

國立高雄大學

全景範圍與溝通管理政策

機密等級：一般

文件編號：NUK-ISMS-A-002

版 次：3.3

發行日期：114.02.26

全景範圍與溝通管理政策					
文件編號	NUK-ISMS-A-002	機密等級	一般	版次	3.3

目錄

1	目的	1
2	適用範圍	1
3	權責	2
4	名詞定義	2
5	作業說明	3
6	審查	5
7	實施	5
8	相關文件	5

全景範圍與溝通管理政策					
文件編號	NUK-ISMS-A-002	機密等級	一般	版次	3.3

1 目的

國立高雄大學（以下簡稱「本校」）為強化資訊安全管理，確保資訊安全管理制度執行之範圍，期使資安管理制度達成既定之目標，以維護相關業務運作之安全。並為使相關業務順利推展，經溝通協調後取得共識，維護業務運作之安全，提供本校營運持續運作之資訊環境，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，特訂此政策規範。

2 適用範圍

2.1 本校主機房設施維運、核心系統維護作業。

2.2 考量本校內部、外部議題。依據如下：

2.2.1 外部議題：

2.2.1.1 為組織尋求達成其目標所處之外部環境，經考量外部利害相關者之目標與關切事項、法令規章要求、利害相關者感知及風險管理過程範圍之相關風險事項，如：國家、區域、社會文化、法令規章、經濟、技術、環境。

2.2.1.2 對組織目標具衝擊之主要推動者與趨勢。

2.2.1.3 與外部利害相關者之關係互動與其對於組織之價值。

2.2.2 內部議題：

2.2.2.1 為組織尋求達成其目標所處之內部環境，可影響組織管理之任何事務，於前後環節進行評估，其組織之專案過程與內容

全景範圍與溝通管理政策					
文件編號	NUK-ISMS-A-002	機密等級	一般	版次	3.3

須以組織目標觀點為主要考量，可能產生無法達成目標之機會進而影響組織承諾、信賴與價值觀影響之事件。

2.2.2.2 針對資通訊治理之組織架構與角色執掌、政策目標達成策略、組織支援與知識管理能力、資訊系統與其流程因應。

2.2.2.3 組織文化與遵循標準、指導綱要與合約關係等模式。

3 權責

- 3.1 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。
- 3.2 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。
- 3.3 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。
- 3.4 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。

4 名詞定義

4.1 內部利害相關者：

組織內可影響、受其所影響、抑或自認會受到決策或活動影響的個人或相關單位。

4.2 外部利害相關者：

組織外可影響、受其所影響、抑或自認會受到決策或活動影響的個人或組織。

全景範圍與溝通管理政策					
文件編號	NUK-ISMS-A-002	機密等級	一般	版次	3.3

4.3 內外部議題：

組織為尋求達成其目標所處之內外部環境，可能影響組織目標與範圍定義之風險因素。

4.4 資訊資產：

係指為維持本校相關業務流程運作之硬體、軟體、服務、文件及人員。

4.5 營運持續運作之資訊環境：係指為維持本校各項業務正常運作所需之電腦作業環境。

4.6 溝通議題：

組織為尋求達成其目標期間，面臨可能影響組織目標與範圍事務之協調議題。

5 作業說明

5.1 進行內外部利害相關團體與議題之確認，以符合資安全景與範圍界定。

5.2 決定可能影響資訊安全管理系統之外部與內部議題，及辨識其利害相關者與對資訊安全相關之要求事項（可包含法令法規要求與契約義務），並將結果彙整填入「利害相關者與議題一覽表」。

5.3 所確認之外部與內部議題及要求事項，可作為決定資訊安全管理制度範圍之考量。

全景範圍與溝通管理政策					
文件編號	NUK-ISMS-A-002	機密等級	一般	版次	3.3

5.4 內部溝通管道

宣達本校資訊安全政策、組織目標及相關規定或校內涉及相關需求，適時參與校內各項溝通會議。

5.4.1 參加人員

本校系統業務流程相關單位主管、業務承辦人員、資訊人員、資安小組成員。

5.4.2 溝通時機

透過校內舉辦之行政會議、校務會議、資訊安全管理會議。

5.4.3 溝通事項

涉及資訊安全之網路、系統、本校相關業務流程與活動議題。

5.5 外部溝通管道

5.5.1 參加人員

與本校業務相關之主管機關、委外(維護)廠商，與本校業務關係或交流互動、具高度關聯或影響之對象。

5.5.2 溝通時機與頻率

非迫切或法令法規要求事項，均由資訊人員決議溝通時機之合宜安排。

5.5.3 溝通事項

涉及資訊安全之網路、系統、本校相關業務流程與活動議題。

全景範圍與溝通管理政策					
文件編號	NUK-ISMS-A-002	機密等級	一般	版次	3.3

5.6 溝通媒介

可適切利用活動、問卷、訪談、會議、滿意度調查表等形式或工具進行取得。

5.7 議題追蹤

溝通結果必須經媒介有效呈現議題討論之共識，並經由單位主管委派相關人員進行後續追蹤與處理。

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。

8 相關文件

8.1 資訊安全組織成員表。

8.2 外部單位聯絡清單。

8.3 利害相關者與議題一覽表。

8.4 業務流程衝擊分析表。