

# 國立高雄大學

## 資訊安全政策

機密等級：一般

文件編號：NUK-ISMS-A-001

版 次：4.0

發行日期：113.08.12

## 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	98.02.25		鄭師華	初版
1.1	99.03.16	2	鄭師華	增加 5.管理指標
1.2	103.05.12	1,2,3	黃姿蓉	1. 「本中心」修改為「本校」 2. 「反應」修改為「反映」
2.0	107.01.01	1,2,3	黃姿蓉	因應 105 年教版資安規範相關 要求事項修訂
3.0	110.07.24	-	董建弘	因應資安法規、主管機關及 ISO 27001 國際資安規範相關 要求事項修訂
3.1	111.02.23	4	董建弘	本政策經「資訊安全委員會」 審議，校級「資通安全暨個人 資料保護推動委員會」核定後 實施，修訂時亦同。
3.2	112.10.04	4	陳靖雅	本政策經「資訊安全委員會」 通過後，送「資通安全暨個人 資料保護推動委員會」核定後 實施，修正時亦同。
4.0	113.08.12	1-6	黃姿蓉	因應 ISO27001:2022 改版

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

## 目錄

1	目的 .....	1
2	適用範圍 .....	1
3	目標 .....	6
4	責任 .....	7
5	管理指標 .....	7
6	審查 .....	9
7	實施 .....	9

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

## 1 目的

為確保國立高雄大學（以下簡稱「本校」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本校之業務需求，訂定本政策。

## 2 適用範圍

2.1 本政策適用範圍為本校之內部人員、委外服務廠商與訪客等。

2.2 資訊安全管理範疇涵蓋 4 類控制措施、93 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

### 2.2.1 組織控制措施：

2.2.1.1 資訊安全政策。

2.2.1.2 資訊安全之角色及責任。

2.2.1.3 職務區隔。

2.2.1.4 管理階層責任。

2.2.1.5 與權責機關之聯繫。

2.2.1.6 與特殊關注群組之聯繫。

2.2.1.7 情資威脅。

2.2.1.8 專案管理之資訊安全。

2.2.1.9 資訊及其他相關資產之清冊。

2.2.1.10 可接受使用資訊及其他相關聯資產。

2.2.1.11 資產之歸還。

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

- 2.2.1.12 資產之分類分級。
- 2.2.1.13 資訊之標示。
- 2.2.1.14 資訊傳送。
- 2.2.1.15 存取控制。
- 2.2.1.16 身分管理。
- 2.2.1.17 鑑別資料。
- 2.2.1.18 存取權限。
- 2.2.1.19 供應者關係中之資訊安全。
- 2.2.1.20 於供應者協議中闡明資訊安全。
- 2.2.1.21 管理 ICT 供應鏈中之資訊安全。
- 2.2.1.22 供應者服務之監視、審查及變更管理。
- 2.2.1.23 使用雲端服務之資訊安全。
- 2.2.1.24 資訊安全事故管理規劃及準備。
- 2.2.1.25 資訊之評鑑及決策。
- 2.2.1.26 對資訊安全事故之回應。
- 2.2.1.27 由資訊安全事故中學習。
- 2.2.1.28 證據之蒐集。
- 2.2.1.29 中斷期間之資訊安全。
- 2.2.1.30 營運持續之 ICT 備妥性。

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

2.2.1.31 法律、法令、法規之契約要求事項。

2.2.1.32 智慧財產權。

2.2.1.33 紀錄之保護。

2.2.1.34 隱私及個人可識別資訊(PII)保護。

2.2.1.35 資訊安全之獨立審查。

2.2.1.36 資訊安全政策、規則及標準的遵循性。

2.2.1.37 書面紀錄之運作程序。

#### 2.2.2 人員控制措施：

2.2.2.1 篩選。

2.2.2.2 聘用條款及條件。

2.2.2.3 資訊安全認知、教育和訓練。

2.2.2.4 獎懲過程。

2.2.2.5 聘用終止或變更後之責任。

2.2.2.6 機密性或保密協議。

2.2.2.7 遠端工作。

2.2.2.8 資訊安全事件通報。

#### 2.2.3 實體控制措施：

2.2.3.1 實體安全周界。

2.2.3.2 實體進入。

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

2.2.3.3 保全辦公室、房間及設施。

2.2.3.4 實體安全監視。

2.2.3.5 防範實體及環境威脅。

2.2.3.6 於安全區域內工作。

2.2.3.7 桌面淨空及螢幕淨空。

2.2.3.8 設備安置及保護。

2.2.3.9 場所外資產之安全。

2.2.3.10 儲存媒體。

2.2.3.11 支援公用服務事業。

2.2.3.12 佈纜安全。

2.2.3.13 設備維護。

2.2.3.14 設備汰除或重新使用之保全。

#### 2.2.4技術控制措施：

2.2.4.1 使用者終端設備。

2.2.4.2 特殊存取權限。

2.2.4.3 資訊存取限制。

2.2.4.4 對原始碼之存取。

2.2.4.5 安全識別。

2.2.4.6 容量管理。

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

- 2.2.4.7 防惡意軟體。
- 2.2.4.8 技術脆弱性管理。
- 2.2.4.9 組態管理。
- 2.2.4.10 資料刪除。
- 2.2.4.11 資料遮蔽。
- 2.2.4.12 資料洩漏預防。
- 2.2.4.13 資料備份。
- 2.2.4.14 資訊處理設施之備援。
- 2.2.4.15 日誌紀錄。
- 2.2.4.16 監視活動。
- 2.2.4.17 鐘訊同步。
- 2.2.4.18 具特殊權限共用程式之使用。
- 2.2.4.19 對運作中系統之軟體安裝。
- 2.2.4.20 網路安全。
- 2.2.4.21 網路服務的安全性。
- 2.2.4.22 網路區隔。
- 2.2.4.23 網頁過濾。
- 2.2.4.24 加密技術之使用。
- 2.2.4.25 開發生命週期之安全。



資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

- 2.2.4.26 應用程式安全要求。
- 2.2.4.27 安全系統架構及工程原則。
- 2.2.4.28 安全程式設計。
- 2.2.4.29 開發和驗收中的安全測試。
- 2.2.4.30 委外開發。
- 2.2.4.31 開發、測試及運作環境之區隔。
- 2.2.4.32 變更管理。
- 2.2.4.33 測試資訊。
- 2.2.4.34 在稽核測試期間的資訊系統保護。

### 3 目標

為維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本校全體同仁共同努力以達成下列目標：

- 3.1 保護本校業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
- 3.2 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
- 3.3 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。
- 3.4 確保本校各項業務服務之執行須符合相關法令或法規之要求。
- 3.5 透由利害相關者(關注方)與議題等要求事項，達成下列目標：
  - 3.5.1 全景與範圍對應其重要業務流程之要求與維運持續。
  - 3.5.2 達成與資安政策一致之預期。
  - 3.5.3 透過可量測的規範進行風險管理過程。

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

3.5.4本校之業務活動執行須符合相關法令或法規之要求，詳「利害相關者與議題一覽表」。

3.6 組織欲達成目標需決定相關要點：

3.6.1執行事項。

3.6.2所需資源。

3.6.3負責人員。

3.6.4完成時間。

3.6.5成果評估方式。

3.6.6各項量測指標(資安工作目標與計畫)、所需資源、負責人員、達成時間及成果評估方式等資訊，請詳閱「資安管理指標暨有效性量測表」。

#### 4 責任

4.1 本校應成立資訊安全組織統籌資訊安全事項推動。

4.2 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。

4.3 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。

4.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

4.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

#### 5 管理指標

為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下：

##### 5.1 定量化指標

5.1.1確保本校資訊服務可用性之要求如下：

5.1.1.1 資訊機房維運服務達全年上班時間 98.5%以上。

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

5.1.1.2 關鍵業務系統服務達全年上班時間 95.4%以上。

5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每年不得超過次數如下：

5.1.2.1 資訊機房維運服務中斷，每季不得超過 2 次。

5.1.2.2 關鍵業務系統服務中斷，每季不得超過 3 次。

5.1.3 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每次最長不得超過工作小時要求如下：

5.1.3.1 資訊機房維運服務中斷，每次最長不得超過 4 工作小時。

5.1.3.2 關鍵業務系統服務中斷，每次最長不得超過 8 工作小時。

5.1.4 應適當保護本校資訊資產之機密性與完整性，每年至少需進行乙次風險評鑑及風險管理。

5.1.5 為確保本校資訊安全措施或規範符合現行法令、法規之要求，每年至少需稽核乙次。

5.1.6 維護及演練業務永續運作計畫每年至少需進行乙次，以確保本校資訊業務服務得以持續運作。

## 5.2 定性化指標

5.2.1 應定期審查本校資訊安全組織人員執掌，以確保資訊安全工作之推展。

5.2.2 應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。

5.2.3 應加強本校資訊機房設施之環境安全，採取適當之保護及權限控管機制。

5.2.4 應確保資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。

5.2.5 應加強存取控制，防止未經授權之不當存取，以確保本校資訊資產已

資訊安全政策					
文件編號	NUK-ISMS-A-001	機密等級	一般	版次	4.0

受適當之保護。

5.2.6本校資訊系統開發應考量安全需求，並定期稽核安全弱點。

5.2.7應確保所有資訊安全事件或可疑之安全弱點，均依循適當之通報機制向上反映，並予以適當調查及處理。

## 6 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本校業務永續運作之能力。

## 7 實施

本政策經「資訊安全委員會」通過後，送「資通安全暨個人資料保護推動委員會」核定後實施，修正時亦同。