1. 目的

高雄科技大學鐵道技術中心（以下簡稱本中心）為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本中心之資訊業務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，特定此政策規範。

2. 適用範圍

本政策適用於各項資產及資通使用者，資通使用者係包含員工、建置維護廠商及其他經授權使用資產之人員。

3. 名詞解釋

3.1 資訊安全管理：保護資產避免遭受各種不當使用、洩漏、竄改、竊取、破壞等事故威脅，並降低可能影響及危害業務運作之損害程度。

3.2 機密性（Confidentiality）：指確保只有經授權之人才能存取資產。

3.3 完整性（Integrity）：指確保資產其處理方法之準確及完整(Completeness）。

3.4 可用性（Availability）：指確保經授權之使用者在需要時，可以使用資產。

3.5 資訊資產：係指為維持本中心資訊業務正常運作之硬體、軟體、服務、文件及人員。

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

4. 資訊安全政策及目標

4.1 資訊安全政策

為使本中心業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循。

4.1.1 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

4.1.2 應保護本中心所提供軟硬體系統機敏資訊及資通系統之機密性與完整

性，避免未經授權存取與竄改。

4.1.3 應強固核心資通系統之韌性，確保本中心業務持續營運，以達成永續發展目標。

4.1.4 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高同仁之資通安全意識，同仁亦應確實參與訓練。

4.1.5 確保本中心資通系統安全，防範資安攻擊事件發生。

4.1.6 應訂定營運持續運作計畫，以確保各種人為或天然災害發生時，核心業務可持續運作。

4.1.7 落實人員辦理業務涉及資通安全事項之獎懲機制。

4.1.8 各項資通安全管理規定必須遵守政府相關法規(如：資通安全管理法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等）之規定。

4.2 資訊安全目標

4.2.1. 量化型目標

4.2.1.1 本中心核心資通系統及網路運作，其可用性需達到當年度預定目標。

4.2.1.2 執行營運持續計畫演練及維護，以確保核心資通系統及網路服務得以持續運作。

4.2.1.3 確保免於侵害著作權，每年審查軟體使用狀況。

4.2.1.4 確保人員資訊安全能力與認知，每年實施資通安全教育訓練。

4.2.1.5 確保資料隱密性、完整性與可用性，每年實施帳號權限審查。

4.2.1.6 確保組織資訊安全，避免發生資訊安全事故。

4.2.2 質化型目標

應定期執行風險評鑑或在營運流程改變、架構變更，或新服務上線前，必須重新進行相關部分風險評鑑，並考量資通安全需求或風險評鑑處理結果，是否符合資通安全政策方針。

5. 責任

5.1 資訊安全管理代表建立及審查此政策。

5.2 資訊安全管理代表透過適當的標準和程序以實施此政策。

5.3 資訊安全管理代表應積極參與資訊安全管理制度活動，提供對資訊安全管理制度之支持，並展現對其持續改善之領導與承諾。

5.4 所有人員和委外服務廠商均須依照相關安全管理程序以維護資訊安全政策。

5.5 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。

5.6 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中心之相關規定進行懲處。

6. 審查

本政策應至少每年審查 1 次，以反映政府法令、技術及業務等最新發展現況，並確保本中心永續運作及資訊安全實務作業能力。

7. 實施

本政策經資訊安全管理代表審查、核定後公告實施，修正時亦同。