



符合

- 1.實際作業依照書面規範進行；紀錄及審核皆按照規定辦理。
- 2.已建立書面規範，但**尚未有實際作業或紀錄**。

部份符合

- 1.雖按照規範執行作業，但於過程中發生疏失或無相關書面紀錄。
- 2.作業流程尚有改善空間。

不符合

- 尚未規劃或執行相關安全管理規定。

不適用

- 學校之現行作業**無相關作業需求**。

訂定學校資通安全管理規範且經校長簽核及公告

- 建議參考新版(103年2月)之資通安全管理系統進行改版。
- 公告佐證

【網路控制措施】02提供資料為架構圖與網段分配。

- 架構圖。
- 網段分配。

163.25.126.130	網路中心	主機		
163.25.126.131	校長室			
163.25.126.132	秘書			
163.25.126.133	總務			
163.25.126.134	會計			
163.25.126.135	教務			
163.25.126.136		201		
163.25.126.137		101		
163.25.126.138				
163.25.126.139				
163.25.126.140				
163.25.126.141				
163.25.126.142	網路中心	101 - 104		
163.25.126.143	網路中心	101 - 104		
163.25.126.144				
163.25.126.145				
163.25.126.146	網路中心			
163.25.126.147				
163.25.126.148	網路中心	101 - 104		
163.25.126.149				
163.25.126.150				
163.25.126.151	網路中心	101 - 104		
163.25.126.152	網路中心	101 - 104		
163.25.126.153	網路中心	101 - 104		
163.25.126.154	網路中心	101 - 104		
163.25.126.155	網路中心	101 - 104		
163.25.126.156	網路中心	101 - 104		
163.25.126.157	網路中心	101 - 104		
163.25.126.158	網路中心	101 - 104		
163.25.126.159	網路中心	101 - 104		
163.25.126.160	網路中心	101 - 104		
163.25.126.161	網路中心	101 - 104		
163.25.126.162	網路中心	101 - 104		
163.25.126.163	網路中心	101 - 104		
163.25.126.164	網路中心	101 - 104		
163.25.126.165	網路中心	101 - 104		
163.25.126.166	網路中心	101 - 104		
163.25.126.167	網路中心	101 - 104		
163.25.126.168	網路中心	101 - 104		
163.25.126.169	網路中心	101 - 104		
163.25.126.170	網路中心	101 - 104		
163.25.126.171	網路中心	101 - 104		
163.25.126.172	網路中心	101 - 104		
163.25.126.173	網路中心	101 - 104		
163.25.126.174	網路中心	101 - 104		
163.25.126.175	網路中心	101 - 104		
163.25.126.176	網路中心	101 - 104		
163.25.126.177	網路中心	101 - 104		
163.25.126.178	網路中心	101 - 104		
163.25.126.179	網路中心	101 - 104		
163.25.126.180	網路中心	101 - 104		
163.25.126.181	網路中心	101 - 104		
163.25.126.182	網路中心	101 - 104		
163.25.126.183	網路中心	101 - 104		
163.25.126.184	網路中心	101 - 104		
163.25.126.185	網路中心	101 - 104		
163.25.126.186	網路中心	101 - 104		
163.25.126.187	網路中心	101 - 104		
163.25.126.188	網路中心	101 - 104		
163.25.126.189	網路中心	101 - 104		
163.25.126.190	網路中心	101 - 104		
163.25.126.191	網路中心	101 - 104		
163.25.126.192	網路中心	101 - 104		
163.25.126.193	網路中心	101 - 104		
163.25.126.194	網路中心	101 - 104		
163.25.126.195	網路中心	101 - 104		
163.25.126.196	網路中心	101 - 104		
163.25.126.197	網路中心	101 - 104		
163.25.126.198	網路中心	101 - 104		
163.25.126.199	網路中心	101 - 104		
163.25.126.200	網路中心	101 - 104		

對於開放提供外部使用者或廠商存取之服務，必須限制使用者之來源IP及網路連線埠(Port)，以確保安全。

- 防火牆設定
- 提供臺南市連線單位開埠申請單。

校園內應提供無線網路存取服務，並採取適當安全管控措施：

- (1)專供行政使用之無線網路熱點建議設定加密金鑰防護，並避免使用開放之無線網路存取重要資訊系統及處理敏感性資料。
- 提供SSID與金鑰畫面。
- 校園無線網路管理要點。

校園內應提供無線網路存取服務，並採取適當安全管控措施：

- (2)於教學區域、會議室等場所佈建之無線網路熱點應具有使用者身分認證機制，並經由校園無線路漫遊服務系統提供外校來賓使用。
- 提供SSID與金鑰畫面。
- 校園無線網路管理要點。

校園內應提供無線網路存取服務，並採取適當安全管控措施：

- (3)專供師生教學活動使用之無線網路熱點，若採用其他管理方式確有不便時，應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。
- (4)開放校外人士出入之公共空間可視需要提供民眾無線上網服務，其網段應與校園網路隔離，或委由網路服務業者提供。
- 校園無線網路管理要點。

【桌面淨空與螢幕淨空政策】

- 個人電腦辦公桌面應避免存放機敏性文件，結束工作時，應將其所經辦或使用具有機密或敏感特性的資料（如公文、學籍資料等）妥善存放。
- 當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及終端機安全，個人電腦應設定螢幕保護機制。
- 提供至少兩人以上照片。

【資料備份】

- 系統管理人員需針對學校重要電腦系統及資料（如：系統檔案、網站、資料庫等）應每週至少進行一次備份工作；建議使用設備執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。
- 提供設定畫面。
 - 手動
 - 自動

【資料備份】

- 每年應定期檢查備份資料之可用性與完整性。
- 提供畫面或設定。
 - 比對大小。
 - 實際測試回讀。

【資訊存取限制】

- 共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）應以特定功能為目的，並設定特定安全管控機制（如：限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。
- 電腦教室使用規範或管理辦法。
- 自動－回復系統（還原卡）。
- 手動－GPO限制安裝。

【使用者註冊】

- 人員報到或離退職應會辦電腦系統帳號管理人員，執行電腦系統的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容：
- (1)使用唯一的使用者帳號。
- (2)檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
- (3)保存一份包含所有帳號註冊的記錄。
- (4)使用者調職或離職後，應移除其帳號的存取權限。
- (5)每學期應檢查使用者帳號，以確保帳號的有效性。
- 提供帳號申請單紀錄。

【使用者註冊】

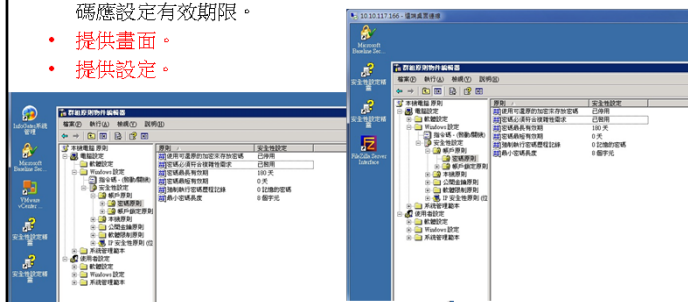
- 電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄。
- 提供特權帳號清單紀錄。

【使用者註冊】

- 電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄。
- 提供特權帳號清單紀錄。

【通行碼 (Password) 之使用】

- 管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。
- 提供畫面。
- 提供設定。



【溫濕度控制】

- 重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控制在 $20^{\circ}\text{C} \sim 25^{\circ}\text{C}$ ，濕度建議控制在相對濕度 $50\%\text{R.H.} \sim 70\%\text{R.H.}$)，以防止資訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。
- 溫度計+溼度計。
- 提供照片。



【財產攜出】

- 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。

【財產攜出】

- 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。
- 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。
- 提供表單紀錄

可攜式電腦設備與媒體

- 公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等。
- 公務用可攜式電腦設備應執行安全相關程序(如：掃毒、預設通行碼更新、系統更新等)，以防範可能隱藏的病毒或後門程式。
- 提供畫面。

資訊業務委外管理

- 【服務委外廠商合約之安全要求】
- 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規定。
- 應要求委外廠商簽訂安全保密切結書。
- 委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書。
- 委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限。
- 保密切結書。
- 帳號申請單紀錄。

資訊業務委外管理

- 【服務委外廠商合約之安全要求】
- 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規定。
- 應要求委外廠商簽訂安全保密切結書。
- 委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書。
- 委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限。
- 適不適用？
- 保密切結書。
- 帳號申請單紀錄。

宣導師生遵守智慧財產權、個人資料保護法及其施行細則、刑法電腦犯罪專章等相關法令規定。

- 教育宣導公告／紀錄。

【界定個人資料之範圍】

- 進行個人資料盤點後，建立「個人資料檔案清冊」，並依個資法規定於網站公布個人資料檔案大綱。

【個人資料蒐集、處理及利用之內部管理程序】

- 進行個人資料之蒐集與利用時，必須符合法令規定，包含：
- (1)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。
- (2)蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。
- (3)除符合法令規定外，有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。
- (4)當資料利用範圍超出蒐集的特定目的時，應依個資法規定取得當事人之書面同意。
- 同意書

【事故之預防、通報及應變機制】

- 學校須設置「個資保護聯絡窗口」，協調聯繫個資事宜，並將聯繫方式(如：電話、email)置於單位網站，以便利民眾提出申訴與救濟。
- 提供聯絡窗口並公告。

【資料安全管理】

- 對於個人資料之調閱，須有申請及核准程序，並記錄保存調閱者身分及行為。
- 提供個資調閱申請單。

全國中小學線上資安稽核介紹

資安注意事項

個資保護

專家破解Adobe外洩帳號資料，近200萬人使用123456當密碼

文章連結: [https://bit.ly/301311106](#)
訂閱 (72) | 分享 | 8+1 | 2 | 我要收藏
Jeremi Gosney 下載在網路上曝光的 Adobe 用戶檔案，並破解其中 600 萬筆密碼，列出最常被使用的前 100 組密碼。Adobe 用戶最常使用的密碼是 123456，總計有 190 萬名。

Adobe 今年 10 月遭資安專家攻擊，公布有 800 萬名用戶的資料清單，其中包括失效帳號則超過 1.5 億，專門破解密碼的 Stricture Consulting Group 創辦人 Jeremi Gosney 下載了在網路上曝光的 Adobe 用戶檔案，並破解其中較容易破解的 600 萬筆密碼，從而列出了前 100 組最常用的密碼。

Adobe 自宣布被駭後餘波不斷，先是受影響的用戶數從原先預估的 200 萬到最後證實 800 萬，而曝光的檔案則顯示包含已失效帳號在內的客戶數總計有 1.5 億名。此外，資安業者還懷疑，其他網站亦受到池魚之殃，因為這些網站使用了已被駭客竊取程式碼的 Adobe 產品。

Gosney 所下載的 Adobe 用戶檔案含有 1.3 億筆帳號，他分析了其中的 600 萬筆，列出最常被使用的前 100 組密碼，不過，由於 Adobe 禁止未更改密碼的用戶登入，因此已無從驗證這些密碼。

根據 Gosney 的統計，Adobe 用戶最常使用的密碼是 123456，總計有 190 萬名的用戶選擇以 123456 作為帳號密碼，其他前十名密碼則依次是 123456789、password、adobe123、12345678、qwerty、1234567、111111、photoshop 及 123123 等。(編譯陳曉莉)

20組最糟糕的數字密碼

- 2011年最糟糕的線上密碼，多數人使用「123456」和「qwerty」當做網路上經常設定的密碼，相信看過報導的你絕對不會再用這些愚蠢的密碼了。不過，人一生中的密碼何其多，還有另一種藏在口袋裡的四位數密碼，如果被解開，帶來的財產損失將會讓你更慘。根據分析業者Data Genetics的調查，研究分析了340萬筆提款卡密碼，你一定可以猜到最多人使用的密碼為何，沒錯！「1234」有11%的人使用，另外「1111」也有6%的人使用。

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

駭客不攻自破！密碼Password1企業最愛、welcome第二

翻譯：可能很多老闆看到這則新聞會抖一下

【漢編】有熊貓眼並不會跟熊貓一樣可愛！

國際中心／綜合報導

密碼

登入
無法登入您的帳戶？

什麼樣的密碼是企業系統的最愛？根據美國有線電視財經新聞網(CNNMoney)報導，Trustwave保安公司日前總結了近200萬筆網路密碼掃描與300筆安全漏洞調查結果發現，企業系統最常用的密碼是「Password1」。

據報導，Password1的密碼組合之所以如此普及，其實得歸咎於技術層面上的原因，Password1因擁有一個大寫字母且包含數字，且包含多達9個字的字符，因此滿足了許多系統的複雜規則。而Trustwave的研究人員也表示，大約有5%的密碼都從password這個字變化而來，另外第2常用的密碼是welcome，也有超過1%的使用量。

▲企業系統最常用的密碼是「Google」

國際中心／綜合報導

另外，根據美國網路密碼管理程式供應商SplashData所公佈的25大最糟的密碼也顯示，有規律可循的密碼最常被破解。而不少人直接用手機號碼、生日等個人資料項目作成簡單易記的密碼，也讓自己容易身陷於網路詐騙與身份竊盜的風險，成為駭客及詐騙集團的目標對象。

SplashData建議，網路使用者應盡量採用英文、數字、與符號交雜的密碼，且字元長度務必超過8個字，另外，在不同的網站也要採取不一樣的使用者名稱與密碼。

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

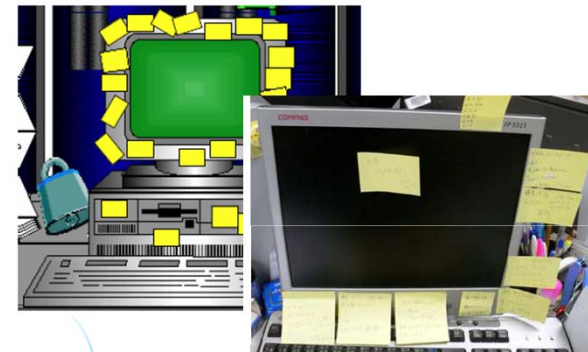


BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

密碼=明碼

密碼輸入？明碼張貼！！



BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

XP系統的病毒感染率是Win8的6倍

- XP 於2014年4月中止技術支援!!

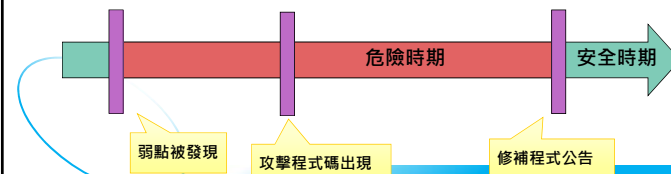


BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

軟體弱點與零時差攻擊

- 只要是軟體即有可能存在弱點，若未能及時修補弱點，即可能讓駭客入侵成功
- 軟體弱點在沒有任何修補方式之前，出現相對應的攻擊行為時，此類攻擊稱為「**零時差攻擊 (Zero-day Attack)**」



BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

IE的使用



BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

國家資安通報警告：KMPlayer更新程式疑遭駭客下毒

文獻文庫 (記者) 2013-08-07

【本報訊】國家資安通報中心(TWNC)向K9Net及KMPlayer反應，期待原廠提出說明。

資通安全辦公室指出，經過檢測KMPlayer軟體更新行為，發現會連線至韓國伺服器下載新程式，部份用戶因不明原因下載惡意程式，側錄使用者鍵盤、連線到中繼站等等。建議曾使用KMPlayer軟體更新的民眾可以防病毒軟體偵測刪除，避免受到影響。

另外，不願具名的知名資安業者表示，透過管道取得惡意程式，確認為遠端後門程式，使用者電腦被感染後可能打劫電腦內的資料，設立控制帳號、連接其他伺服器等等。

由於韓國在今年3月爆發最大規模的APT攻擊事件，導致韓國多家銀行、電視台、保險公司電腦故障，駭客便是利用其更新程式大規模散佈惡意程式。統計約有4.8萬台設備故障，影響韓國日常生活正常。

有鑑於此，行政院資通安全辦公室指出，先前韓國重大資安事件中駭客攻擊手法就透過軟體更新滲透用戶電腦主機，以此發起影響層面更大的DDoS攻擊。韓國近期政府網站被攻擊都是經由此手法進行。另外，駭客利用具發行權的合法程式植入惡意程式進行攻擊，駭客攻擊行為已更為隱密。民眾應加強資安意識，避免使用來源不明軟體，成為駭客攻擊的跳板。

根據其說明，KMPlayer用戶啟動更新後，給出現版本3.7.0.87更新訊息，啟動更新後將連線至http://cdn.kmplayer.com/player/hpdata下載假冒的更新程式KMPlayer_3.7.0.87.exe，執行該程式後不會變更版本，但使用者電腦將被植入惡意程式。

BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

檔管局電子公文交換中心入侵事件

• 事件說明：

- 調查局於5月8日發現，該局5台安裝eClient公文軟體的電腦，出現不正常連線至孟加拉地區中繼站。追查後，發現惡意程式源頭來自檔管局。
- 至5月10日1730時，經調查局查證確認，原由研考會發包建置，去年中移交檔管局管理之「政府公文電子交換系統」中之「版本更新系統」遭駭後被植入惡意程式。

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

BYOD

員工自帶設備上班

BYOD的兩難

手機、平板等行動裝置的流行，在歐美企業收稅一點讓員工自帶設備上班的BYOD (Bring Your Own Device) 風潮，員工可以透過新一代行動裝置隨時掌握業務、快速協同合作，不再受到固定裝置束縛之後，工作生產力可以大為提升。但私人設備進入企業網路，一旦被駭客攻擊，企業網路就與門戶大開，如何保護這些不屬於企業、而且移動性高的裝置，就是一個全新的挑戰。該如何兼顧效益又能避免風險，正是BYOD帶給CIO的兩難。(請見第23頁)

病人隱私是所有醫療人員的責任—從小護士網路分享剖腹生產過程照片談起

為此項目評分 ☆☆☆☆☆ (0 票)

心儀 誰？人說這話，成為你朋友中第一個被罵的人。

在行醫時所見所聞或關於他人生活上的隱私，我必對這不可洩漏的祕密守口如瓶。～西遊交拉恩的書信[1]

醫療機構及其人員因疏忽或持有病人病歷或健康資訊，不得洩漏洩漏。～醫法第72條[2]

一位實習護士將前線發生的照片張貼在個人部落格，再度引起社會大眾對於醫療人員洩漏病人隱私之行為的關注。這對新聞隱私保護問題[3-5]：

1. 將沒經過適當消毒滅菌的物品帶進手術室內，可能增加病人感染風險。
2. 實習學生也是醫療團隊的一員，在維護生命健康的醫療工作場合，應專注於照顧病人及學習，怎麼有時間拍照拍VIA?
3. 洩漏病人病歷，洩漏醫療資訊，將病人資料放在網路上，洩漏病人隱私。
4. 缺乏同理心，完全沒考慮病人的感受，以及可能受到的傷害。
5. 醫療團隊會對學生要求嚴格的時候，不但完全考慮消毒及感染問題，而且以為是為了教學的經驗分享就洩漏拍攝，完全沒考慮是否已經洩漏病人隱私，對於病人安全及病人隱私的意識有問題。
6. 顯然是個人行為，但是會影響社會大眾對於醫療的信任，擔心自己會不成為下一個被偷拍的對象。

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

資料外洩

南韓爆發1.04億筆信用卡資訊外洩案，40%人口受影響！

竊取大量資料的是南韓信用評價組織所聘請的39歲男性電腦工程師，他負責開發可辨識偽卡的軟體，並有機會存取南韓三大發卡公司KB Kookmin Card、Lotte Card與NH Nonghyup Card的資料庫，自2002年5月到去年12月間多次趁機將資料庫中的個人資料複製到USB裝置上，並在今年1月被捕。



2009電子郵件社文...ppt
取消

因應措施

- 公用隨身碟
- 資料加密

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

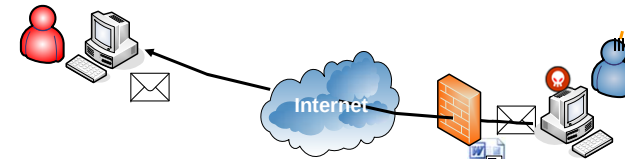
郵件社交工程攻擊之定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊。
- 透過電子郵件進行攻擊之常見手法
 - 假冒寄件者
 - 使用與業務相關或令人感興趣的郵件內容
 - 含有惡意程式的附件或連結
 - 利用應用程式之弱點(包括零時差攻擊)

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

社交工程攻擊模式



1. 駭客設計攻擊陷阱程式(如特殊 Word 檔案或外部惡意連結)
2. 將攻擊程式置入電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，將被植入後門程式

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

真實案例

顯示名稱雖為政府單位，但寄件者仍有可能偽造!!!!

Q1: 收件者不是交通部員工，為何會收到此郵件？
A: 原來是密件副本傳送！
Q2: 部分文字及用語來自對岸？
A: 出現異常簡體字！
Q3: 公告之規定需要加密嗎？
A: 違反常理！

BCC 漢昕科技

資安稽核

使用者防護停看聽(1/4)

- **停** – 使用任何電子郵件軟體前，必須先**確認**

1. 執行各種作業系統、應用軟體設定更新
2. 必須**安裝防毒軟體**，並確實**更新病毒碼**
3. 收信軟體安全性設定
 - 必須以**純文字模式**開啟郵件
 - 必須**取消郵件預覽**功能
4. 防止垃圾郵件
 - 設定**過濾垃圾郵件**機制
5. 啟用個人防火牆

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

使用者防護停看聽(2/4)

• 看 – 開啟電子郵件前應先依序檢視：

【寄件者】：

1. 若【寄件者】與您業務相關且認識，並確認電子郵件信箱位址無誤，如有冒用偽裝情形，則建議直接刪除該郵件。
2. 若【寄件者】來自政府機關，其信箱位址應屬於gov.tw，若【寄件者】來自非政府機關，則應特別謹慎確認。

【郵件主旨】：

- 若【郵件主旨】與您業務無關或主旨怪異，則建議直接刪除該郵件。

使用者防護停看聽(3/4)

【附加檔案】：

1. 若【附加檔案】名稱顯示與您業務無關或檔名怪異、錯誤，請勿開啟【附加檔案】或建議直接刪除該郵件。
2. 若有需要開啟【附加檔案】，不得直接點選開啟檔案，應先另存新檔後，再使用相關軟體開啟。

使用者防護停看聽(3/4)

• 聽 – 若懷疑郵件來源，必須進行確認

- 透過電話或電子郵件向寄件人確認郵件真偽

不要在開啟郵件狀況下，直接按刪除鈕，
應回到郵件清單(index)下刪除郵件，
以免無意間直接開啟下一封郵件。

雲端運算??

是白雲?

是烏雲?

雲端



BCCS 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

安全性議題-資料保密

- 使用雲端儲存服務時，所有的資料都是交由第三方幫忙儲存，這也意味著雲端服務的提供商有能力去窺探資料。



BCCS 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

安全性議題-資料的責任歸屬

• 檔案的刪除

— 當使用者刪除了儲存在雲端的資料時，有沒有辦法確認資料真的已經被刪除了呢？像是雲端儲存供應商有沒有可能說謊，沒有刪除資料卻回覆使用者說資料已經被刪除了；或者是雲端儲存供應商因為有將資料進行多份的儲存機制（如Amazon，或是像Google所使用的The Google File System），有沒有可能有漏刪掉其中某一份儲存的資料呢？這個問題對使用者來說很難確認，因為所有的機制都掌握在雲端儲存供應商那邊。

BCCS 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

- 絕大部分的雲端儲存服務供應商都有完善的備援機制，但「如果真的不幸發生的話怎麼辦？」

BCCS 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

- Dropbox

- You, **and not Dropbox**, are responsible for maintaining and protecting all of your stuff. Dropbox will not be liable for any loss or corruption of your stuff, or for any costs or expenses associated with backing up or restoring any of your stuff.

- Amazon

- Data that is maintained within running instances on Amazon EC2, or within Amazon S3 and Amazon SimpleDB, is all customer data and therefore AWS does not perform backups.

- Google

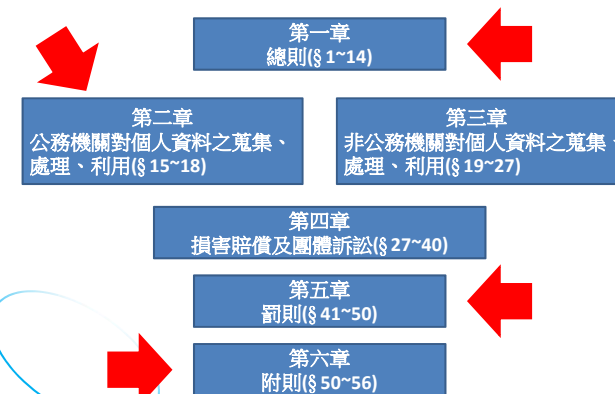
- Google、其子公司及關係企業，及其授權人，就以下事項並未向台端作出聲明或保證：
 - (A) 台端對服務之使用將符合台端需求；
 - (B) 台端對服務之使用將不受中斷，且及時、安全、無錯誤；
 - (C) 台端因使用服務而獲得之任何資訊，皆屬準確或可靠；及
 - (D) 台端連同服務獲得提供之任何軟體所發生之操作或功能瑕疵將獲得改正。

全國國中小學線上資安稽核介紹

資安注意事項

個資保護

個人資料保護法



個人資料保護法重點

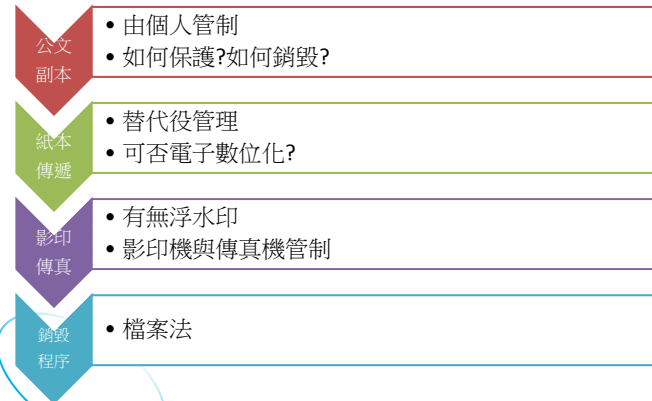
• 擴大保護客體

- 為落實對個人資料之保護，將保護客體予以擴大，**將非經電腦處理之個人資料(即人工資料)一併納入保護**

• 普遍適用主體

- 刪除非公務機關行業別之限制，**使任何自然人、法人或其他團體**，除為單純個人或家庭活動之目的而蒐集、處理或利用個人資料外，皆須適用本法
- 公務機關及非公務機關，**在中華民國領域外對中華民國人民蒐集、處理或利用個人資料者**，亦適用本法

紙本文件為個資外洩最容易遺忘的漏洞



蒐集：指為建立個人資料檔案而取得個人資料

直接向當事人蒐集者
間接從第三人取得者

處理：指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

國際傳輸：指將個人資料作跨國(境)之處理或利用
機關內部之資料傳送(資料處理)
將資料提供當事人以外之第三人(資料利用)

個人資料保護法重點

• 增修行為規範

- 增訂醫療、基因、性生活、健康檢查及犯罪前科等五類資料為特種資料，除符合法定要件外，原則上不得蒐集、處理或利用
- 如符合法定要件需要去識別化

個資去識別化



BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

個人資料保護法重點

• 增修行為規範

- **書面同意內涵明確化**，特定目的外利用個人資料需當事人書面同意者，**應另以單獨書面同意方式為之**
- 不論是直接或間接蒐集資料，除符合得免告知情形者外，**均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項**
- 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除或停止蒐集、處理或利用其個人資料
- 從事商品行銷之非公務機關，**應於首次行銷時免費提供當事人表示拒絕之方式**

BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核



BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

個人資料保護法重點

• 調整責任內涵

- **民事責任**：提高基於同一原因事實應對當事人負**損害賠償責任之總額2億**(被害人不易或不能證明其實際損害額時，得請求法院依侵害情節以**新臺幣5百元以上2萬元以下計算**)
- **刑事責任**：非「意圖營利」者得**科處2年以下有期徒刑(告訴乃論-除罪化)**；「意圖營利」者得**科處5年以下有期徒刑(非告訴乃論)(41)**
- 公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(44)

BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

個資法爭議-兩階段實施

第6條規定，包括「醫療、基因、性生活、健康檢查和犯罪前科之個人資料，不得蒐集、處理或利用。」

暫緩實施。未來修法方向：將新增經當事人同意，可以使用敏感性個資的條文。

第41條第1項規定，若有違反個資蒐集、處理、利用，足生損害於他人者，處2年以下有期徒刑。

如期實施。未來可能修法：針對不同情節的輕重，重新釐清相關的罰則。(非意圖營利除罪化)

第54條規定新版個資法在施行後1年內，企業必須以書面告知個資當事人。

暫緩實施。未來修法方向：將1年內完成告知的方式，改為在企業要使用到個資之前完成告知。

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

個資法考量的重點

個資盤點及保存(蒐集、處理、利用、種類、數量、型式)

適當安全維護措施(12)

- 成立管理組織，配置相當資源。
- 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。
- 必要之使用紀錄、軌跡資料及證據之保存。
- 個人資料安全維護之整體持續改善。

特定目的(5)

告知(直接/間接蒐集)(8,9)

書面同意(7)
(電子文件、契約取得、書面)

蒐集(2) 處理(2)

利用(2)

違法侵害之通知(12)

特定目的外的利用(7)

利用目的

利用範圍

書面同意

公開作業 § 17

委外管理(7,8)

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

適當安全維護措施

徵求託者、約定之委託

違約通知及補救

保留指示事項

資料返還及刪除

接受當事人行使權利(3)

查詢

閱覽

制給複本

補充

更正

停止蒐集處理利用

刪除

個人資料檔案維護計畫(非公務機關)

個人資料安全維護規定(公務機關-18)

業務終止後個人資料處理方法

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

個資主要外洩管道

1 • 電子郵件社交工程

2 • 惡意/非法軟體

3 • 可攜式設備(USB/智慧型手機)

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

案例1

• 680份保單掉滿街 妥洩個資 台灣產險未道歉

【石永軒／新北報導】新北市一名男子前晚帶著家人在三重街頭散步時，發現數百張紙片沿街飄散，拾起一看竟是台灣產物保險公司的客戶個資，上頭不但清楚列出客戶年籍通訊資料，還有重要證件影本，熱心的他怕資料遭盜用，全家動員撿拾，將680多份資料送交警局，當警方通知保險公司領回資料，保險公司還不情願地說：「可不可以過完年再領？」令警民大呼離譜。

「詐騙集團添業績」

從事資訊業的葉先生表示，前晚8時許他飯後跟妻子及5歲的兒子，在三重厚德國小旁散步，發現沿路約4、5百公尺散落著大量紙片，撿起來一看竟是台灣產物保險公司的要保單，上面有客戶年籍資料，貼著各式證件影本，還有外國人的護照資料，他搖頭痛批：「天啊！這些個人私密資料竟被隨便丟在大馬路上，詐騙集團拿到肯定業績增加不少。」

葉先生說，他當時立刻報警並與妻兒一張一張將資料撿起，過程中也有3名熱心的路人加入，其5歲兒子自豪地說：「我也有幫忙撿哦！」警員到場後也加入搶救個資行列，15分鐘後總算將街上所有個資都撿回。

警方表示，台灣產物保險公司散落的個資計有680多份，事後打電話通知該公司來領回，一度遭誤認是詐騙集團，隨後保險公司稱資料已報廢，可否年後再派員領回，「難以理解業者竟如此漫不經心對待個資。」

BCC 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

案例2

- 新聞事件：買二手硬碟 赫見銀行往來個資 【中央社台北29日電】2012.02.29
- 全文網址: [買二手硬碟 赫見銀行往來個資 | 生活新聞 | 生活天氣 | 聯合新聞網 http://udn.com/news/LIFE/LIF1/6930184.shtml#ixzz1ul7CxtsR](http://udn.com/news/LIFE/LIF1/6930184.shtml#ixzz1ul7CxtsR)
- 在某黃姓立委於舉行記者會時指出，一名林姓民眾向他反映，在光華商場購買2顆中古硬碟，接上電腦後發現有銀行業者的工作資料、民眾與銀行往來借貸相關資料，並清楚記載與銀行業務往來的民眾姓名、身分證資料、地址、借款金額等相關資料。
- 其實報廢IT設備或紙本資料出現機密資料的新聞時有所聞，一旦要汰換IT設備或報廢紙本資料時，往往直接丟棄或交由廠商回收，不會想到要檢查硬碟內或紙本資料是否還存有機密資料，由此看來許多機構在系統和技術上的資安表現可以做到近滿分，但在管理上卻常受到忽視。

因應措施

- 檔案銷毀執行
 - 確認保存期限
 - 銷毀前：需有相關人員再場見證，並再次由管理人員確認銷毀之標的物。
 - 銷毀時：於銷毀過程中需會同相關單位派員全程監控，且進行錄音/錄影/拍照存證，並由承辦人員負責安排相關事宜。此外，相關銷毀作業亦需配合環境保護相關作法。
 - 銷毀作法：
 - 硬體/檔案銷毀方式
 - » 可選擇消磁、格式化、覆寫、物理摧毀/光碟磨損(毀)、化為粉末等
 - 紙本資料方式
 - » 可選擇消化為碎紙或溶為紙漿、焚化、碎至檔案內容無法辨識等

學生個資

蒐集、處理、利用可以免告知的情形

- 特定目的內
 - 執行法定職務必要範圍內
 - 經當事人書面同意
- 特定目的之外
 - 法律明文規定
 - 公務機關或學術研究機構基於公共利益為統計或學術研究
 - 經當事人書面同意

何謂[法定職務]?

依個資法施行細則第 10 條

- 一、法律、法律授權之命令。
- 二、自治條例。
- 三、法律或自治條例授權之自治規則。
- 四、法律或中央法規授權之委辦規則。

法律賦予學校法定義務

- 國民教育法第 6 條
 - 國民小學及國民中學學生學籍資料，應以書面或電子方式切實記錄，永久保存並依法使用；其學籍管理辦法，由直轄市、縣（市）政府定之。
- 國民小學學籍管理要點

何謂特定目的？

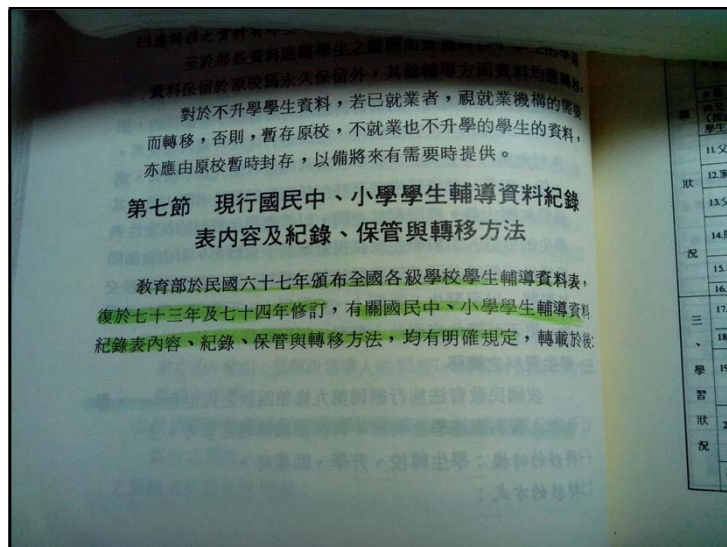
- 特定目的法務部已經公布
 - 請參照[個人資料保護法之特定目的及個人資料之類別]修正條文(101.10.04)
- 與教育相關的特定目的
 - 001 人身保險
 - 063 非公務機關依法定義務所進行個人資料之蒐集處理及利用
 - 109 教育或訓練行政
 - 158 學生（員）(含畢、結業生)資料管理
 - 159 學術研究

個資需有專人管理與安全維護

- 公務機關須指派專人管理與維護個資
 - 第 18 條：公務機關保有個人資料檔案者，應指定專人辦理安全維護事項.....
 - 本法第18條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。
- 個人資料輸入、輸出、更新或註銷時，應該釐定使用範圍，以及調閱或存取的權限

當事人對學生個資的權利

- 第三條：當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：
 - 查詢或請求閱覽。
 - 請求製給複製本。
 - 請求補充或更正。
 - 請求停止蒐集、處理或利用。
 - 請求刪除



國小校務系統應檢視系統表單

- 檢視空白表單列印區
 - 校務系統小組已開始檢視所有表單欄位，未來會將[無法令依據]或[違背法定職務與特定目的]個資欄位刪除。
- 檢視系統內各種匯出檔案
 - 匯入健康管理檔案
 - 緊急連絡卡
 - EXCEL成績匯出

BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

未來教育活動涉及個資需要告知或書面同意?

- 除非處理個資可能逾越特定目的、超過法定職務之必要範圍，否則應不需再請求同意(免告知)。
- 參閱個資法第8條，
 - 有下列情形之一者，得免為前項之告知(節錄)
 - 一、依法律規定得免告知。
 - 二、個人資料之蒐集係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。

BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

書面同意時機

- 書面同意?學生簽名或家長簽名?
 - 學生---國中小學生為[限制行為能力人]，需得法定代理人允許
- 學生入學後，填寫基本資料時，須告知家長個資運用範圍
 - 校務系統要修正[入學基本資料]表單

BCCJ 漢昕科技

代理通路 顧問服務 教育訓練 資安稽核

新法實施前所蒐集之個資，可繼續處理利用

- 個資法施行細則第 32 條
 - 施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得繼續為處理及特定目的內之利用
 - 其為特定目的外之利用者，應依本法 修正施行後之規定為之。

個案討論1---行政公告需要書面同意?

- ▶ 若符合學校「教育與訓練行政」特定目的，並有法律明文規定者，公佈免告知
 - 全市或後報到編班公告
(依高雄市國民小學學生常態編班補充規定)
- 有爭議之公告應個別告知或隱藏個資
 - 例如未繳註冊費、午餐費學童名單
 - 低收入戶、單親、外配子女、清寒等身分註記不宜公告，並維護與保管個資安全。

個案討論2

- 戶外教學保險
 - 戶外教學時投保平安保險，屬教育特定目的，亦有法律規定
 - 保險公司透過學校取得這份個資後，只能作為與保險業務範圍內的應用，不得延伸做其他不符合保險業務外之行銷或其他目的使用

學校全體須遵守個資法規範

- 凡學校教職員經手個資，皆須負個資安全維護之責
 - 全校教職員可為內部資料處理與利用並負安全維護之責
 - 個資利用需法定職務之必要範圍，並不可逾越特定目的

行政人員可因教育特定目的運用全校個資

- 依個資法，機關視為一個主體
 - 公務或非公務機關在合法蒐集個資後，得在特定目的以及有安全維護機制下，進行個資[處理]
- 個資處理定義(第2條第四款)
 - 個資法的[處理]原文：指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。
- 校務系統未來作法
 - 校務系統將開放行政人員依特定目的(辦理註冊、平安保險、獎助學金申請...)下載全校或學年名冊，但須經校內主管核准方可使用

校務系統個資安全維護措施



蝴蝶效應



總結

- 個資保護與資訊安全必須是一種習慣與文化，而不能只是一種技術與專業。

Thank You

感謝聆聽 請指教



代理通路 顧問服務 教育訓練 資安稽核