全校導入資訊安全管理系統

CNC 計算機與網路中心
COMPUTER & NETWORK CENTER

報告日期:111年3月24日
系統組黃慧娟組長
系統組林建成技術員
網路組陳志豪技術員

報告大綱

1. 導入緣由及年度規畫
2. 資通安全法應辦事項
3. 資通安全維護計畫
4. 資通系統與服務資產盤點
5. 資通安全政策與控管

全校導入資訊安全管理制度緣由

教育部-本校全機關實地稽核及後續改善措施
教育部-大專校院全校導入資安或個資管理制度諮詢會議

背景說明

- 近來教育體系資安事件頻傳，多為學校單位接受政府委辦補捐助計畫發生個資外洩。
- 根因顯示部分學校個人資料保護或資訊安全管理制度導入範圍限於資訊單位。
- 行政院資安處請本部督導改善，研議全校導入個人資料保護及資訊安全管理制度作法。

全校導入資訊安全管理制度緣由

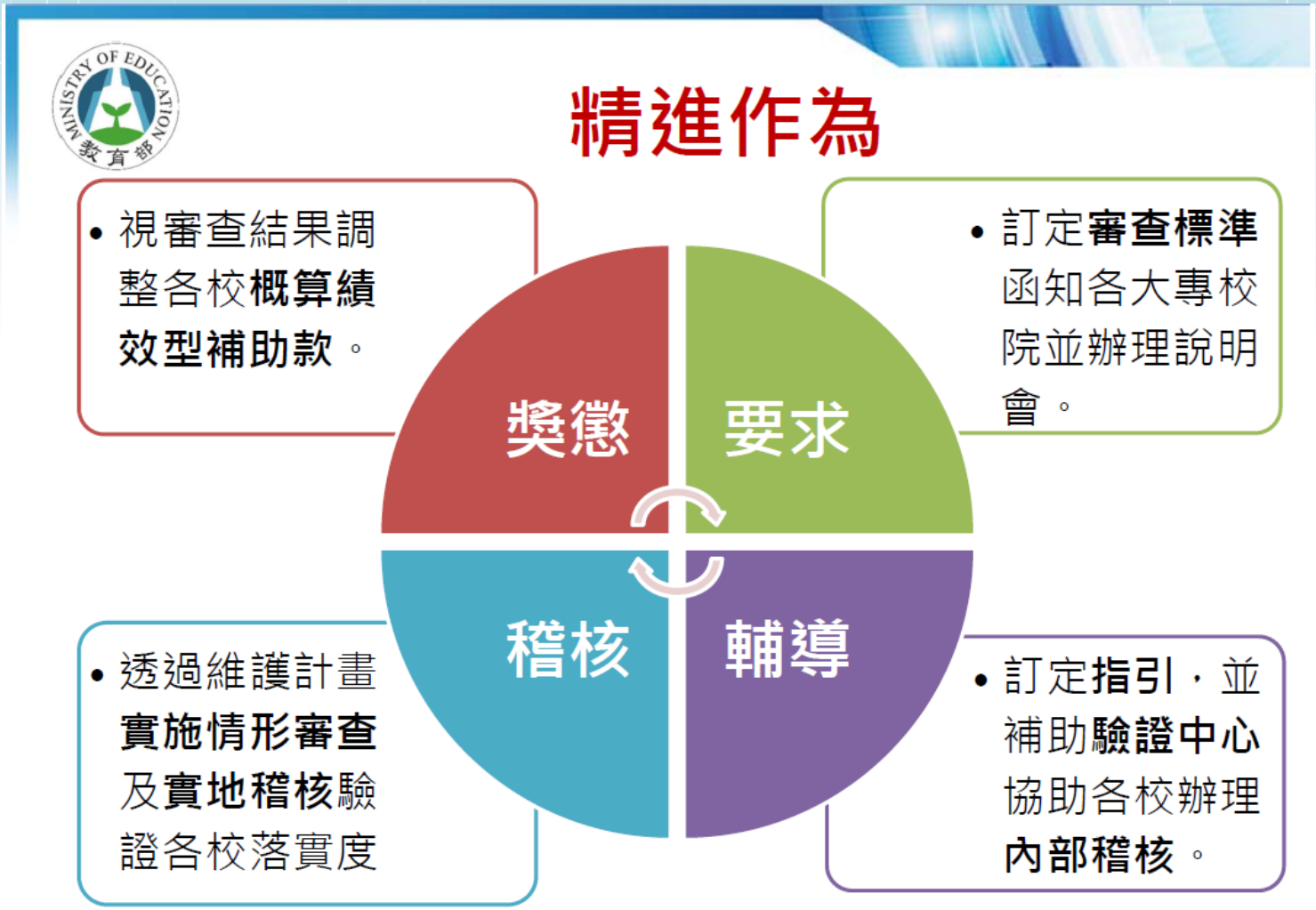
教育部-大專校院全校導入資安或個資管理制度諮詢會議

教育部初步規劃

- 研議全校導入個人資料保護及資訊安全管理制度作法，至少含全校業務或計畫涉及學生或民眾個人資料持有，或維運民眾服務，或跨機關共用性資通系統之系統。
- 110年9月30日前完成規劃並辦理說明會，110年12月31日前函文學校執行。

全校導入資訊安全管理制度緣由

教育部-大專校院全校導入資安或個資管理制度諮詢會議



全校導入資訊安全管理制度緣由

教育部-國立大專校院資通安全維護作業指引

二、各校依資通安全管理法第 10 條訂定、修正及實施資通安全維護計畫，適用範圍應涵蓋全校各系、院、所教學單位及各行政單位（以下簡稱全校各單位），並應注意下列事項：

（一）**資通安全長之配置**：各校置資通安全長，宜指派主任秘書以上人員兼任，以落實推動及監督校內資通安全相關事務。

（二）**資通安全推動組織**：各校資通安全推動組織宜由資通安全長召集全校各單位主管或副主管組成，每年至少召開會議一次。

（三）**資通系統及資訊之盤點**：各校辦理資通系統及資訊之盤點，盤點範圍應包含全校各單位。各校每年提交之「資通系統資產清冊」至少應包含落於各校 IP 網段內、或使用各校網域名稱之資通系統。

（四）**內部資通安全稽核**：各校辦理內部資通安全稽核，稽核範圍應包含全校各單位。各校得就資通系統（保有個人資料）風險高低、教學單位特性評估訂定推動先後順序，分年分階段規劃辦理，並明訂於各校資通安全維護計畫。

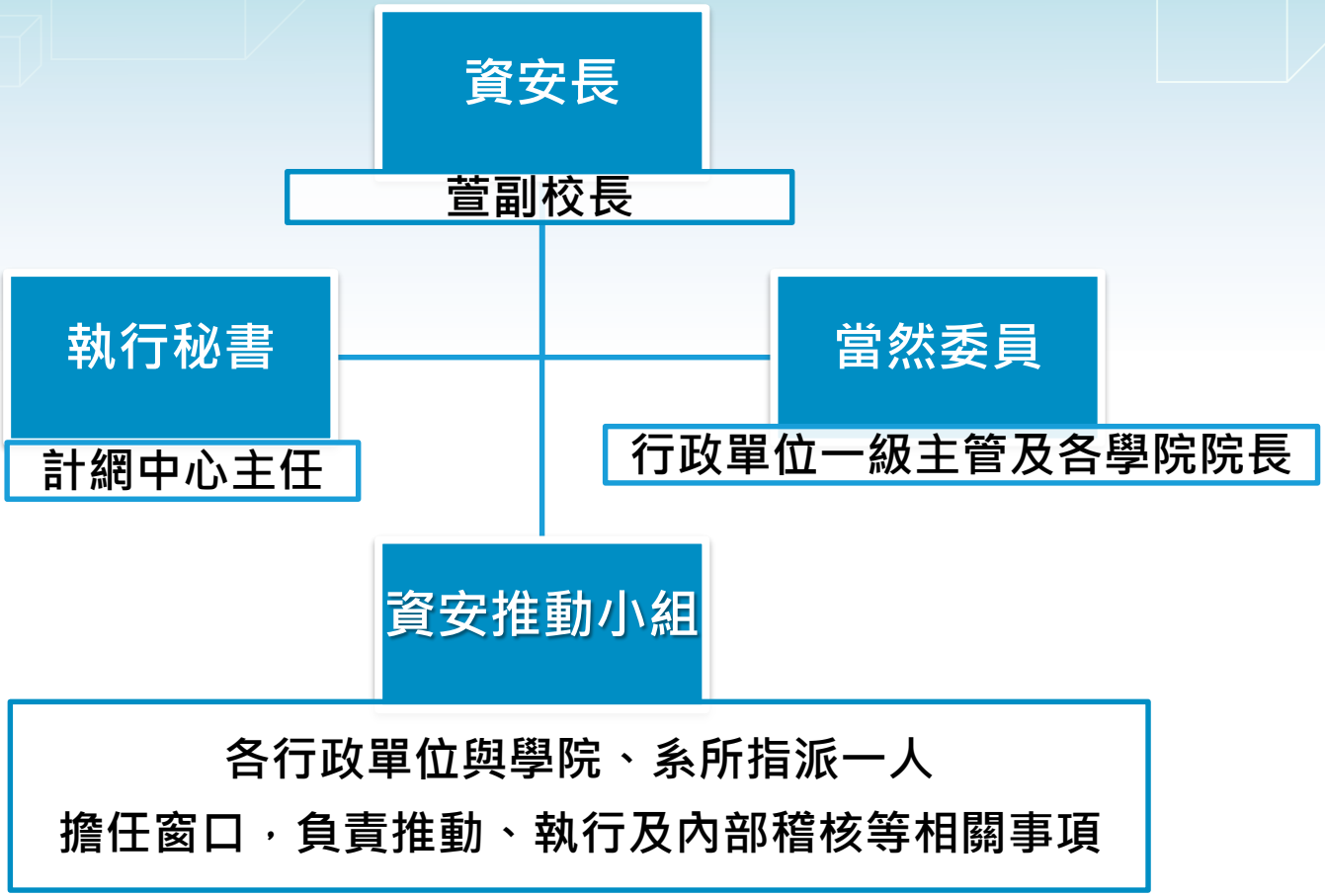
全校導入資訊安全管理制度規畫

111年重要工作項目

本校資通安全維護計畫 資通安全推動委員會	• 依教育部來文規範適用範圍涵蓋全校，成立資通安全推動委員會，設立「資安推動小組」
建置ISMS專區網站 小郵差進行全校性宣導	• 漏洞警訊公告.ISMS新聞.政府法規要求、導入推動事項、資安規範公告、資訊安全新知
辦理全校導入ISMS說明 資通系統與服務資產盤點	• 「資安推動小組」協助單位進行全校資通系統盤點、資通系統分級作業
辦理單位自我檢核訓練 全校資產盤點、自我檢核	• 參考教育部稽核項目檢核表，辦理自評說明 「資安推動小組」協助單位進行全校資產盤點、自我檢核並陳核主管
辦理全校資安內部稽核	• 「資安推動小組」協助全校資通系統內部稽核重點抽查

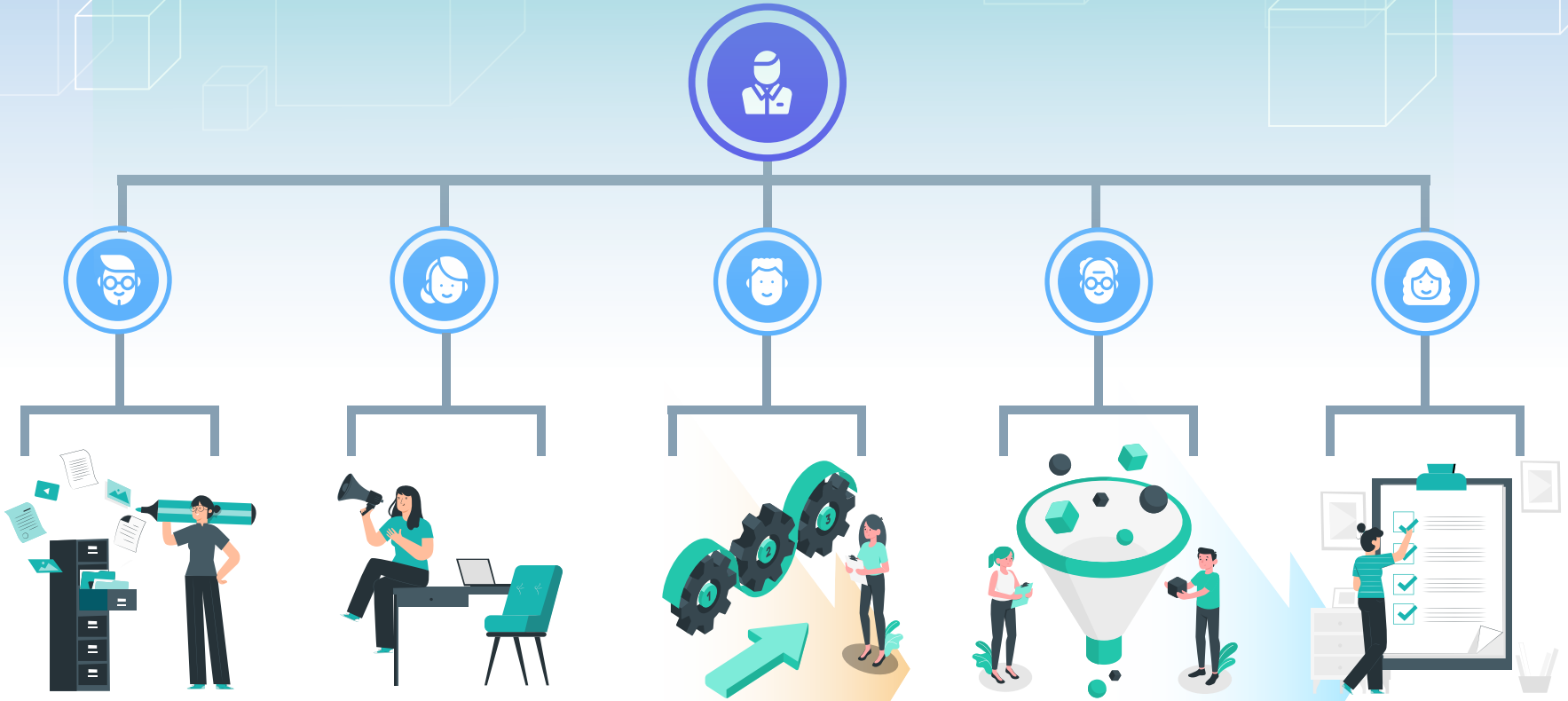
全校導入資訊安全管理制度規畫

臺北科技大學-資通安全推動委員會



全校導入資訊安全管理制度規畫

教育體系資安驗證中心-應優先落實的執行策略



- 2.4 成立資通安全推動組織，負責推動、協調監督及審查資通安全管理事項？推動組織層級之適切性，且業務單位是否積極參與？

全校導入資訊安全管理制度規畫

劃分法規及範圍依循方向

全校導入資訊安全管理制度規畫

劃分法規及範圍依循方向

全校每二年辦理一次內稽

資安推動小組協助行政、教學單位資通系統內部稽核分批分年重點抽查

計畫案應自行編列預算辦理內稽，由主管機關安排第二方稽核事宜

完整規畫>全面宣導>教育訓練>向下落實>重點稽核>管理審查

配合法規進行調整，循序漸進化繁為簡，依人力及資源調整

資通安全法應辦事項

資安法規及學校政策

C級公務機關應辦事項	• 主管機關每二年核定資通安全責任等級，教育部評定本校為C級(分級辦法附表五)
資通系統防護需求分級原則	• 防護需求等級分為普.中.高，構面分為機密性.完整性.可用性.法律遵循性(辦法附表九)
資通系統防護基準	• 對應防護需求等級普、中、高，需執行相對的控制措施(分級辦法附表十)
本校資通安全維護計畫	• 公務機關訂定、修正及實施資通安全維護計畫，主管機關對公務機關實施情形稽核
本校委外SOP流程	• 行政單位針對委外系統採購或維護前依本作業流程項目先行檢核，送計中協助審核

資通安全法應辦事項

C級之公務機關應辦事項-管理面

辦理項目	辦理內容
資通系統分級及防護基準	**每年至少檢視一次**資通系統分級妥適性，並應於初次受核定或**等級變更後之二年內，完成附表十之控制措施**。
資訊安全管理系統之導入	核定或等級變更後之二年內，**全部核心資通系統**導入CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等標準，或經主管機關認可之標準，並持續維持導入。
資通安全專責人員	初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
內部資通安全稽核	**每二年辦理一次**。
業務持續運作演練	**全部核心資通系統**每二年辦理一次。

資通安全法應辦事項

C級之公務機關應辦事項-技術面

辦理項目	辦理項目細項	辦理內容
安全性檢測	弱點掃描、 滲透測試	全部核心資通系統每2年辦理1次
資通安全健診	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視	每二年辦理一次。
資通安全弱點通報機制		110年前已受核定者，應於修正施行後二年內，**完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。**
資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
	網路防火牆	
	具有郵件伺服器者，應備電子郵件過濾機制	

資通安全法應辦事項

C級之公務機關應辦事項-認知與訓練

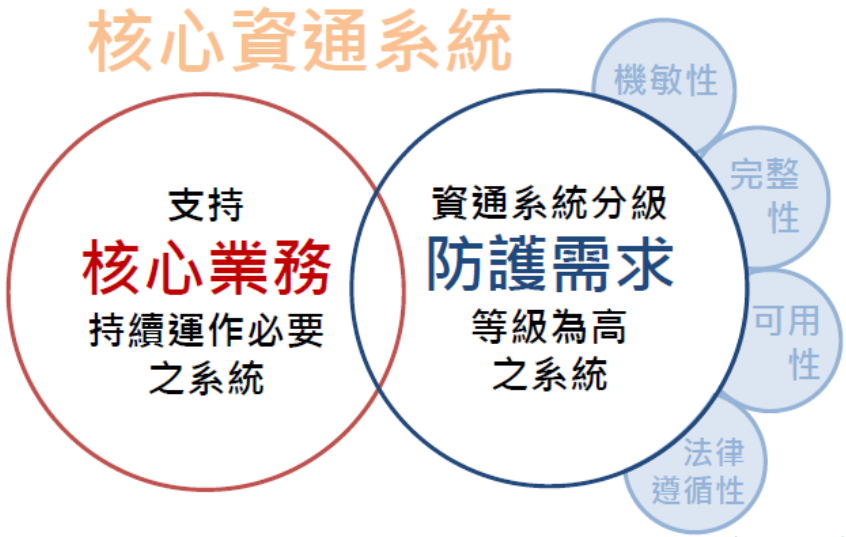
辦理項目	辦理項目細項	辦理內容
資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
	資通安全專職人員以外之資訊人員	每人**每二年**至少接受**三小時**以上之**資通安全專業課程**訓練或**資通安全職能訓練**，且**每年接受三小時以上之資通安全通識教育訓練**。
	一般使用者及主管	**每人每年接受三小時以上之資通安全通識教育訓練。**
資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。

★e等公務園>機關業務知能訓練>資訊安全與管理>資通安全>(通、專、職)

資通安全法應辦事項

核心資通系統

- 指支持**核心業務**持續運作必要之系統，或依資通安全責任等級分級辦法附表九**資通系統防護需求分級原則**之規定，判定其**防護需求**等級為**高**者。



-資通安全管理法施行細則第7條第2項-

資通安全法應辦事項

資通系統防護需求分級原則(附表9)

<table>
<tr><th>防護需求等級
構面</th><th>高</th><th>中</th><th>普</th></tr>
<tr><td rowspan="2">機密性</td><td colspan="3">發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生的影響</td></tr>
<tr><td>非常嚴重或災難性</td><td>嚴重</td><td>有限</td></tr>
<tr><td rowspan="2">完整性</td><td colspan="3">發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生的影響</td></tr>
<tr><td>非常嚴重或災難性</td><td>嚴重</td><td>有限</td></tr>
<tr><td rowspan="2">可用性</td><td colspan="3">發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生的影響</td></tr>
<tr><td>非常嚴重或災難性</td><td>嚴重</td><td>有限</td></tr>
<tr><td rowspan="2">法律遵循性</td><td colspan="2">如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性</td><td rowspan="2">其他資通系統設置或運 作於法令有相關規範之 情形。</td></tr>
<tr><td>並使機關所屬人員負刑事責任</td><td>並使機關或其所屬人員受行政罰、懲戒或懲處</td></tr>
</table>

★資通系統之防護需求等級，以任一構面之防護需求等級之最高者定之

資通安全法應辦事項

系統管理者及資安推動小組

資通系統防護基準	• 防護等級以上盡力規範
降低風險	• 督導委外廠商、系統向上集中
善盡職責	• 參與→宣導→彙整→陳核→提報
謹守法規	• 公務機關所屬人員資通安全事項獎懲辦法

資通安全維護計畫

相關重點1

資通安全目標

- 核心資通系統可用率達98.0%以上。(((每月總時數-預告時數-非預期時數)/(每月總時數-預告時數))*100%)
- 第二級資安事件發生次數小於1次。
- 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
- 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於10%及6%。

資通安全維護計畫

相關重點2

線上環境作業系統與資料庫系統之所有帳號皆應套用密碼政策。密碼政策如下所列：

- 使用者應變更初始或預設密碼。
- 密碼長度不可少於8個字元。
- 密碼應具備複雜性，如大小寫英文字母、數字或符號構成。
- 應至少每90天變更乙次，最短使用期限為1天。
- 密碼不可與前3組重覆。
- 密碼驗證失敗達3次後，至少15分鐘內不允許該帳號繼續嘗試登入。

資通安全維護計畫

相關重點6

應用程式或服務所使用之帳密依「國立臺北科技大學計算機與網路中心電腦帳號管理要點」，例如校園入口網站。

- 與前述密碼原則僅一項不同處為「密碼最長使用期限為180天，最短使用期限為1天。」

個人電腦應設定30分鐘後自行啟動螢幕保護程式(須輸入密碼)或自行登出。人員離開座位前，應登出個人電腦或鎖定螢幕。

資通安全維護計畫

相關重點3

資通安全教育訓練要求

- 資通安全專職人員每年至少1名人員接受12小時以上之資通安全專業課程訓練或資通安全職能訓練。
- 資訊人員(含系統管理者)每人每2年至少接受3小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受3小時以上資通安全通識教育訓練。
- 本校之一般使用者與主管，每人每年接受3小時以上之一般資通安全通識教育訓練。

資通安全維護計畫

相關重點4

資通安全教育訓練要求

- 「資通安全通識教育訓練」係指資通安全相關之通識性概念課程，或機關內部資通安全管理規定之宣導課程。
  - 公務人員終身學習入口網站之資通安全(通識) 代碼522
- 資通安全專業課程訓練係指可對應資安職能訓練發展藍圖中策略面、管理面、技術面之課程為原則，其相關時數，可透過以下方式取得：

  (一)參加技服中心舉辦之政府資通安全防護巡迴研討會，或所開設之資通安全策略、管理、技術相關課程。

  (二)參加資通安全專業證照清單上所列之訓練課程。

  (三)參加國內外之公私營訓練機構所開設或受委託辦理之資通安全策略、管理或技術訓練課程。

資通安全維護計畫

相關重點5

資通安全教育訓練要求

- 前述第 3 種辦理之訓練機構以下列型態為限：
- 1、公私立大專校院。
- 2、依法設立 2 年以上之職業訓練機構。
- 3、依法設立 2 年以上之短期補習班。
- 4、依法設立 2 年以上之學術研究機構或財團法人，其設立章程宗旨與人才培訓相關，且有辦理人才培訓業務。
- 公務人員終身學習入口網站之資通安全(專業、職能)代碼 523

資通安全維護計畫

相關重點6

其他遵循細節請依資通安全維護計畫正式公告，請參閱校園入口網站雲端資料夾。

資通系統與服務資產盤點

本次配合填報事項1

依據「資通安全管理法」第12條及「資通安全責任等級分級辦法」第11條規定辦理。(教育部轉行政院來函)

填寫附表3機關資通系統與服務資產清冊填報注意事項如下：

- Q:被委辦的系統是否進行盤點？(如教育部、國教署及其他委託開發之系統)
- A:全部盤點於清冊，並列出F欄與G欄載明主管機關。

請資安推動小組協助各單位彙整後陳核主管，於4/21(一)前上傳「資訊安全管理制度專區」網站

資通系統與服務資產盤點

本次配合填報事項2

C欄「系統屬性」

- 行政類： 指機關內部輔助單位之業務（如：人事、薪資等），惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別
- 業務類：指機關內部業務單位之業務（如：教學、研究等）

資通系統與服務資產盤點

本次配合填報事項3

L欄「機敏資訊」定義？

- 像是個資、公文機密文件或機關自定義之機敏感資料。

M欄「機敏資訊以非明文方式儲存」？

- 相關資訊儲存動作對資料庫已正規畫的資料也算非明文(由不同資料表組成)、去識別化、雜湊亂碼等就是非明文。
- 對系統而言的認定，資料庫也是其一環，所以儲存進資料庫後的資料是否存在非明文也應該考量。

資通系統與服務資產盤點

本次配合填報事項4

O欄「是否與民生權益相關」？

- 民生系統的定義以是否影響全國性資料的系統，如全國聯招等。

P欄「防護需求等級」？

- 請依資通安全責任等級分級辦法，附表九資通系統防護需求分級原則進行，可參閱本校委外資訊系統建置需求標準作業流程S1資訊系統安全等級評估表進行評估與簽核

資通系統與服務資產盤點

本次配合填報事項5

W欄「是否符合防護基準」？

- 請依資通安全責任等級分級辦法，附表十資通系統防護基準

Y欄「系統是否對外」？

- 係指以網際網路即可連線檢視或使用之系統(校外可直接連線使用之系統)，需透過VPN使用之系統則不算對外。

AB欄「弱密碼」？

- 密碼應具備複雜性，如大小寫英文字母、數字或符號構成。

資通系統與服務資產盤點

未來配合事項

辦理本校資通系統自我檢核說明會

- 依據本校資通安全維護計畫與教育部稽核項目檢核表(控制措施)，進行全校自我檢核說明會。

進行資訊資產盤點、風險評鑑及自我檢核作業

- 針對資訊資產盤點及機密性、完整性、可用性(CIA)等風險評鑑。
- 參考教育部稽核項目檢核表(控制措施)，辦理資通系統自我檢核，經單位主管核章後送計中彙整。

資通系統與服務資產盤點

未來配合事項

內部資通安全稽核

- 稽核範圍應包含全校各單位，就資通系統（保有個人資料）風險高低、教學單位特性評估訂定推動先後順序分階段規劃辦理。

持續精進及績效管理

- 將全校實施情形、內稽結果及推動成果，提報「資通安全推動委員會」進行管理審查及後續追蹤。

資通安全政策與控管

資安政策強化說明

行政面

- 本校資安責任等級為C，行政面上以C級為主

實務面

- 因本校校內具有數個教育部核心系統，其責任等級A與B，實務面上政策導入將高於C級，藉以防護主管機關重要核心系統

最大化

- 依據教育部資科司補助要求，補助本校之A、B級防護設備，應拓展協防校內相關系統，以達補助設備項目之活用最大化

資通安全政策與控管

資安法規政策

各單位電腦重灌作業

- 為配合資通安全管理法，本中心將於今年導入GCB+VANS控管機制，相關衝擊請詳閱

Google、Gmail與各雲端不得傳遞公務資料

- 有關機敏感資料(含個資)非經主管書面同意不得透過雲端或第三方傳送一事，請詳閱

法規導入無法即時改善時

- 為確實配合法遵，單位系統如受防火牆控管時，若有業務衝擊無法即時改善者，請詳閱

資通安全政策與控管

校園網路連線政策及架構調整

網路管理政策調整說明

- 臺北科技大學校園網路使用規範

行政單位：網路防護基準提升

- 配合教育部要求提升行政單位網路防護措施，請詳閱說明與配套

學術單位：網路連入阻擋政策

- 有關本校網路連入政策變動說明，請務必詳讀以避免影響自身權益

私接如中華電信線路中斷與例外說明

- (資安法) 針對校內私接一般電信網路將於108年7月進行中斷之說明

資安政策與控管

資通訊系統控管作業

資通訊產品風險控制措施

- 為強化本校資通訊產品(含軟體、硬體、服務及物聯網設備)風險控制，請詳閱相關措施說明

物聯網設備使用原則與注意事項

- 全校物聯網設備資通安全改善事項說明

委外廠商與連入相關措施

- 針對資通訊產品委外廠商強化控管作業說明
- 委外系統維運人員VPN帳號申請/清查

資通安全政策與控管

資訊系統向上集中與上線流程

系統建置前

- 國立臺北科技大學雲端虛擬主機租用管理要點

  C4-1雲端虛擬主機租用申請表

  C4-2雲端虛擬主機資安服務租用申請表

  委外建置：委外資訊系統建置需求標準作業流程說明

系統建置時

- C3-2防火牆服務埠新增異動申請表

  委外建置:委外系統維運人員VPN帳號申請/清查

系統上線前

- C3-1防火牆申請前置作業-主機網站弱點掃描申請表

  C3-2防火牆服務埠新增異動申請表

資通安全政策與控管

中國品牌資通訊設備採購說明

有關本校採購或使用資通訊產品(軟體、硬體及服務)為中國大陸品牌或製品注意事項

有關行政院要求110年完成汰換大陸廠牌資通訊產品一事，請詳閱

資通安全政策與控管

資安通報流程

如發現系統漏洞或疑似遭侵害破壞、資料洩漏等狀況，
請立即通報：計網中心網路作業組陳志豪
(3226 joey@ntut.edu.tw)

系統如收到外部(行政院、教育部、調查局)通報或來函，
將依資通安全通報應變作業程序先執行斷網，
避免災害擴大

感謝您的參與推動
敬祝平安順利

CNC 計算機與網路中心
COMPUTER & NETWORK CENTER