第 9 條要求)

(三)個人資料盤點作業

(四)盤點結果中個人資料範圍界定作業(施行細則第 8 條第 2 項第 2 款規定)

(五)個資法規盤點作業

(六)風險評估與風險管理作業(施行細則第 8 條第 2 項第 3 款規定)

(七)個人資料事故之預防、通報及應變作業。(施行細則第 8 條第 2 項第 4 款規定)

(八)個人資料蒐集、處理、利用行為之檢查(施行細則第 8 條第 2 項第 5 款要求)

(九)資料安全維護作業檢查(施行細則第 8 條第 2 項第 6 款規定)

(十)認知宣導及教育訓練作業檢查(施行細則第 8 條第 2 項第 7 款規定)

(十一)設備安全維護 (施行細則第 8 條第 2 項第 8 款規定)

(十二)個人資料保護持續改善作業(施行細則第 8 條第 2 項第 11 款規

定)

(十三)使用紀錄、軌跡資料及證據保存作業檢查(施行細則第 8 條第 2 項第 10 款規定)

(十四)當事人行使權利所執行之各項檢查。(個資法第 3 條及第 10、11、13 條要求)

六、稽核頻率

(一)本校個人資料保護管理每年(或於該年度委託執行期間)至少執行一次內部稽核，對於特殊事項之稽核，本校管理代表得指派人員進行特別追蹤稽核。

七、稽核方法

(一)稽核採抽樣方式進行，一般單一查核項目之抽樣不得少於 5 件，對於特別查核項目之抽樣數可由稽核人員指定。

八、稽核紀錄與報告

(一)個人資料稽核工作底稿如附件九、稽核查檢表

(二)稽核工作必須保留工作底稿，工作底稿形式由稽核人員指定，工作底稿可為電子檔或書面手寫但須清楚顯示每一查核項目之查核準則、訪談對象、所檢視紀錄及所進行之抽樣及該項查核之結果。

(三)對於不符合事項必須填具矯正預防單如附件十一、矯正預防單，進行改善。

(四)稽核人員須於稽核結束兩週內提交稽核報告，報告須包括各項建議、觀察事項及不符合事項之匯整及統計、對於整體個人資料保護管理之有效性及適切性之評估以及就稽核過程之有效性之自我檢討與評估。

(五)稽核報告應送交本校個資專人及管理代表。

九、改善行動與跟催

(一)對於不符合事項，受稽核單位必須於一週內提出原因分析及改善行動，並通知稽核人員或稽核組長，經該稽核人員認定為有效之措施方可實施，對於改善行動之追蹤可由開立稽核報告書之稽核人員進行確認。稽核報告書之格式如附件十、稽核報告書

(二)改善的記錄與跟催應由個資專人監督並簽核本校管理代表，並由管理代表確認改善。

壹拾參、個資安全維護之整體持續改善

一、程序目的

本校個人資料保護須依循管理系統所揭櫫之 PDCA 循環,除本校於計畫階段進行訂定個資政策及本個資保護管理規定及要求人員遵循政策及本規定外，本程序將建立持續改善之方式以確保本校對於個資管理的有效性。

二、檢查

本校透過稽核機制及通報機制進行相關個資遵循的檢查作業包括

(一)例行性的個人資料保護稽核作業。

(二)設置個資專人，針對個人資料保護進行例行性的檢查作業

(三)管理審查會議:

透過管理審查作業，由管理代表每年進行至少召開一次對於個人資料保護作業整體成效審查，參加成員包括個資專人及各單位主管確保所有之管理制度及結果均符合本校之需求。審查項目得包括

(1)風險管理結果

A.個人資料風險評估結果

B.風險管理結果報告

(2)內部稽核結果

提供內部稽核報告。

(3)事故處理分組

該年度的個人資料相關事故統計及處理情形。

(4)矯正預防措施

(5)個資專人

針對本校個人資料保護管理作業情形進行報告。

三、持續改善

(一)於各項檢查後之發現結果，該資料保護管理個資管理專人應該針對該發現點提出矯治預防包括

1.發現原因，事件發生或異常發生的原因。

2.矯正計畫: 針對原因提出解決方案。

3.預防計畫: 針對原因提出預防事件再次發生之解決方案。

4.計畫預計完成日期: 矯正、預防措施所需之完成時間預估。

5.計畫執行人員: 指派之矯正預防措施執行人員。

6.需求資源: 完成計畫所需之資源，包括人員、預算或相關資訊資源之需求。

(二)矯正預防計畫之審查

各單位提出之矯正預防措施，應由個資專人監督並簽核至管理代表後進行核准後監控執行到完成，後將相關執行結果送交管理代表簽核後結案存查。矯正預防單之格式如附件十一、矯正預防單

壹拾肆、抱怨、申述及當事人權利行使管理程序

一、抱怨處理作業

(一)抱怨處理

1.接受抱怨

當事人對於本校個人資料的處理方式有疑慮時，本校應提供正式管道接受民眾之抱怨。學校人員接獲學員或民眾提出對本校個人資料蒐集、處理、利用之疑慮時，應以正式管道接受當事人之抱怨或說明。

2.抱怨之受理及處理方式

本校對於個人資料抱怨作業，應以附件十二、個人資料抱怨處理單進行作業之處理，該單據可由學員或投訴人進行填寫，也可由受理單位之人員代為填寫，填寫後交由個資專人進行審查，並事情行由受理單位對提出報員人員回覆，或由個資專人事情行決定由個資專人或管理代表進行回覆。

回覆之方式儘可能以書面或電子文件方式留下回覆內容及回覆方式，並留下事後可追查之紀錄。

3.情節嚴重抱怨或疑似之個人資料事故處理

如該抱怨為疑似之個人資料事故(例如洩漏、違法利用等情形)，應通報個資專人或事故處理分組進行個資事故之處理作業。

如抱怨的人數眾多，例如對於本校蒐集之資料或處理方式有多人不滿、有意見或疑慮時，應以正式方式接受該抱怨，並於彙整後通知個資專人，並由個資專人通知本校之管理代表。

如個資專人為抱怨投訴之對象，應由管理代表要求稽核人員進行該事件之調查。

4.通報勞動力發展署

如抱怨之情節嚴重，或疑似個人資料事故，應由個資專人判定是否需要通知勞動力發展署或其指定之彙管單位。疑似個人資料事故，應以個人資料事故之處理方式進行。

二、當事人權利請求作業流程說明

1.抱怨受理及作業流程說明

(1)受理當事人權利申請可能管道

A.當事人於本校訓練場所向本校人員提出

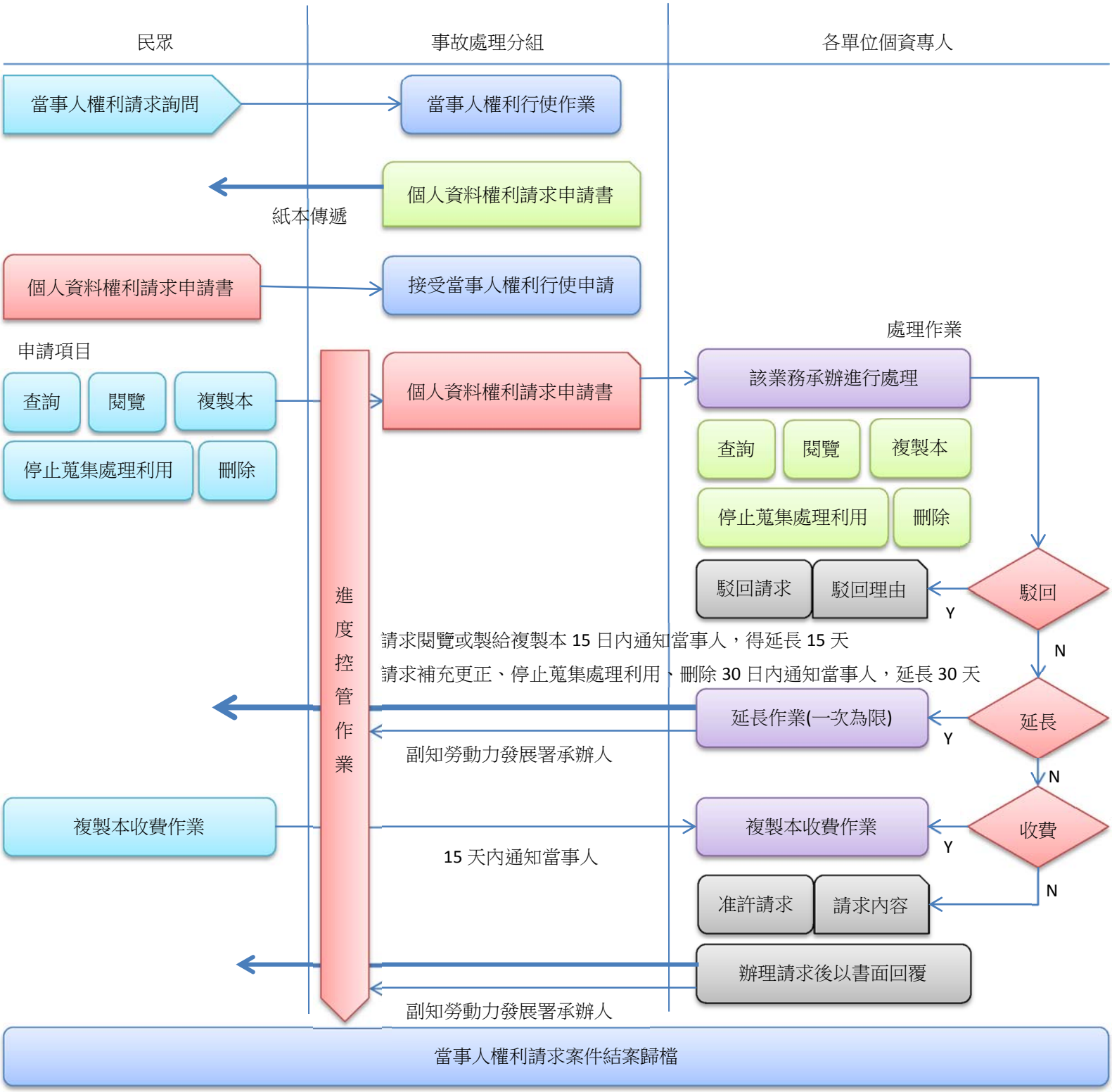
B.當事人透過書面投書至本單位或學校郵遞信箱

C.當事人透過 e-mail 至本校電子郵件信箱

D.當事人透過勞動力發展署或其他單位進行申訴(如透過或其他公務機構函轉)

(二)當事人本校個資作業當事人權利請求作業流程

當事人權利請求作業流程



1.當事人權利:

依個資法第 3 條之規定，當事人就以下事項，可向本校行使其權利:

(1)查詢或請求閱覽

(2)請求製給複製本

(3)請求補充或更正

(4)請求停止蒐集、處理或利用

(5)請求刪除

2.個人資料當事人請求行使查詢或請求閱覽時,若有下列情形之一者，本校可拒絕當事人行使權利之申請：

(1)妨害公務執行之虞者

(2)妨害第三人之重大利益

(3)妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益

(4)妨害公務機關執行法定職務

(5)妨害本校或第三人之重大利益

3.當事人權利行使處理方式

要求當事人進行表格填寫，表單如附件二、個人資料權利請求申請書

(1)當事人如於現場，應請當事人填寫表單，如非於現場提出請當事人

A.上網下載抱怨表單

B.以郵寄方式傳遞抱怨表單

C.承辦人員代為填寫內部作業表單，代為申請

(2)當事人權利行使時應檢具之文件

對本校行使當事人權利時應檢具下列文件:

A.當事人本人提出申請者

B.當事人權利行使申請書

C.當事人須出示其身分證、健保卡、護照、駕照、學生證、居留證或其他足資證明身分之證件以供查驗。

D.受託之法定代理人提出申請

受託人須出示其身分證、健保卡、護照、駕照、學生證、居留證或其他足資證明身分之證件以供查驗。

E.當事人權利行使申請書以及授權書，授權書必須經當事人親筆簽名。

F.當事人查詢資料應檢具真實文件並據實填寫相關資料，如有虛偽不實者，本校得拒絕其查詢。

(3)受理作業

本校人員於完成前述表單填寫後，應向當事人說明辦理所需之時間及個資法律之規定，並將該表單轉予個資專人進行後續處理作業

(4)查明是否為勞動力發展署之公務資料

個資專人於接收申請後，應查明是否該資料為勞動力發展署所管轄之資料，如為如該資料為勞動力發展署所管轄之資料，應由承辦人詢問勞動力發展署承辦人員後，依據勞動力發展署指示方式進行後續作業辦理，本校個資專人應留存相關聯

繫及指示之證據。

如該資料為勞動力發展署所管轄或本校無權進行之資料管理作業，應回覆當事人，並協助當事人將該申請案件轉交勞動力發展署承辦人員。

(5)查明承辦單位

如該資料係由本校所蒐集及處理利用之範圍，且本校依法有對該資料之完整處理權利或授權，應依據以下步驟辦理後續作業:

A.由個資專人判斷該申請案件之主要個資蒐集或利用單位，由該單位進行後續處理後，將處理結果回覆給個資專人。

B.如為全校均使用之資料，一律由個資專人進行後續程序之辦理，並由個資專人進行後續通知回覆當事人之事項。

C.如遇爭議或無法核決是否辦理知情行，應由個資專人進行分析並取得管理代表之核准後辦理，必要時得諮詢外部法律顧問資源或諮詢勞動力發展署之承辦人員後辦理。

(6)當事人行使個資法第 3 條之權利時，應由當事人本人填寫申請書及出示身份證明文件向本校提出申請，若委託法定代理人代為申請時，除檢具申請書外，尚須提出委託之授權書。

4. 處理期間

(1)本校受理當事人行使查詢、閱覽、製給複製本之申請後，應於十五日內處理；必要時得延長十五日，並應將其原因以書面通知客戶。如駁回當事人之申請時並附駁回之原因。

(2)本校受理當事人行使更正補充、刪除、停止處理利用申請後，應於受理日起三十日內回覆結果，必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。如駁回當事人

之申請時並附駁回之原因。

附件一、個人資料保護小組名單

組別	代表/小組長	成員	備註
管理代表	推廣教育中心中心主任	何崑榮	
個資專員	助理	張億萱	
稽核人員	推廣教育中心中心主任	何崑榮	
教育訓練分組	助理	張億萱	
事故管理分組	助理	張億萱	

附件二、個人資料權利請求申請書

<table>
<tr><td colspan="3">雲嘉南分署 個人資料權利請求申請書</td></tr>
<tr><td rowspan="4">申請人</td><td>姓名</td><td></td></tr>
<tr><td>身分證統一號碼</td><td></td></tr>
<tr><td>設籍或通訊住址</td><td></td></tr>
<tr><td>聯絡電話</td><td></td></tr>
<tr><td rowspan="2">法定代理人（或代表人）</td><td>姓名</td><td rowspan="2"></td></tr>
<tr><td>通訊處所</td></tr>
<tr><td>個人資料權利請求說明</td><td colspan="2"></td></tr>
<tr><td>申請件數</td><td colspan="2"></td></tr>
<tr><td>申請用途</td><td colspan="2"></td></tr>
<tr><td colspan="3">（組織名稱）</td></tr>
<tr><td colspan="3">中華民國　　年　　月　　日</td></tr>
</table>

附件三、資通安全適用法規一覽表

編號	領域	法規名稱	頒布機關	版本	確認	備註
1	個人資料	個人資料保護法	法務部	99 年 5 月 26 日	何崑榮	
2	個人資料	個資法施行細則	法務部	101 年 9 月 26 日	何崑榮	

附件四、新個資蒐集前查檢表(範本)

申請日期 2012 年 1 月 1 日

大同技術學院 新資料蒐集前檢核申請表	
蒐集目的	辦理參訪及研習
蒐集類別	(格式　項目: 法定類別編號) C001　C003　C023　C088
特定目的	1. 001 2. 053 3. 039 特定目的與本公司業務相關性說明：　本公司代辦住宿、平安保險
符合法定職務說明	
法源依據及法律要求說明(例如: 最小保存時間)	(請注意確認為法律規定，行政命令)，如有公文請列為附件 法律名稱:　　條文: 公文名稱:
蒐集格式	紙本 電子檔(活動報名系統轉出資料)
個資保存時間	活動報名及舉行期間
個資保存方式	紙本 電子檔(活動報名系統轉出資料)
預計利用方式(期間、地區、方式)	1. 100/7/10~100/7/15 2. 國內 3. 辦理保險、訂房、核發研習證明
資料蒐集方式	☐直接蒐集
如為間接蒐集	間接蒐集資料來源:_____

	來源分類:☐和法公開資料庫☐公開可取得來源☐其他 _____ 間接蒐集資料來源合法性檢查:_____		
第十五條蒐集處理合法要件	☑合於法定職務 ☐採用書面同意，書面說明:_____ _____, 該書面預計保存方式:_____ _____		
其他項目項目檢查	內容	是否符合	
會簽意見			
個資專人			
單位二:			
核准			
申請人		**單位主管核准**	
個資專人			
管理代表			

附件五、個人資料利用前申請書

申請日期　　年　月　日

大同技術學院個資利用申請書	
將利用之個資說明 (說明利用的標的及簡述利用之狀況)	
現有個資蒐集、處理狀況說明	
利用之資料說明: ☐ 直接蒐集資料 ☐ 間接蒐集資料: 取得來源說明 _____ 告知義務: ☐ 已依法告知　依法免告知_____ 目前資料保存方式、存放地點:_____ _____ 目前資料管理單位及管理人員:_ ☐ 同申請單位 ☐_____已以法告知者請簡述已告知之內容於下方欄位	
原蒐集取得同意之方式	☐ 法定職務: ☐ 書面同意 _____ ☐ 其他方式_____
個人資料檔案說明	
已公開之個人資料檔案名稱	
保有之依據	
範圍	

預計利用方式說明			
利用之方式說明（方式、對象、地區、期間）交付方法、安全措施	方式: 期間: 地區: 對象:		
與原蒐集目的檢查	是否與原告知之利用方式、對象、期間、地區相符或與原蒐集之法定職務範圍目的相符 ☐是 ☐否 ☐保留意見_____		
是否合於本組織法定職務(如超出法定職務,依據個資法第 16 條，不應利用)			
是否合於原蒐集之特定目的			
利用方式(傳遞方式)是否合乎適當安全維護之說明			
會簽意見			
單位一:			☑是☐否☐不適用
單位二:			☑是☐否☐不適用
核准			
申請人:		**單位主管**	
管理代表			

附件六、個人資料盤點暨風險管理計畫表(另提供 EXCEL 檔)

項目 編號	Part 1 個資盤點										Part 2 風險評估及處理					
	個人資料檔案名稱	個人資料欄位	個人資料類別	保有單位	屬性	種類	筆數	保存期限	格式	保存方式	衝擊	風險分級	處理/強化方式	預計完成日期	負責人員	核准
1	業務外包廠商派駐人員名冊	姓名、身分證號碼、性別、職業、學歷、證照	C001識別個人者、C003政府資料中之辨識者、C011個人描述、C038職業、C052資格或技術	養護課	一般個資	廠商資料	微量	10年	紙本	高	低	低				
3	勞安課辦理教育訓練資料	姓名、身分證號碼、性別、婚姻、職業、學歷、證照、職稱	C001辨識個人者、C003政府資料中之辨識者、C011個人描述、C021家庭情形、C052資格或技術、C061現行之受僱情形	勞安課	一般個資	員工資訊	微量	10年	紙本/檔案	高	低	低				
5	健康檢查申報資料	姓名、身分證號碼、性別、身高、體重、血型、病歷史、身心障礙紀錄	C001辨識個人者、C003政府資料中之辨識者、C011個人描述、C012身體描述、C066健康與安全紀錄、C111健康紀錄	勞安課	特種個資	員工資訊	微量	30年	紙本/檔案	高	高	中	紙本上鎖/檔案加密	102/06/15		
6																
7																
8																

空白表 | 範本參考 | 筆數 | 保存方式 | 衝擊性 | 風險分級

就緒 70%

附件七、全年教育訓練計畫書

大同技術學院　年度

全年教育訓練計畫書(年 月~ 年 月)

製表:　　年　月　日　製表人(教育訓練負責人):

大同技術學院全體教育訓練			
【目的】			
【主要內容】			
教育訓練內容/教育訓練對象	執行負責人	予定日期	小時

個別部門教育			
【目的】			
【主要內容】			
教育訓練內容/教育訓練對象	執行負責人	予定日期	小時
訓練			
【目的】			
【主要內容】			
教育訓練內容/教育訓練對象	執行負責人	予定日期	小時

附件八、個別部門教育訓練計畫、執行紀錄

教育訓練計畫　　製表日期 年 月 日 執行教育訓練負責人(　　)		
教育訓練名稱		
教育訓練目的		
教育對象		
執行教育訓練人(講師)	總計　　名	
使用資料		
預定執行日期		場所
例) 第 1 次　年 月 日		
第 2 次　年 月 日		
教育訓練內容		
<反應上次教育訓練內容>		
<教育訓練內容>		
確認教育訓練效果方法	例)問卷調查、隨堂測驗 等	
教育訓練負責人 核決	年　月　日　印	
執行教育訓練紀錄 製表日期　年　月　日　製表人(　　)		
<執行教育訓練內容>		
<應出席學員人數/出席學員人數>	簡任	(　名/　名)
	薦任	(　名/　名)
	委任	(　名/　名)
	派遣、計時人員	(　名/　名)
	總計	(　名/　名)
<本次教育訓練結果應反映於下次教育訓練事項>		
教育訓練結果處理	□ 不須處理 □ 需要追蹤教育訓練 □其他	
處理內容		
教育訓練負責人 審核	年　月　日　印	
管理代表　核決	年　月　日　印	

附件九、稽核查檢表

勞動力發展署 雲嘉南分署 委訓單位內部稽核自評表									
委訓機構名稱			OOOOO股份有限公司(完整名稱)		業管單位名稱		0000 發展中心		
個人資料保護規定				分類	檢核結果				檢核結果說明
					不適用(不列入計分)	未建立文件化或無機制(0)	不盡完整(4)	非常完整(8)	
A、個人資料保護政策與組織									
	A.1	個人資料保護政策							
1		A1.1	是否依據訂定個人資料保護政策，並公告實施。						
2		A1.2	管理政策是否規定於年度或組織重大改變時進行審查						
3		A1.3	工作人員(包括正職、約聘僱、工讀生或外包人員) 是否均了解個人資料保護規定及政策						
	A.2	個人資料管理組織							
4		A2.1	是否依規定指定個資專人，專人具備個人資料管理能力，並明確指派其個人資料管理執掌。						
5		A2.2	是否依規定指定專人，稽核人員具備個人資料稽核能力及獨立性，並明確指派其個人資料管理執掌。						
6		A2.3	是否針對個人資料事故處理指派管理人員，管理人員具備個人資料管理能力，並明確指派其個人資料管理執掌。						
7		A2.3	是否針對個人資料教育訓練指派管理人員，教育訓練具備個人資料管理能力，並明確指派其個人資料管理執掌。						
B、個人資料蒐集、處理及利用管理程序									
	B.1	招生管理							
			於委訓課程招生階段所有招生之文件，包括文宣品、廣告、網站、電子文件(包括檔案、電子郵件)、電子訊息(簡訊、其他						

使用說明 | 文件對照表 | 適當安全維護 | 內部稽核自評表 | 外部稽核查檢表 | 2.稽核審查報告書

附件十、稽核報告書

00 年度 內部稽核報告書

報告日期:_____

報告人(個人資料保護稽核負責人):_____

受內部稽核部門	
實施內部稽核日期	
內部稽核主題	
執行內部稽核人員所屬部門	
<內部稽核內容>	
<糾正事項。改善指示事項>	

附件十一、矯正預防單

矯正預防措施報告書

編號				年月日	
矯正預防措施執行部門		措施負責人（部門負責人）		提出糾正不符合人	

矯正措施計畫	「不符合內容」（記載為內部稽核報告書<糾正事項。要求改善指示事項>、機關外部糾正等）			
	「原因」（記載糾正事項發生的根本原因）			
	「防止再度發生方法」（提出消除發生原因之計畫）			
	提出計畫日期:		核決計畫日期:	
	提出計畫人: （部門負責人）		計畫核決人: （個人資料保護管理負責人）	
	預定執行矯正預防措施完畢日期:		是否需要確認矯正預防措施:■ 是 □ 否	
矯正措施執行結果	【執行矯正預防措施 內容】			
	執行完畢日期:		核決日期:	
	提出計畫人: （部門負責人）		計畫核決人: （個人資料保護管理負責人）	
審核	【確認矯正預防措施效果及有效性】			
	執行日期:		核決日期:	
	報告人:		核決人(機關代表人)	

附件十二、個人資料抱怨處理單

<table>
<tr><td colspan="3">大同技術學院　個人資料抱怨處理單</td></tr>
<tr><td rowspan="4">申請人</td><td>姓名</td><td></td></tr>
<tr><td>身分證統一號碼</td><td></td></tr>
<tr><td>通訊住址</td><td></td></tr>
<tr><td>聯絡電話</td><td></td></tr>
<tr><td>抱怨事項說明</td><td colspan="2"></td></tr>
<tr><td>建議處理方式</td><td colspan="2"></td></tr>
<tr><td>備註</td><td colspan="2"></td></tr>
<tr><td colspan="3">中華民國　　年　　月　　日</td></tr>
</table>