康寧學校財團法人康寧大學

資訊暨圖書中心

資訊安全政策

機密等級：一般

文件編號：ISMS-A-01

版　　次：2.0

發行日期：112.11.01

文件編號	ISMS-A-01	康寧學校財團法人康寧大學 資訊安全政策	保密區分	一般
版　　次	V 2.0		發布日期	112/11/01

修　訂　紀　錄				
版次	**修訂日期**	**修訂頁次**	**修訂者**	**修訂內容摘要**
1.0	108.07.15		資訊安全小組	初版
1.1	112.11.01	3	資訊安全小組	ISO 27001:2022 改版修訂

文件編號	ISMS-A-01	康寧學校財團法人康寧大學 資訊安全政策	保密區分	一般
版　　次	V 2.0		發布日期	112/11/01

目錄

文件編號	ISMS-A-01	康寧學校財團法人康寧大學 資訊安全政策	保密區分	一般
版　　次	V 2.0		發布日期	112/11/01

1. 目的

確保康寧大學資訊暨圖書中心（以下簡稱本中心）所屬之資訊資產的機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

2. 範圍

2.1 考量學校之核心資訊系統及相關利害關係者之需求及期望，基於保護資訊資產機密性、完整性、可用性為目標，將教務系統及資訊組辦公室、機房優先納入資訊安全管理範圍，展現本校負責之永續發展經營管理理念。

2.2 為避免因人為疏失、蓄意或天然災害等因素，導致資訊資產不當使用、洩漏、竄改、破壞等情事發生，對本中心帶來可能之風險及危害。依據組織面、人員面、實體面、技術面控制措施，具體執行資訊安全管理系統之管理事項如下：

2.2.1 資訊安全管理
2.2.2 資訊安全政策管理。
2.2.3 資訊安全組織管理。
2.2.4 人力資源安全管理。
2.2.5 資訊資產管理。
2.2.6 存取控制管理。
2.2.7 密碼管理。
2.2.8 實體與環境安全管理
2.2.9 作業安全管理。
2.2.10 通訊安全管理。
2.2.11 資訊系統獲取、開發及維護管理。
2.2.12 供應商關係管理。
2.2.13 資訊安全事件管理。
2.2.14 業務持續管理。
2.2.15 遵循性（適法性）管理。
2.2.16 資料安全管理。
2.2.17 變更與組態管理。
2.2.18 雲端服務安全管理。

3. 權責

3.1 資訊安全委員會

本校資訊發展暨安全管理階層決策組織。

3.2 資訊安全小組

本中心資訊組辦公室與資訊機房資訊安全管理制度規劃、建立、實施、維護、審查與持續改善，並將資訊安全相關議題於資訊安全委員會提報。

3.3 資訊組辦公室同仁、資訊系統服務使用者、委外人員

3.3.1 配合資訊安全管理制度作業。

3.3.2 遵守相關資訊安全管理制度規範。

4. 定義

4.1 資訊安全

保存資訊的機密性、完整性及可用性；亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。

5. 作業內容

5.1 原則

5.1.1 應考量相關法律規章及營運要求，進行資訊資產之資訊風險評估，確定資訊作業安全需求，建立「資訊安全管理程序」作業標準，採取適當資訊安全措施，確保資訊資產安全。

5.1.2 依人員角色及職能為基礎，建立評估或考核制度，並視實際需要辦理資訊安全教育訓練及宣導活動。

5.1.3 資訊資產存取權限之賦予，應依業務需求並考量最小權限，並以職務及權責區隔。

5.1.4 建立資訊安全事件管理程序，以確保事故妥善回應、控制與處理，訂定業務持續計畫並定期演練，以確保資訊系統或服務持續運作。

5.1.5 依據個人資料保護法與智慧財產法之相關規定，審慎處理及保護個人資訊與智慧財產權。

5.1.6 定期執行資訊安全稽核作業，檢視資訊安全管理制度之落實。

5.1.7 違反本政策與資訊安全相關規範，依相關法規或本校人事規定辦理。

5.1.8 為確保本中心同仁皆知悉資訊安全要求，另訂定「資訊安全宣言」告知本中心同仁遵悉。

5.2 瞭解組織及其全景

5.2.1 依營運目的，鑑別其會影響資訊安全管理系統之結果的內部、外部議題，包含相關法律要求或主管機關政策需求及利害關係者需求，並依鑑別結果建立「組織全景評鑑表」以作為鑑別及執行之依據，並據以確認 ISMS 之範圍符合性。

5.2.2 「組織全景評鑑表」得於每年重大議題變更時進行確認及必要之修訂。

5.3 目標

5.3.1 維護資訊之機密性、完整性與可用性，並保障使用者資料隱私。

5.3.2 保護本中心業務服務資訊，避免未經授權的存取、修改，確保其正確完整。

5.3.3 建立資訊業務永續運作計畫，以確保本中心業務服務之持續運作。

5.3.4 本中心之業務服務執行須符合相關法令或法規之要求。

5.4 審查

5.4.1 本政策應於每年檢討乙次，以反映主管機關、法令規範、技術、組織及業務等最新發展現況，以確保資訊安全實務作業之有效性。

5.4.2 本政策必須以書面、電子或其他方式告知所有同仁及提供資訊服務之相關廠商共同遵行。

5.5 實施

本政策經資訊安全委員會核定後實施，修訂時亦同。

6. 相關資料

6.1 ISMS-B-01 資訊安全管理程序。

7. 附件

7.1 ISMS-A-01-01 資訊安全宣言。