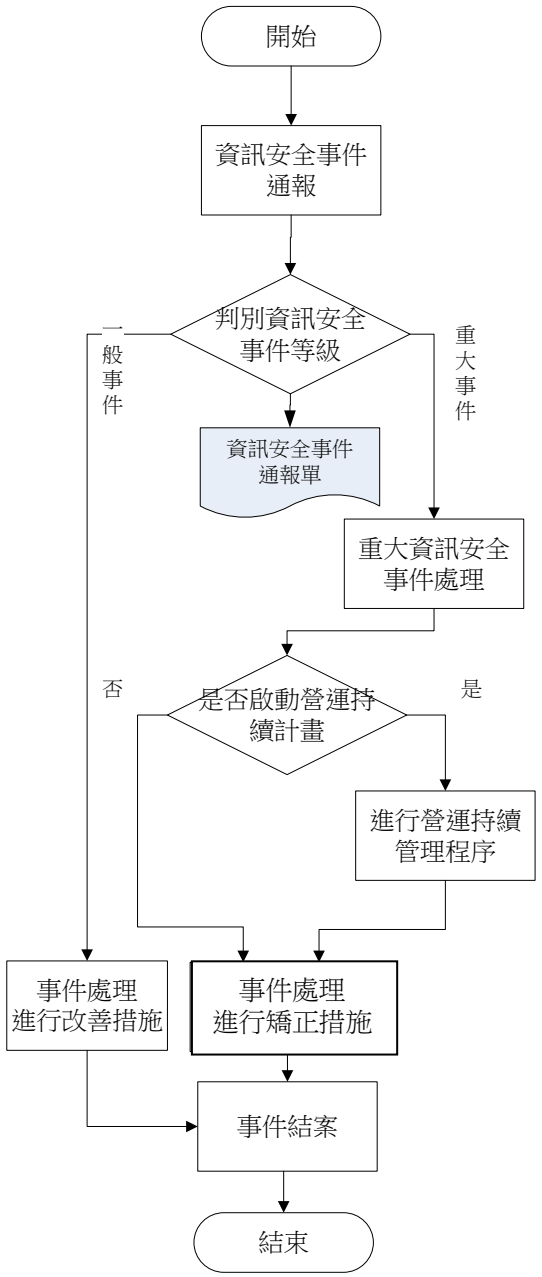
國立金門大學 National Quemoy University

資訊安全事件通報與應變作業流程

1　流程圖：

流程	說明	權責分工
	察覺資訊安全事件 資訊安全事件通報 評估資訊安全事件之等級，，並填製「資訊安全事件通報單」。 進行資訊安全事件之證據蒐集及判斷是否啟動營運持續計畫辦法。 參考「營運持續運作管理程序」，並啟動營運持續管理程序。 事件處理(應變措施) 一般事件⇨進行改善措施 重大事件⇨進行該事件排除與執行改善措施。 事件結案，必要時依相關法規究責。	本校全體同仁 資訊安全小組

2　流程說明：

2.1　資訊安全事件通報：

2.1.1 本校員工於業務處理過程中發生資訊安全事件，或發現與資訊安全有關之潛在風險時，應向資訊安全通報窗口通報。

2.2　判別資訊安全事件等級：

2.2.1 資訊安全通報窗口於收到通報後，應立即進行該事件等級評估，並填寫「資訊安全事件通報單」。

2.2.2 若為「一般事件」直接進行改善作業並將改善措施記載於應變措施欄位後歸檔；若為「重大事件」，則依照下列重大資訊安全事件流程處理。

2.3　重大資訊安全事件處理：

2.3.1 證據蒐集：

2.3.1.1　當重大資訊安全事件發生時，若涉及行政或法律責任之追究，資訊安全小組應協助蒐集完整證據(如 Log、表單記錄、合約等)。

2.3.1.2　判斷是否啟動營運持續計畫作業：

2.3.1.2.1 依照「營運持續運作管理程序書」內有關營運持續計畫作業指導書啟動條件，判斷是否啟動營運持續作業。

2.3.2 進行營運持續管理程序

2.3.2.1　依照「營運持續運作管理程序書」之流程處理。

2.3.3 進行矯正措施程序

2.3.3.1 重大事件之矯正措施需記載於「資訊安全事件通報單」應變措施欄位。

2.3.4 事件結案

2.3.4.1 資訊安全事件必須確實排除後始得結案。