資訊安全手冊

1.目的

確保本處資訊安全管理系統執行之有效性，使資訊安全政策、資訊安全目標與資訊安全各流程清楚展現與說明。

2.範圍

資訊安全管理系統所涵蓋之所有流程與單位均適用。

3.權責

- 3.1資訊安全手冊核准：圖資長
- 3.2資訊安全手冊修訂審核：資訊服務組組長
- 3.3資訊安全手冊制訂與修改：資訊服務組組員
- 3.4資訊安全手冊作廢：資訊服務組組員

4.名詞解釋

無

5.作業內容

5.1 本中心簡介

- 5.1.1 學校名稱：中臺科技大學
- 5.1.2 學校地址：台中市北屯區廍子路666號
- 5.1.3 連絡電話：04-22391647轉6400
- 5.1.4 傳真號碼：04-22395970
- 5.1.4 員工人數：480人

5.2 範圍

本手冊之內容與規定事項均適用於本校圖書資訊處所有服務（本處排除電子商務及線上交易兩項服務在ISMS系統範圍內），從電腦機房之管理學生資料、網路資源服務、網路線上教學、提供資訊系統開發及辦公室資訊安全管理，均依循教育體系資通安全管理規劃之資訊安全管理之標準要求。

5.3 資訊安全政策

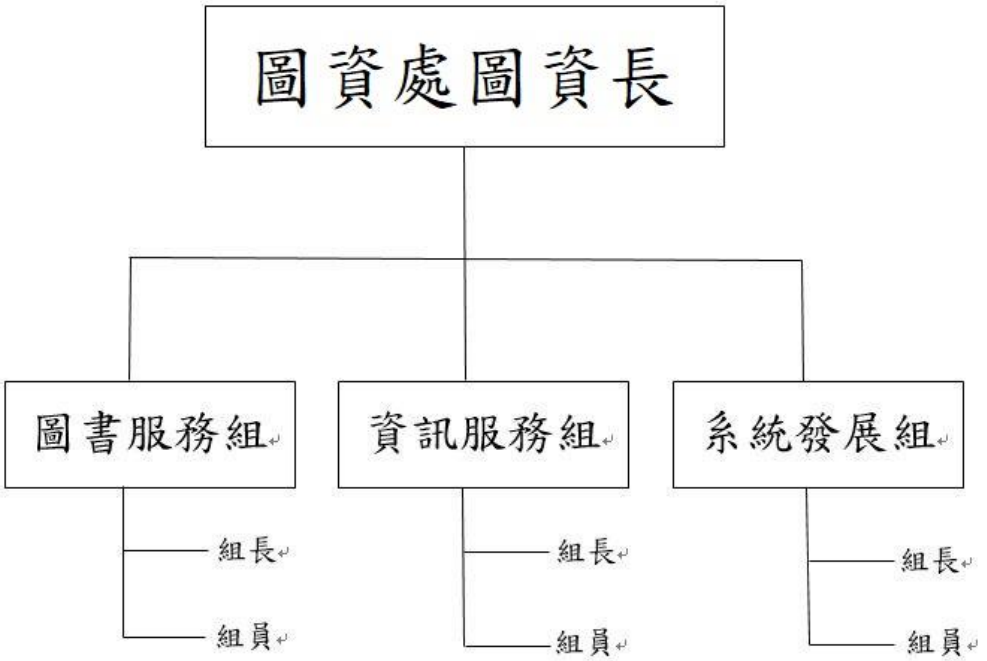
- 5.3.1 中臺科技大學圖書資訊處（以下簡稱本處）為強化資訊安全管理、增進同仁對資訊安全之認知，並確保資料、系統、設備與網路安全，特訂定本政策。
- 5.3.2 為統籌資訊安全管理等事項之協調及推動，成立資通安全小組，該小組之幕僚作業由系統發展組負責。
- 5.3.3 依下列分工原則，配賦有關單位及人員權責：
  - 5.3.3.1資訊安全管理政策、計畫及規範之研議、建置及評估等事項，由本處資訊服務組負責辦理。
  - 5.3.3.2資料及資訊系統之安全需求研議、管理及保護等事項，由本處各業務單位負責辦理。
  - 5.3.3.3資訊機密維護及安全稽核等事項，由本處資訊服務組會同相關單位負責辦理。
- 5.3.4本政策之範圍如下，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資訊安全本處人員管理及資訊安全教育訓練。
  - 5.3.4.2電腦系統安全管理。
  - 5.3.4.3網路安全管理。
  - 5.3.4.4系統存取控制。
  - 5.3.4.5系統發展及維護安全管理。
  - 5.3.4.6資訊資產安全管理。
  - 5.3.4.7實體及環境安全管理。
  - 5.3.4.8資訊安全事故管理。
  - 5.3.4.9業務永續運作計畫之規劃與管理。
  - 5.3.4.10資訊安全政策之適用性。
- 5.3.5人員管理及資訊安全教育訓練
  - 5.3.5.1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。
  - 5.3.5.2針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立同仁資訊安全認知，提升資訊安全水準。
- 5.3.6電腦系統安全管理
  - 5.3.6.1辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。
  - 5.3.6.2依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。
  - 5.3.6.3採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。
- 5.3.7網路安全管理
  - 5.3.7.1開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
  - 5.3.7.2與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。
  - 5.3.7.3利用網際網路及全球資訊網公布及流通資訊，應實施資料安全監控，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。
  - 5.3.7.4訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。

- 5.3.8系統存取控制
  - 5.3.8.1系統存取應依人員職務或角色，訂定相關權限。
  - 5.3.8.2離（調）職人員，應立即取消各項資訊資源之所有權限，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。
  - 5.3.8.3建立系統使用者註冊管理制度，加強使用者通行密碼管理。
  - 5.3.8.4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。
  - 5.3.8.5建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。
- 5.3.9系統發展及維護安全管理
  - 5.3.9.1自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、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、暗門及電腦病毒等危害系統安全。
  - 5.3.9.2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。
  - 5.3.9.3委託廠商建置及維護重要之軟硬體設施，應在本機關相關人員監督及陪同下始得為之。
- 5.3.10資訊資產安全管理
  - 5.3.10.1建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及資訊資產分類等。
  - 5.3.10.2已列入資訊資產安全分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。
- 5.3.11實體及環境安全管理：就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。
- 5.3.12資訊安全事故管理
  - 5.3.12.1各項資訊安全活動或服務過程之意外與緊急事故鑑定。
  - 5.3.12.2資訊安全緊急事故通報。
  - 5.3.12.3資訊安全意外與緊急事故應變之測試與訓練。
  - 5.3.12.4持續監控、管理及改善資訊安全。
- 5.3.13業務永續運作計畫之規劃與管理
  - 5.3.13.1 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。
  - 5.3.13.2建立資訊安全事件緊急處理機制，在發生資訊安全事件時，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。
- 5.3.14本政策應每學年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。
- 5.3.15評估時，應將審查輸入事項納入考量：
  - 5.3.15.1利害關係方的反應（例如中心及校內同仁、軟硬體廠商、學生、主管機關）
  - 5.3.15.2客觀第三者審查的結果（例如教育部稽核小組）
  - 5.3.15.3預防措施及改進對策狀態
  - 5.3.15.4前次評估的結果
  - 5.3.15.5資訊安全政策遵行及執行效果
  - 5.3.15.6影響組織管理資訊安全的改變，包括組織環境、營運事項、可用資源、合約、法規及技術等改變

- 5.3.15.7威脅、弱點的新趨勢。
- 5.3.15.8已回報的安全事件。
- 5.3.15.9相關權責單位提供的建議。（例如消防單位）

- 5.3.16審查產出結果可包括下列事項
  - 5.3.16.1組織資訊安全管理方法及程序的改善。
  - 5.3.16.2控制目標及安控措施的改善。
  - 5.3.16.3資源及責任分配的改進。
- 5.3.17資訊安全政策評估應納入管理審查會議或資訊安全相關會議中評估，並留下會議記錄。
- 5.3.18本資訊安全管理政策由圖資處圖資長核可後實施，修正時亦同。

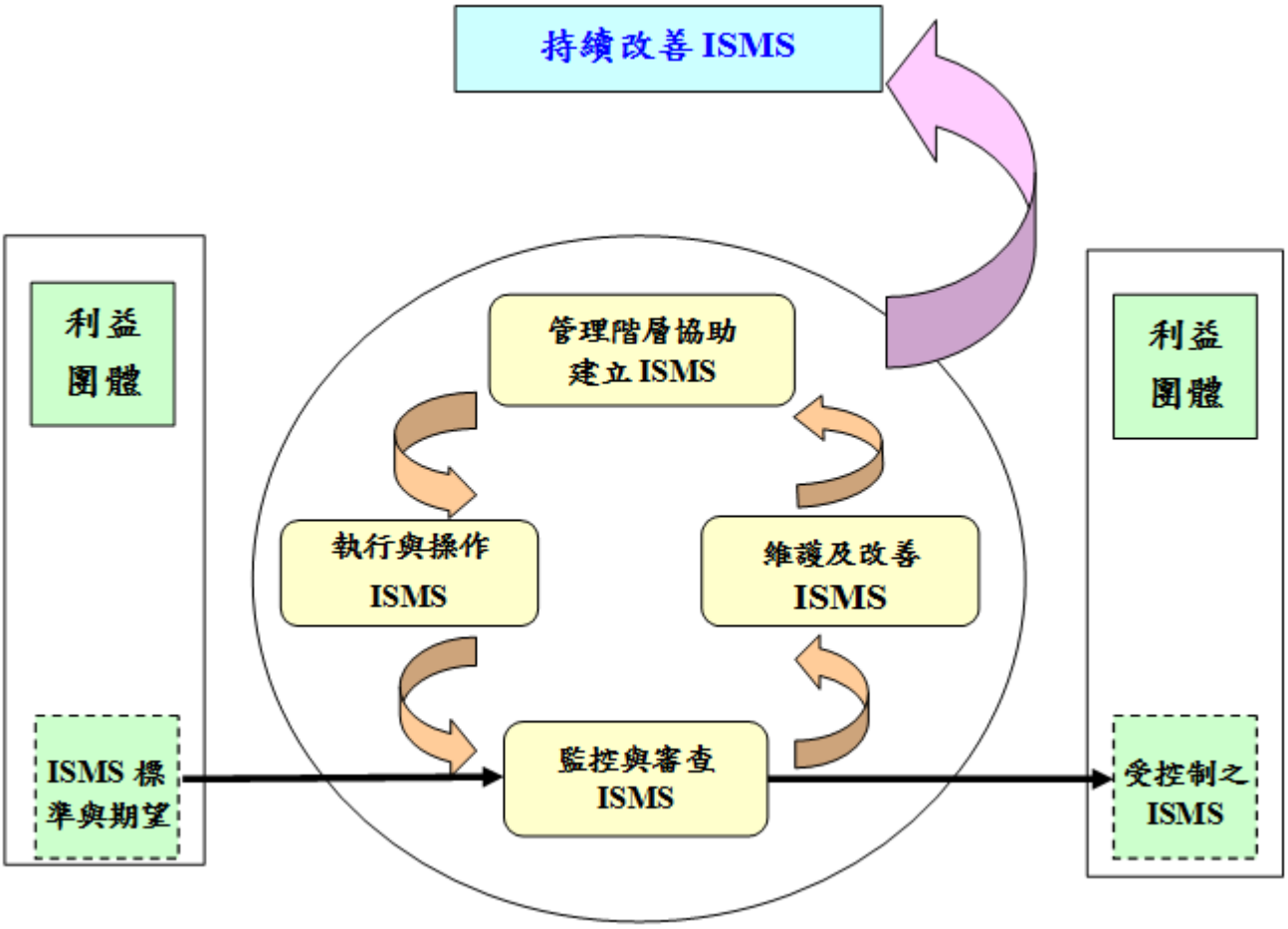
5.4 本處架構



5.5 資訊安全手冊制（修）訂、廢止、分發及管制規定

- 5.5.1資訊安全手冊之制（修）訂、廢止流程依照「資訊安全文件及資料管制程序」規定辦理。
  - 5.5.1.1制（修）訂、廢止提案：資訊服務組組員。
  - 5.5.1.2制（修）訂、廢止審查：資訊服務組組長
  - 5.5.1.3制（修）訂、廢止核准：圖資長。
- 5.5.2資訊安全手冊之分發及管制規定流程依照「資訊安全文件及資料管制程序」規定辦理。
  - 5.5.2.1資訊安全手冊分發由系統發展組文件管制人員執行，可行時，應辦理回收。
  - 5.5.2.2資訊服務組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，若因服務或宣導資訊安全需求，需由圖資長核准發送。

5.6 資訊安全系統模式



5.7 資訊安全管理系統文件展開表

項目	ISMS系統文件名稱	單位名稱	文件編碼
1	資訊安全手冊（資訊安全政策文件）	資訊服務組	CTU-LC-1-001

2	資訊安全文件及資料管制程序	資訊服務組	CTU-LC-2-001
3	資訊安全管理審查程序	資訊服務組	CTU-LC-2-002
4	資訊安全稽核管理程序	系統發展組	CTU-LC-2-003
5	資訊安全矯正與預防措施處理程序	資訊服務組	CTU-LC-2-004
6	資訊安全風險評鑑管理程序	系統發展組	CTU-LC-2-005
7	適用性聲明管理程序	系統發展組	CTU-LC-2-006
8	資安資產管理程序	系統發展組	CTU-LC-2-007
9	資訊安全組織管理程序	系統發展組	CTU-LC-2-008
10	人力資源管理程序	資訊服務組	CTU-LC-2-009
11	實體與環境安全管理程序	資訊服務組	CTU-LC-2-010
12	網路安全管理程序	資訊服務組	CTU-LC-2-011
13	存取控制管理程序	資訊服務組	CTU-LC-2-012
14	營運持續暨資安事件通報管理程序	系統發展組	CTU-LC-2-013
15	資料備份管理程序	系統發展組	CTU-LC-2-014
16	系統開發與維護管理程序	系統發展組	CTU-LC-2-015
17	電子傳輸管理程序	系統發展組	CTU-LC-2-016
18	帳號及密碼控制管理程序	系統發展組	CTU-LC-2-017
19	委外作業管理程序	資訊服務組	CTU-LC-2-018
20	弱點作業管理程序	系統發展組	CTU-LC-2-019
21	法規評估管理程序	資訊服務組	CTU-LC-2-020
22	辦公區域作業管理程序	資訊服務組	CTU-LC-2-021

6.文件異動表

文件版本	修訂日期	修改內容	修訂人員

<table>
<tr><td>V1.0</td><td>20200708</td><td>依據2020年度資安外稽建議修訂</td><td>呂令如</td></tr>
<tr><td></td><td>20200413</td><td>修改版本名稱，原本版名稱為CTU-LC-1-001-20190110，版本名稱修改為CTU-LC-1-001-20200210</td><td></td></tr>
<tr><td></td><td>20190116</td><td>修改版本名稱，原本版名稱為CTU-CC-1-001-20180330，版本名稱修改為CTU-LC-1-001-20190110</td><td></td></tr>
<tr><td></td><td>20190116</td><td>附件文件編號名稱修改，原版本CTU-CC-1-001，修改為CTU-LC-1-001，依序變更。</td><td></td></tr>
<tr><td></td><td>20181009</td><td>為配合組織再造，於107年7月與圖書館合併為圖書資訊中心，將原電子計算機中心單位名稱修正為圖書資訊中心，以及行政作業組、設備組修改為資訊服務組。</td><td></td></tr>
<tr><td></td><td>20180417</td><td>修改版本名稱，原本版名稱為CTU-CC-1-001-20170731，版本名稱修改為CTU-CC-1-001-20180330</td><td></td></tr>
<tr><td></td><td>20170718</td><td>修改版本名稱，原本版名稱為CTU-CC-1-001，版本名稱修改為CTU-CC-1-001-20170731</td><td></td></tr>
<tr><td></td><td>20160421</td><td>依據 2016/04/21 資通安全推動小組會議，修【5.12】
<table>
<tr><th>原程序書內容</th><th>修改後內容</th></tr>
<tr><td>5.12資訊資產報廢及再使用之管理

5.12.1資訊資產報廢應依總務處保管組之報廢或移轉程序辦理，以避免資訊資產遭誤用，申請報廢或移轉的資訊資產放置在中心庫房。

5.12.3含有儲存媒體的資訊設備（例如硬碟、電腦、磁帶、光碟或隨身碟等），應在報廢或移轉時進行檢查或將資料移除，以確保機密性或敏感性資料或版權軟體不當外流。</td><td>5.12資訊資產報廢及再使用之管理
5.12.1資訊資產報廢應依本校總務保管組之報廢程序辦理，以避免資產遭誤用，申請報廢資訊資產在中心庫房。
5.12.3含有儲存媒體的資訊設備（如硬碟、磁帶等），應在報廢或時進行檢查，報廢之硬碟、磁帶行消磁或實體破壞，拍照存檔確料已被完全銷毀。
5.12.4書面之機密文件應由碎紙機碎處理。
5.12.5報廢完畢，應更新資產清冊</td></tr>
</table></td><td></td></tr>
<tr><td></td><td>20160421</td><td>依據 2016/04/21 資通安全推動小組會議，修【5.3.14】</td><td></td></tr>
</table>

		原程序書內容 / 修改後內容 ○ 5.3.14本政策應每學期評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。 / 5.3.14本政策應每學年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。 說明□**為配合資通安全小組會議開會時程，特修訂本辦法**□ 決議：**照案通過。**	
	20140521	增加文件異動表	