文件名稱：資通安全手冊 文件編號：NPUST-ISO-1-001 制定單位：電子計算機中心 申請類別：☐ 制定　☑修訂　□廢止 保密等級：☐ 密　☑一般	文件發行章

NO	修訂日期	頁次	版本	修 訂 內 容 摘 要
1	98.05.01	16	1	新制定
2	99.06.15	16	2	1.修訂 5.1.4 員工人數，由 15 人修正為 21 人。 2.針對 5.7 資通安全管理系統文件展開表，修正負責組別，帳號及密碼控制管理程序(18)，由負責單位由網路組修改為系統組負責。
3	100.01.03	16	3	因中心人員異動頻繁，所以刪除 1. 5.1.4 員工人數記載。 2. 5.7 資通安全管理系統文件展開表內之負責單位。
4	105.05.20	12	4	修改全部 5.作業內容
5	110.04.09	12	5	修改全部 5.4 本校或電子計算機中心架構
6	113.01.31	14	6	修訂內容為 ISO/IEC 27001:2022 年版

擬稿人	審查	核准
		西元：　2024 年　01 月　31　日

國立屏東科技大學

1.目的：確保本校或電子計算機中心資通安全管理系統執行之有效性，使資通安全政策、資通安全目標與資通安全各流程清楚展現與說明。

2.範圍：資通安全管理系統所涵蓋之資通設備儲放環境及辦公室所有流程與單位均適用。

3.權責：

3.1 資通安全手冊核准：資安長

3.2 資通安全手冊修訂審核：電子計算機中心單位主管

3.3 資通安全手冊制訂與修改：電子計算機中心

3.4 資通安全手冊作廢：電子計算機中心

4.名詞解釋：

為文件有效運作目的之標準用語，適用 ISO/IEC 27001 所明訂的用語釋義。

5.作業內容

5.1 本校簡介

5.1.1 本校名稱：國立屏東科技大學

5.1.2 本校地址：91201 屏東縣內埔鄉老埤村學府路 1 號

5.1.3 連絡電話：(08)7703202

5.1.4 傳真號碼：(08)7740165

5.1.4 員工人數：　人

5.2 範圍：

本手冊之內容與規定事項均適用於本校各單位、電子計算機中心及各單位辦公室所有服務(沒有排除任何適用性聲明控制措施)，從資通設備儲放環境之學生資料後台管理、網路資源服務、網路線上教學系統、提供資通系統開發及辦公室資通安全管理，均依循 ISO/IEC 27001:2022 年版之資通安全管理系統之標準要求執行。

5.3 資通安全政策：

5.3.1 國立屏東科技大學及電子計算機中心(以下簡稱本校或電子計算機中心)為強化資通安全管理、增進同仁對資通安全之認知，並確保資料、系統、設備與網路安全，特訂定本政策。

5.3.2 為統籌資通安全管理等事項之協調及推動，成立資通安全管理小組，該小組之幕僚作業由電子計算機中心負責。

5.3.3 依下列分工原則，配賦有關單位及人員權責：

5.3.3.1 資通安全管理政策、計畫及規範之研議、建置及評估等事項，由本校或電子計算機中心負責辦理。

5.3.3.2 資料及資通系統之安全需求研議、管理及保護等事項，由本校或電子計算機中心各

業務單位負責辦理。

5.3.3.3 資訊機密維護及安全稽核等事項,由本校或電子計算機中心會同相關單位負責辦理。

5.3.4 **本校或電子計算機中心資通安全政策**之範圍如下，有關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效：

5.3.4.1 資通安全政策適用性。

5.3.4.2 資通安全暨利害關係人管理。

5.3.4.3 存取控制管理。

5.3.4.4 供應商管理。

5.3.4.5 資通安全事件通報管理。

5.3.4.6 營運持續管理。

5.3.4.7 法規遵循性管理。

5.3.4.8 人力資源管理。

5.3.4.9 實體及環境安全管理。

5.3.4.10 網路安全管理。

5.3.4.11 資料備份管理。

5.3.4.12 密碼控制管理。

5.3.4.13 資通系統及資訊資產管理

5.3.4.14 系統發展及維護安全管理

5.3.4.15 資通安全稽核管理

資安長：_____

5.3.5 本校或電子計算機中心政策至少每年會在管理審查會議中檢討一次適切性，以反映法令、技術及業務等最新發展現況，確保資通安全實務作業之有效性。

5.3.6 本校資通安全管理小組暨利害關係人管理：

5.3.6.1 資通安全管理小組由行政副校長擔任資安長，電子計算機中心主任為執行秘書、置委員若干人，透過小組的運作，來強化資通安全管理的橫向連結與溝通，進而優化本校資通安全管理的能力。

5.3.6.2 本校利害關係人包含學生、學校職員、學校老師、本校同仁、軟/硬體廠商、主管機關，每年透過本校同仁與利害關係人互動狀況，來評估需求，進而協助本校的資通安全管理，可以更符合利害關係人的期望。

5.3.7 存取控制管理

5.3.7.1 系統存取應依人員職務或角色，訂定相關權限。

5.3.7.2 離(調)職人員，應立即取消各項資通資源之所有權限，並列入離(調)職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

5.3.7.3 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過六個月為原則。

5.3.7.4 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，課其相關安全保密責任。

5.3.7.5 建立資通安全稽核制度，定期或不定期進行資通安全稽核作業。

5.3.7.6 讓資訊刪除、資料遮蔽、資料洩露預防、儲存紀錄、特殊權限公用程式之使用得到有效管理。

5.3.8 供應商管理

5.3.8.1 透過採購流程評選後，可採用之供應商，會簽署合約或保密協議，才能進行本校資通軟體及硬體的服務。

5.3.8.2 供應商服務人員的異動，也應通知本校知悉，經本校同意後，才可進行資通服務作業。

5.3.8.3 供應商維修服務的門禁及系統權限管理，均應遵守本校規定。

5.3.8.4 建立 ICT 供應鏈中之資通安全管理。

5.3.9 資通安全事件通報管理

5.3.9.1 各項資通安全活動或服務流程之意外與緊急事故鑑定。

5.3.9.2 資通安全緊急事故通報。

5.3.9.3 建立資通安全事件緊急處理機制，在發生資通安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，必要時，並聯繫檢警調單位協助偵查。

5.3.9.4 資通安全意外與緊急事故應變之測試與訓練。

5.3.9.5 持續監控、管理及改善資通安全。

5.3.10 營運持續管理

5.3.10.1 依風險評估高風險項目、營運衝擊分析、資通安全策略、日常營運持續需求或資通安全事故等持續營運需求來源，訂定營運持續運作計畫。

5.3.10.2 營運持續包含資通安全政策、處理流程、處理人員及 ICT 架構。

5.3.10.3 針對營運持續 ICT 架構訂定緊急應變、回復作業程序及降低營運持續風險計畫。

5.3.10.4 並定期演練及調整更新營運持續計畫，讓營運持續從困難中迅速恢復的能力提升。

5.3.11 法規遵循性管理

5.3.11.1 每年應定期蒐集資通安全相關法規。

5.3.11.2 與本校有關資通安全相關法規應上網公告。

5.3.11.3 強化對智慧財產權、隱私及個人識別資訊 PII 保護。

5.3.11.4 針對不符合資通安全法規條款，應通知相關同仁處理。

5.3.12 人力資源管理

5.3.12.1 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

5.3.12.2 針對管理、業務及資訊等不同工作類別之需求，定期辦理資通安全教育訓練及宣導，建立同仁資通安全認知，提升資通安全水準。

5.3.12.3 建立適切的資通安全獎懲措施。

5.3.13 實體及環境安全管理

5.3.13.1 須採取適當的門禁管制，以防止對資通資產不當存取或造成損害，對外提供服務之主機系統與網路設備及對內服務之網路伺服器均須放置於有適切門禁管制之場所。

5.3.13.2 進入辦公場域或管制區域，非本校之人員，須由本校人員在場陪同下，方可進入本

校工作區域。

5.3.13.3 本校所有人員須遵守電腦螢幕保護及桌面淨空原則，存放機密資料之抽屜及櫥櫃之保管人在離開辦公場所時須將其上鎖。

5.3.13.4 實體安全監視、場所外資產之安全、儲存媒體、支援之公用服務、佈纜安全、設備維護、設備汰除或重新使用之保全，都在可控的作業環境下運作。

5.3.14 網路安全管理

5.3.14.1 架設硬體防火牆、入侵偵測系統及弱點掃描等，來阻隔來自網際網路未知的入侵攻擊，以保護網站資料的安全及完整性。

5.3.14.2 安裝網路監控系統，監控網路流量，針對異常之狀況，發揮即時控管的功效。

5.3.14.3 架設防毒系統，以防止病毒之入侵，提供使用者一個安全的網路環境。

5.3.14.4 定期與不定期備份網站資料，當不可預期的災害發生後，以期能在最短時間內使系統復原，繼續上線服務廣大的使用者。

5.3.14.5 定期或不定期更新相關作業系統或應用程式廠商所發布的相關更新程式，以確保系統對於任何攻擊的防禦性，使遭受攻擊的機率降到最低。

5.3.14.6 確保使用雲端服務之資通安全及啟動有限的遠端連線功能，減少資通安全風險。

5.3.15 資料備份管理

5.3.15.1 應針對重要資通與軟體進行定期備份作業，以便在發生系統失效或資料錯誤時，可迅速地回復正常作業，及還原正確資料。

5.3.15.2 各項系統設定檔、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期。

5.3.15.3 備份管理人員應注意備份系統運作是否正常，並不定期抽查系統之鐘訊同步狀態與運作紀錄。

5.3.16 密碼控制管理

5.3.16.1 透過帳號及密碼管理複雜度及長度的管制，再配合系統存取權限控制，來有效管理校整體系統密碼。

5.3.16.2 同仁應定期變更密碼，以避免密碼被不當使用。

5.3.17 資通系統及資訊資產管理

5.3.17.1 建立與資通系統有關的資通資產目錄，訂定資通資產的項目、擁有者及資通資產分類等。

5.3.17.2 已列入資通資產安全分類的資通及系統之輸出資料，應標示適當的保密等級以利使用者遵循。

5.3.17.3 核心系統所延伸的 ICT 設備，進行資通處理設施之多備源鑑別。

5.3.18 系統發展及維護安全管理

5.3.18.1 自行開發或委外發展系統，應在系統生命週期之初始階段，即將資通安全需求納入考量；系統之安全程式設計、維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、後門及電腦病毒等危害系統安全。

5.3.18.2 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

5.3.18.3 委託廠商建置及維護重要之軟硬體設施，應在本校相關人員監督及陪同。

5.3.19 資通安全稽核管理

5.3.19.1 建立全校性年度稽核計畫以符合 ISMS 與相關法令或法規之要求。

5.3.19.2 訓練合格稽核員，建立稽核查檢表格，執行稽核作業。

5.3.19.3 進行稽核檢討與改善，持續資通安全管理有效性。

5.3.19 本資通安全管理政策由資安長核可後實施，修正時亦同。

5.4 本校資通安全組織：

5.4.1 資通安全長

依資通安全法第 11 條之規定，本校資通安全管理會議訂定行政副校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

5.4.1.1 資通安全管理政策及目標之核定、核轉及督導。

5.4.1.2 資通安全責任之分配及協調。

5.4.1.3 資通安全資源分配。

5.4.1.4 資通安全防護措施之監督。

5.4.1.5 資通安全事件之檢討及監督。

5.4.1.6 資通安全相關規章與程序、制度文件核定。

5.4.1.7 資通安全管理年度工作計畫之核定

5.4.1.8 資通安全相關工作事項督導及績效管理。

5.4.1.9 其他資通安全事項之核定。

5.4.2 資通安全推動小組

5.4.2.1 組織

為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各業務部門主管/副主管以上之人員代表成立資通安全推動小組 ，其任務包括：

5.4.2.1.1 規劃及督導資通安全管理相關措施之執行。

5.4.2.1.2 協助訂定校內有關資通安全管理之稽核計畫及相關規範。

5.4.2.1.3 負責執行資通安全管理、狀況應變及事件處置。

5.4.2.1.4 督導資通安全教育訓練之實施與落實執行。

5.4.2.1.5 協助落實校內有關資通安全管理自我考核機制。

5.4.2.1.6 其它臨時交辦事項。

5.4.2.2 分工及職掌

依據「屏東科技大學資通安全會報組織架構(NPUST-ISO-1-004)」，本校之資通安全推動小組依下列分工進行責任分組：安全預防小組、危機處理小組及稽核小組，並依資通安全長之指示負責下列事項，本校資通安全推動小組分組人員名單及職掌應列冊，並適時更新之 ：

5.4.2.2.1 安全預防小組：

5.4.2.2.1.1 蒐集資通安全資訊

5.4.2.2.1.2 培訓資通安全技術
5.4.2.2.1.3 訂定系統安全等級
5.4.2.2.1.4 建置資通安全措施
5.4.2.2.1.5 執行資通安全監控
5.4.2.2.2 危機處理小組
5.4.2.2.2.1 規劃危機處理程序
5.4.2.2.2.2 查明安全事件原因
5.4.2.2.2.3 確定影響範圍並作損失評估
5.4.2.2.2.4 執行緊急應變措施
5.4.2.2.2.5 辦理安全事件
5.4.2.2.2.6 執行解決辦法
5.4.2.2.3 稽核小組
5.4.2.2.3.1 訂定相關之稽核
5.4.2.2.3.2 計畫或作業程序
5.4.2.2.3.3 內部稽核作業

5.5 資通安全手冊制(修)訂、廢止、分發及管制規定：

5.5.1 資通安全手冊之制(修)訂、廢止流程依照「資通安全文件與紀錄管理程序」規定辦理。
5.5.1.1 制(修)訂、廢止提案：電子計算機中心。
5.5.1.2 制(修)訂、廢止審查：電子計算機中心。
5.5.1.3 制(修)訂、廢止核准：資安長。

5.5.2 資通安全手冊之分發及管制規定流程依照「資通安全文件與紀錄管理程序」規定辦理。
5.5.2.1 資通安全手冊分發由電子計算機中心文件管制人員執行，可行時，應辦理回收。
5.5.2.2 電子計算機中心文件管制人員依核准數量分發並造冊列管。
5.5.2.3 本手冊不得任意影印，若因服務或宣導資通安全需求，需由資安長核准發送。

5.6 資通安全管理系統文件展開表：

項目	文件編號	系統文件名稱	負責單位
0	NPUST-ISO-1-001	資通安全手冊	電子計算機中心
1	NPUST-ISO-2-001	資通安全文件與紀錄管理程序	電子計算機中心
2	NPUST-ISO-2-002	資通安全管理審查程序	電子計算機中心
3	NPUST-ISO-2-003	資通安全稽核程序	電子計算機中心
4	NPUST-ISO-2-004	資通安全矯正與預防措施處理程序	電子計算機中心
5	NPUST-ISO-2-005	資通系統及資訊資產風險評鑑管理程序	電子計算機中心
6	NPUST-ISO-2-006	適用性聲明管理程序	電子計算機中心
7	NPUST-ISO-2-007	資通系統及資訊資產管理程序	電子計算機中心
8	NPUST-ISO-2-008	資通安全組織暨利害關係人管理程序	電子計算機中心
9	NPUST-ISO-2-009	人力資源管理程序	電子計算機中心

10	NPUST-ISO-2-010	實體與環境安全管理程序	電子計算機中心
11	NPUST-ISO-2-011	網路安全管理程序	電子計算機中心
12	NPUST-ISO-2-012	存取控制管理程序	電子計算機中心
13	NPUST-ISO-2-013	營運持續暨資通安全事件通報管理程序	電子計算機中心
14	NPUST-ISO-2-014	資料備份管理程序	電子計算機中心
15	NPUST-ISO-2-015	系統開發與維護管理程序	電子計算機中心
16	NPUST-ISO-2-016	無線網路安全管理程序	電子計算機中心
17	NPUST-ISO-2-017	電子傳輸管理程序	電子計算機中心
18	NPUST-ISO-2-018	帳號及密碼控制管理程序	電子計算機中心
19	NPUST-ISO-2-019	委外作業管理程序	電子計算機中心
20	NPUST-ISO-2-020	弱點作業管理程序	電子計算機中心
21	NPUST-ISO-2-021	法規評估管理程序	電子計算機中心
22	NPUST-ISO-2-022	辦公區域作業管理程序	電子計算機中心
23	NPUST-ISO-2-023	資通安全目標管理程序	電子計算機中心

5.7 資通安全管理系統敘述：

5.7.1 適用範圍

本校或電子計算機中心依組織全景，建立、施行、運作、維持及持續改進資通安全管理系統。

也參照資通安全管理系統需求，進行資通安全風險評鑑與處理。

本校或電子計算機中心參照 ISO/IEC 27001：2022 年版條文第 4 章至第 10 章所規定執行資通安全管理系統，且針對適用性聲明要求，沒有排除任何 A5~A8 的控制項目。

5.7.2 引用標準

CNS 27000 標準因本標準所引用，成為本標準的一部份。下列引用標準適用最新版本(包括任何修訂)。

CNS 27000 資訊技術-安全技術-資通安全管理系統-概觀與詞彙。

5.7.3 用語釋義

CNS 27000 所規定之用語及定義，適用 ISO/IEC 27001 所明訂的用語釋義。

5.7.4 組織全景

5.7.4.1 了解組織與其背景(參照「資通安全組織暨利害關係人管理程序」)

本校或電子計算機中心應決定與其資通安全管理相關，且會影響其資通安全管理系統預期結果的達成能力之外部與內部議題。

5.7.4.2 了解利害相關團體的需求與期望(參照「資通安全組織暨利害關係人管理程序」)

本校或電子計算機中心應決定：

5.7.4.2.1 與資通安全管理系統有關的利害相關團體(包含學生、學校職員、學校老

師、中心同仁、軟/硬體廠商、主管機關等)。

5.7.4.2.2 與資通安全有關的利害相關團體之關注議題。(如：網路穩定性、存取資料安全等)

5.7.4.2.3 利害相關團體之關注議題，會透過資通安全管理系統因應。

5.7.4.2.4 利害相關團體之關注議題可能包含法律及法規要求事項，以及契約義務。

5.7.4.3 決定資通安全管理系統的適用範圍(參照「資通安全手冊」)

本校或電子計算機中心應決定資通安全管理系統的界線與適用性，以建立其適用範圍。

當決定適用範圍時，應考量：

5.7.4.3.1 應考量 7.4.1 所提到的外部與內部問題。

5.7.4.3.2 及 7.4.2 所提到的要求事項。

5.7.4.3.3 在本校或電子計算機中心與其他利害相關人執行的活動之間，連結與互相信賴的關係。

5.7.4.3.4 此適用範圍應以文件化資訊取得。

5.7.4.4 資通安全管理系統(參照「資通安全手冊」)

5.7.4.4.1 本校或電子計算機中心依據本資通安全管理系統的要求，建立相關 SOP、實作、維持和持續改進資通安全管理系統。

5.7.4.4.2 包括所需流程及其互動。

5.7.5 領導能力

5.7.5.1 領導能力與承諾

高階管理者應藉由下列事項，展現對資通安全管理系統有關的承諾：

5.7.5.1.1 確保資通安全政策與目標已建立，並且和組織的策略方向相容。

5.7.5.1.2 確保資通安全管理系統的要求整合到組織的各項流程中。

5.7.5.1.3 確保資通安全管理系統所需的資源可取得。

5.7.5.1.4 傳達有效的資通安全管理的重要性，以符合資通安全管理系統要求事項之重要性。

5.7.5.1.5 確保資通安全管理系統達成預期結果。

5.7.5.1.6 指導與提供支援人員，讓人員對資通安全管理系統有效性做出貢獻。

5.7.5.1.7 推動持續改進。及

5.7.5.1.8 支援其他的相關管理角色，展現出在職責運用上的領導能力。

5.7.5.1.9 本標準所提及之”營運”，能廣義詮釋為本校或電子計算機中心存在目的具核心意義的活動。

5.7.5.2 政策(參照「資通安全手冊」)

5.7.5.2.1 高階管理者應建立一個資通安全政策：

5.7.5.2.1.1 適合本校或電子計算機中心資通安全管理目的。

5.7.5.2.1.2 提供訂立資通安全目標(參照 5.7.6.2)或提供設定資通安全目標的框架。

5.7.5.2.1.3 滿足有關資通安全之適用要求事項的承諾。

5.7.5.2.1.4 對資通安全管理系統持續改進的承諾。

5.7.5.2.2 資通安全政策應符合下列項目：

5.7.5.2.2.1 建立文件化資訊。

5.7.5.2.2.2 在組織內傳達。

5.7.5.2.2.3 適當時，可提供給利害相關團體。

5.7.5.3 組織角色、責任與權限(參照「資通安全組織暨利害關係人管理程序」、「人力資源管理程序」)

最高管理階層應確保有關資通安全的角色、責任與權限已在本校或電子計算機中心分派和傳達。

最高管理階層應分派下列責任與權限：

5.7.5.3.1 確保資通安全管理系統符合標準的要求事項。

5.7.5.3.2 向高階管理者報告資通安全管理系統的績效。

5.7.6.規劃

5.7.6.1 因應風險及機會的行動(參照「資通系統及資訊資產風險評鑑管理程序」)

5.7.6.1.1 一般要求

在規劃資通安全管理系統時，組織應考量 5.7.4.1 所提到的問題與 5.7.4.2 所提到的要求，並且決定因應的風險與機會，以達成下列事項：

5.7.6.1.1.1 確保資通安全管理系統可達成其預期成果。

5.7.6.1.1.2 預防或減少異常的影響。

5.7.6.1.1.3 持續達成改善。

組織應規劃下列事項：

5.7.6.1.1.4 因應風險與機會的對應措施；及

5.7.6.1.1.5 執行下列事項之方法：

5.7.6.1.1.5.1 將各項對應措施整合及實作到資通安全管理系統流程。

5.7.6.1.1.5.2 評估這些對應措施的有效性。

5.7.6.1.2 資通安全風險評鑑(參照「資通系統及資訊資產風險評鑑管理程序」)

組織應定義及應用資通安全風險評鑑的流程於下列事項中：

5.7.6.1.2.1 建立與維持資通安全風險的準則，包含：

5.7.6.1.2.1.1 風險的接受準則。

5.7.6.1.2.1.2 執行資通安全風險評鑑的準則。

5.7.6.1.2.2 確保可重複執行資通安全風險評鑑，並產出一致性、有效性和可比較性的結果。

5.7.6.1.2.3 識別資通安全風險

5.7.6.1.2.3.1 應用資通安全評鑑流程，以識別資通安全管理系統範圍內喪失資訊之機密性、完整性及可用性的相關聯的風險。

5.7.6.1.2.3.2 識別與風險有關的當責者。

5.7.6.1.2.4 分析資通安全風險

5.7.6.1.2.4.1 評估若在 5.7.6.1.2.3 中識別的風險發生時,可能導致的潛在後果。

5.7.6.1.2.4.2 評估 5.7.6.1.2.3.1 識別的風險,實際發生的可能性。

5.7.6.1.2.4.3 決定風險等級。

5.7.6.1.2.5 評估資通安全風險

5.7.6.1.2.5.1 比較被分析的風險,與在 5.7.6.1.2.1 建立的風險準則。

5.7.6.1.2.5.2 訂定已分析風險處理的優先順序。

5.7.6.1.2.5.3 組織應將資通安全風險評鑑流程的文件化資料，做好保存。

5.7.6.1.3 資通安全風險處理(參照「資通安全風險評鑑管理程序」、「適用性聲明管理程序」)

組織應定義與實施資通安全風險處理流程，以達成下列事項：

5.7.6.1.3.1 考量風險評鑑結果，選擇適當的資通安全風險處理選項。

5.7.6.1.3.2 選擇資通安全風險處理選項，決定所有必須實作的管制措施。

5.7.6.1.3.3 比較上述 5.7.6.1.3.2 決定的管制措施與附錄 A(參照「適用性聲明管理程序」)，應查證沒有忽略到必要的控制措施。

5.7.6.1.3.4 製作適用性的聲明，必要的控制(參照 5.7.6.1.3.2 與 5.7.6.1.3.3)、納入控制措施衡量理由、是否實作必要的控制措施、排除任何附錄 A 控制措施衡量理由。

5.7.6.1.3.5 制定資通安全風險處理計畫。

5.7.6.1.3.6 取得風險負責人員對資通安全風險處理計畫之核准，以及對接受殘留資通安全風險的接受條件。

5.7.6.1.3.7 組織應保存資通安全風險處理流程的文件化資訊。

5.7.6.2 資通安全目標與實現的規劃(參照「資通安全目標管理程序」)

組織應在各相關部門及層級，建立資通安全目標。

5.7.6.2.1 資通安全目標應滿足下列事項：

5.7.6.2.1.1 與資通安全政策一致。

5.7.6.2.1.2 可測量(如果可行時)。

5.7.6.2.1.3 考量適用的資通安全要求事項，以及風險評鑑與處理結果。

5.7.6.2.1.4 可監控。

5.7.6.2.1.5 在組織內已予溝通與瞭解。

5.7.6.2.1.6 適當時作更新。

5.7.6.2.1.7 以文件化資訊提供。

組織應保存資通安全目標的文件化資訊。

5.7.6.2.2 當規劃執行資通安全目標時，組織應決定：

5.7.6.2.2.1 要做什麼。

5.7.6.2.2.2 需要什麼資源。

5.7.6.2.2.3 誰要負責。

5.7.6.2.2.4 何時完成。

5.7.6.2.2.5 評估結果的方式。

5.7.6.3 變更之規劃

當組織決定對資通安全管理系統進行變更時，應以標準要求及「資通安全文件與紀錄管理程序」變更流程進行規劃。

5.7.7 支援

5.7.7.1 資源

組織應決定與提供用來建立、施行、維持和持續改進資通安全管理系統所需的資源。

5.7.7.2 人員能力(參照「人力資源管理程序」)

組織應：

5.7.7.2.1 決定於組織控制下，執行影響資通安全績效，工作人員必需的能力。

5.7.7.2.2 確保人員在有適當的教育、訓練或經驗基礎上，來勝任這份工作。

5.7.7.2.3 適用時，採取行動取得必要的能力，並評估採取的行動有效性。

5.7.7.2.4 保存適當的文件化資訊，做為勝任能力的證據。

5.7.7.3 認知(參照「人力資源管理程序」)

受組織管控下的工作人員應認知到：

5.7.7.3.1 資通安全政策。

5.7.7.3.2 對資通安全管理系統有效性之貢獻，包含改進資通安全績效的好處。

5.7.7.3.3 未遵循資通安全管理系統要求的後果。

5.7.7.4 溝通或傳達(參照「人力資源管理程序」、「委外作業管理程序」)

組織應決定與資通安全管理系統有關的內部與外部溝通之需求，包含：

5.7.7.4.1 要溝通或達傳的事項。

5.7.7.4.2 溝通或達傳時間。

5.7.7.4.3 和誰溝通或達傳。

5.7.7.4.4 溝通或達傳方式。

5.5.7.5 文件化資訊(參照「資通安全文件與紀錄管理程序」)

5.5.7.5.1 概述

組織的資通安全管理系統應包含：

5.5.7.5.1.1 本標準要求的文件化資訊。

5.5.7.5.1.2 由組織決定，資通安全管理系統有效性所必需的文件化資訊。

5.5.7.5.2 制定與更新

當制定與更新文件化資訊時，組織應確保適當的：

5.5.7.5.2.1 識別與描述(例如標題、日期、作者或參引號碼)。

5.5.7.5.2.2 格式(例如語言、軟體版本或圖表)與媒體(例如紙本、電子)。

5.5.7.5.2.3 適用性與充足性的審查與核准。

5.5.7.5.3 文件化資訊的管制

資通安全管理與本標準要求的文件化資訊應受管制以確保：

5.5.7.5.3.1 在需要的地點與時間可取得，並使用。

5.5.7.5.3.2 適當的維護(例如避喪失機密性、使用不當或喪失完整性)。

對於文件化資訊的控制，適用時，組織可闡明下列活動：

5.5.7.5.3.3 派送、存取、檢索與使用。

5.5.7.5.3.4 儲存與保存，包含可讀性保存。

5.5.7.5.3.5 變更控制（例如：版本控制）。

5.5.7.5.3.6 留存及到期處置。

於適切時，組織決定資通安全管理系統的計畫與運作所必需的外來文件，適當時應識別且進行管制文件化資訊。

5.5.8 運作

5.5.8.1 運作規劃與控制(參照資通設備管控區域與辦公室相關文件)

5.5.8.1.1 組織應規劃、實作及控制符合資通安全要求的流程，施行 7.5.6 處理風險與機會的對應措施的流程，包含建立準則及依準則實作流程的控制措施。

5.5.8.1.2 組織應提供文件化的資料，其程度須足以達成其流程已依規劃執行的信心。

5.5.8.1.3 組織應控制規劃的變更，並審查非預期變更可能帶來的後果，在必要時，採取措施以降低任何可能造成的負面效果。

5.5.8.1.4 組織應確保外包流程是受控制的。

5.5.8.2 資通安全風險評鑑(參照「資通系統及資訊資產風險評鑑管理程序」)

5.5.8.2.1 組織應在計劃執行期間內，如有發生或提出重大變時，請依 7.5.6.1.2.1 建立的準則，執行資通安全風險評鑑，。

5.5.8.2.2 組織應保存資通安全風險評鑑結果的文件化資訊。

5.5.8.3 資通安全風險處理(參照「資通系統及資訊資產風險評鑑管理程序」)

5.5.8.3.1 組織應執行資通安全風險處理的計畫。

5.5.8.3.2 組織應保存資通安全風險處理結果的文件化資訊。

5.5.9 績效評估

5.5.9.1 監督、量測、分析與評估(參照「資通安全稽核程序」、「資通安全目標管理程序」、「資通安全管理審查程序」)

組織應決定下列事項：

5.5.9.1.1 什麼需要監督與量測，包含資通安全流程與控制措施。

5.5.9.1.2 監督、量測、分析與評估的方法，用以確保有效的結果。所選擇的方法應可產生比較及可重製有效性的結果。

5.5.9.1.3 監督與量測應何時執行。

5.5.9.1.4 應由誰監督與量測。

5.5.9.1.5 監督與量測結果應何時分析與評估。

5.5.9.1.6 應由誰分析與評估這些結果。

5.5.9.1.7 組織應保存適當的文件化資訊，作為監督與量測結果的證據。

5.5.9.1.8 組織應評估資通安全績效及資通安全管理系統之有效性。

5.5.9.2 內部稽核(參照「資通安全稽核程序」)

5.5.9.2.1 一般要求

組織應在計劃期間執行內部稽核，以提供資訊確認資通安全管理系統是否：

5.5.9.2.1.1 是否符合下列事項：

5.5.9.2.1.1 組織本身有關資通安全管理系統的要求事項。

5.5.9.2.1.2 本標準的要求事項。

5.5.9.2.1.2 有效地實作與維持。

5.5.9.2.2 內部稽核計畫

組織應規劃、建立、施行與維護稽核計畫，包含了頻率、方法、責任、規劃要求與報告。

建立內部稽核計畫時，組織應考量所關切的流程的重要性，以及先前稽核的結果。

組織應採購下列作為：

5.5.9.2.2.1 定義稽核標準與適用範圍。

5.5.9.2.2.2 選擇稽核員並執行稽核，以確保稽核流程的客觀與公正。

5.5.9.2.2.3 確保稽核結果對相關管理階層報告。

5.5.9.2.2.4 保存文件化資訊，作為稽核計畫實作與稽核結果的證據。

5.5.9.3 管理階層審查(參照「資通安全管理審查程序」)

5.5.9.3.1 一般要求

高階管理者應定期審查組織的資通安全管理系統，以確保其持續的合宜性、適切性與有效性。

5.5.9.3.2 管理審查輸入

管理審查應包含的考慮事項：

5.5.9.3.2.1 先前管理審查決議的處理狀態。

5.5.9.3.2.2 有關資通安全管理系統的外部與內部議題之變更。

5.5.9.3.2.3 資通安全的績效回饋，包含下列趨勢。

5.5.9.3.2.3.1 不符合事項與矯正措施。

5.5.9.3.2.3.2 監督與量測結果。

5.5.9.3.2.3.3 稽核結果。

5.5.9.3.2.3.4 完成的資通安全目標。

5.5.9.3.2.4 利害相關人的回饋。

5.5.9.3.2.5 風險評鑑的結果與風險處理計畫狀態。

5.5.9.3.2.6 持續改進的機會。

5.5.9.3.3 管理審查結果

管理審查結果應包含和持續改進機會與資通安全管理系統需要變更的項目。

組織應保存文件化資訊，做為管理審查結果的證據。

5.5.10 改進(參照「資通安全矯正與預防措施處理程序」)

5.5.10.1 持續改善

組織應持續改善資通安全管理系統合宜性、適切性及有效性。

5.5.10.2 不符合事項與矯正措施

當不符合事項發生時，組織應：

5.5.10.2.1 對不符合事項作出回應：

5.5.10.2.1.1 採取行動，以控制並矯正。

5.5.10.2.1.2 處理其後果。

5.5.10.2.2 評估消除不符合事項的原因之措施需求，使其不再發生或是在別處發生，可經由：

5.5.10.1.2.1 審查不符合事項。

5.5.10.1.2.2 決定不符合事項的原因。

5.5.10.1.2.3 決定是否有類似的不符合事項存在，或有可能發生。

5.5.10.2.3 施行任何需要的措施。

5.5.10.2.4 審查採取的矯正措施之有效性。

5.5.10.2.5 必要時，對資通安全管理系統進行變更。

矯正措施應切合所遇到不符合事項之影響

矯正措施應具備文件化資訊，作為下列證據：

5.5.10.2.6 不符合事項的真因與採取任何後續改善措施。

5.5.10.2.7 所有矯正措施的結果記錄。