臺中市立圖書館
資訊安全政策

文件編號：TCL-ISMS-1-01

版　　次：1.3

實施日期：113 年 8 月 26 日

機密等級：普通

文件制/修訂履歷

制/修訂 版次	制/修訂 日期	制/修訂 說明	修訂人	備 註
1.0	109/12/31	初版發行	林思宏	
1.1	110/8/19	本館資訊安全政策已包含民眾之個資保護，因此於「陸、參考文件」增加個人資料保護法及其施行細則	林思宏	
1.2	113/8/26	調整陸、參考文件項目名稱	林思宏	

目　　錄

壹、 目的

臺中市立圖書館(以下簡稱本館)資訊相關系統設備除提供內部人員作業處理外，亦透過資訊網路提供與民眾互動之溝通管道，其相關資訊系統作業應用之持續性運作，攸關本館形象及圖書業務推動，故訂定本資訊安全政策，作為資訊安全工作之指導方針，藉以降低資訊風險。

貳、 全景與宗旨

為辦理本館整體資訊發展規劃與推動，提升電腦處理效率，確保整體資通訊環境安全，本館規劃並提供所有轄區圖書館必要之網路基礎設施、核心資訊系統維運管理，以達成安全穩定且持續的資訊服務。

參、 適用範圍

臺中市立圖書館暨所屬分館及其資訊業務相關系統。

肆、 名詞定義

資訊機房：本館總館資訊機房。

伍、 作業內容

一、 政策聲明

（一）為確保本館資訊系統安全及建立可信賴之環境，相關使用者需經過正常程序之申請授權，方能閱讀或存取授權範圍內之機敏資訊，期間並保障資訊於處理、傳輸、儲存之過程中皆能正確無誤之使用，及避免資訊與系統被無意或惡意之竄改或變更，並確保智慧財產權及個人資料都能得到妥適的保護，避免不當的使用。

（二）對於個人資料之蒐集、處理及利用，將依相關法令之規定，僅就其特定目的之用，不會恣意對其他第三者揭露。

（三）以簡單且容易記憶並符合資訊安全管理為原則，訂定資訊安全政策聲明口號：

機密資料保護好，資安管理不可少，持續服務為首要，養成習慣沒煩惱。

二、 目標

參考資通安全政策，每年於管理審查會檢討及議定下年度之目標。

三、 作業流程執行與要求

（一）法律要求

遵守資通安全管理法第 10 條及其施行細則第 6 條規定，實施相關作業。

（二）高層支持：

推動資訊安全管理，必須由高層主管支持與參與。

（三）政策先行：

列出優先實施範圍，逐步推廣與落實。

（四）全體共識：

充分了解資訊安全管理制度的重要性，建立使命感。

（五）教育訓練：

適度資訊安全教育訓練，加強資訊安全管理觀念與技能。

（六）定期稽核：

透過稽核程序，發現資訊安全問題，提出改善建議，降低資安風險。

（七）適時改善：

發生資訊安全問題，即時研商對策，謀求改善機制，健全資訊安全管理制度。

（八）電腦病毒及惡意程式之防範：

1.事前預防及保護措施，防制及偵測電腦病毒及惡意程式侵入。

2.建立個人電腦使用規範及適當宣導，促使同仁正確認知電腦病毒及惡意程式的威脅並提升資訊安全警覺。

（九）重要資訊備份：

1. 正確及完整的重要備份資料，除存放在主要的作業場所外，應另外存放在不同的存放地點，以防止主要作業場所發生災害時可能帶來的傷害。

2.不定期測試並還原重要備份資料，以確保可用性與完整性。

3. 重要資料的保存時間，以及檔案的保存需求，由資料擁有者研提及控管。

（十）資訊交換：

1. 資訊資料交換應有妥善安全措施，以防止資料遭破壞、誤用或未經授權存取。

2.確保傳送過程中之實體媒體安全，不受未經授權的存取、誤用或毀損。

（十一）營運資訊保護：

使用辦公室電子設備（含影印機與傳真機），應注意資訊安全；產出機敏性文件時，應全程監看並於產出後妥善收存。

（十二）存取控制：

1. 訂定系統存取授權規定，並告知使用者相關之權限及責任。

2. 人員異動或職務調整時，應依系統存取授權規定，限期調整其權限。

3. 強化使用者通行密碼管理並定期更新。

4. 使用機敏性媒體應於離開座位時放置安全處所，避免未授權者取閱；電腦設施亦應設置螢幕保護機制並設定密碼保護，於離開操作後限定十分鐘內啟動鎖定。

5.除申請核准之事由外，不得攜帶可攜式之儲存裝置或個人筆記型電腦進入資訊機房，避免機敏資料外流。

6.辦公桌面、伺服器及個人電腦螢幕應保持淨空，不置放機敏性文件。

（十三）電腦網路服務的使用：

1. 被授權的電腦網路使用者，只能在授權範圍內存取電腦網路資源。

2. 訂定電子郵件使用規定，機敏性資料不宜以電子郵件方式傳送。

（十四）行動通訊及遠距工作：

未經授權禁止於總館與各所屬分館內使用行動式通訊設備及以遠端連線方式存取圖書館相關之資訊資產。

四、 溝通或傳達

為使本館之政策、需求及目標能有效地傳達到與業務相關之推廣，將利用媒體、影片、函文、會議、網頁、電子郵件及海報文宣等途徑，進行彼此關注議題討論及溝通，於必要時得邀請相關人員參與，並留存紀錄做為後續之依據，相關內容說明詳見「TCL-ISMS-1-01-T01 內外部關注方議題一覽表」。

五、 政策修訂

本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全管理實務作業之可行性及有效性。

陸、 參考文件

（一）資通安全管理法及相關子法

（二）ISO 27001:2022

（三）ISO 27002: 2022

（四）臺中市政府數位治理局 (TC-ISMS-1-01)資訊安全政策

（五）個人資料保護法及其施行細則

柒、 附件

一、 (TCL-ISMS-1-01-T01) 內外部關注方議題一覽表。