宏國德霖科技大學

資訊中心

資訊安全政策

機密等級：公開使用

文件編號：HDUT-ISMS-A-001

版　　次：1.3

發行日期：112 年 11 月 28 日

資訊安全政策					
文件編號	HDUT-ISMS-A-001	機密等級	公開使用	版次	1.3

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	104 年 10 月 16 日	N/A	資訊安全執行小組	初版發行
1.1	106 年 08 月 01 日	P.1	資訊安全執行小組	修訂本校校名
1.2	109 年 8 月 06 日	P.1	資訊安全執行小組	修訂單位名稱
1.3	112 年 11 月 28 日		資訊安全執行小組	ISO 27001 標準改版

目錄

資訊安全政策					
文件編號	HDUT-ISMS-A-001	機密等級	公開使用	版次	1.3

1 總則

1.1 為保護宏國德霖科技大學資訊中心（以下簡稱「本中心」）所管理之資訊資產安全，免於因內部或外部、蓄意或意外之各種威脅與破壞，致使業務無法正常運作或資訊遭受竄改、揭露、破壞或遺失等風險，特制訂本政策。

1.2 本政策適用之範圍係含本中心所有資訊作業。

1.3 本中心教職員、委外廠商及相關資訊業務之第三方人員均應遵守本政策。

2 目標

2.1 本中心之資訊安全政策包含下列目標：

2.1.1資訊安全政策範疇涵蓋四大控制措施領域，分別為組織控制措施、人員控制措施、實體控制措施及技術控制措施，並視需要發展出各項主題政策由管理階層核准、發布及傳達予相關人員和相關關注方。

2.1.2確保本中心資訊資產之機密性、完整性與可用性，防止非法使用。

2.1.3確保本中心所提供資訊服務之完整性與可用性，提供全校師生便利和穩定的資訊服務。

2.1.4確保本中心所提供軟硬體資源之可用性，均能被合法及正確地使用。

3 資訊安全準則

3.1 本中心全體教職員工於日常作業中確實遵守「個人資料保護法」、「著作權法」等資訊安全相關法令。

3.2 本中心全體教職員工遵守本中心相關資訊安全規定，確保適當使用本中心資源。

3.3 視實際需要辦理資訊安全教育訓練及宣導，提高所有人員資訊安全意識並熟悉工作中之資訊安全職責。

3.4 對於資訊安全事件須有完整的通報及應變措施，以確保資訊系統及重要

業務的持續運作。

3.5 組織全景，包括內外部議題、各關注方之需要及期望。

3.5.1內部全景議題，可分為組織管理層面(安全政策、管理者支持、安全組織與措施、風險管理、文件控管程序、事故應變程序、存取權限控管等)、人事層面(安全意識建立、持續教育訓練、保密、安全通報等)、技術層面(安全的資訊環境、安全的應用軟體開發、軟體與硬體維護、安全通訊、網路環境安全、防範惡意軟體、存錄等)、實體安全層面(進出管理、場域安全、設備安置及保護等)。

3.5.2外部全景議題，考量現行作業之各項外部環境議題，包括自然環境災害、法令要求、客戶要求、公共資源提供、外包服務等。

3.5.3各關注方(內外部關注方)，如主管單位(之法令法規)、客戶(之合約內容需求)、外包商(之合約及管理需求)、股東(公司穩定永續經營、獲利提高)等。

3.6 違反本政策與本校之資訊安全相關規範,依相關法規或本校懲戒規定辦理。

4 責任

4.1 為能有效確保本中心之資訊安全，應針對各資訊安全領域訂定資訊安全規範。

4.2 應每年至少召開 1 次管理審查會議，審核本中心資訊安全業務執行狀況，建立管理指標量測方式與評估管理指標量測結果。

4.3 高階主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。

4.4 所有相關同仁皆應遵循本中心資安事件通報機制，通報所發現之資訊安全事件或資訊安全弱點。

4.5 應建立資訊資產風險評鑑機制，每年至少進行 1 次風險評鑑，並由資訊安全會議訂定可接受風險值。

4.6 每年應至少進行 1 次業務永續經營計畫及資安事件通報程序之演練、測試、檢討。

4.7 每年應規劃並提供本中心人員資訊安全訓練課程，以提昇人員資訊安全認知。

4.8 與本中心簽署合約之委外廠商應簽署保密協議書，並遵循本政策以及相關程序之規定，不得未經授權使用或濫用本中心之各類資訊資產。

4.9 與本中心業務相關之專案，無論其類型均應將資訊安全要求納入專案管理考量，以落實資訊安全目標。

4.10 組織全景於管理審查會議，將與資訊安全管理系統相關之關注方需求和期望的變更、關注方的回饋等進行報告。

4.11 本中心~~校~~規劃、實作及控制資訊安全要求事項所需過程之相關準則，並實作控管措施，以「HDUT-ISMS-D-013　適用性聲明書」作為文件化資訊紀錄，對控制所規劃之變更，需審查非預期變更之後果，必要時採取行動以減輕任何負面效果，藉此確保與資訊安全管理系統相關的外部提供的過程、產品或服務受到控制。當學校確定需要對資訊安全管理系統變更時，應以規劃的方式執行變更。

4.12 本~~校~~中心於規劃資訊安全管理系統時，應了解關注方的需要及期望，並依據國際標準之要求事項來建立、實作、維持即持續改善，包括所需過程及其互動，以決定因應之風險及機會，達成資訊安全管理系統之預期成果、預防或減少非預期的影響、確保持續改善。

4.13 透過所訂定風險接受準則及具備有效、可比較與重複評鑑產生一致結果之原則執行資訊安全風險評鑑，適切選擇風險處理方法。

4.14 當決定對資訊安全管理系統進行重大變更時，採事先規畫提請管理審查會議審議後執行變更。

4.15 對於資訊安全管理系統執行成效，除依擬定適於比較即可重製的監督、

量測、分析及評估方法外，應規劃、建立、實作及維持稽核作業，並具備文件化資訊作為稽核活動及結果之佐證。

4.16 當發現不符合事項，應採取行動以控制並矯正，對消除不符合事項之原因及矯正措施進行有效性審查。

5 審查與實施

5.1 本政策應每年定期審議，或因組織、業務、法令或環境等因素之變迭時，予以適當修訂。

5.2 本政策應由資訊安全執行小組審議通過，呈請執行秘書核定後公布施行，修正時亦同。