特定非公務機關資通安全事件通報應變及演練作業規範

（範本）

目錄

壹、 目的

ＯＯＯ〔以下簡稱本機關（請依需求替換為本公司、本基金會….等，下同）〕為遵照資通安全事件通報應變及演練辦法第四條、第五條，及本機關資通安全維護計畫之規定，建立本機關資通安全事件之通報應變及演練作業規範，以迅速有效獲知並處理資通安全事件，特制定本資通安全事件通報應變及演練作業規範（以下稱本作業規範）。

貳、 適用範圍

發生於本機關之資通安全事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、 責任

一、本機關所屬人員於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本機關應於知悉資通安全事件後，依本程序之規定，儘速完成事件通報、損害控制、復原與事件之調查及處理作業。完成後，應依中央目的事業主管機關指定之方式及時限進行結案登錄作業，並送交調查、處理及改善報告。

三、本機關應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變作業規範，並於知悉資通安全事件後向本機關進行通報，於完成事件之通報及應變程序後，依本機關指示提供相關之紀錄或資料。

肆、 資通安全事件通報窗口及緊急處理小組

一、本機關之資通安全事件通報窗口及聯繫方式為：（各機關自行定義）

二、本機關應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

三、本機關所屬人員發現資通安全事件後，應立即向所屬單位主管及本機關之通報窗口通報。

四、本機關應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

五、負責事件處理之單位（該事件發生之單位）權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

六、事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全管理代表報告，由資通安全管理代表成立緊急處理小組，立即協助進行處理；接獲受託廠商所通報之資通安全事件時，比照辦理。

七、緊急處理小組成員由資通安全管理代表指派機關之資通安全相關技術人員擔任，或亦得聘任外部專家擔任之。

八、各相關權責人員應記錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、 通報程序

一、通報作業程序

（一）判定事件等級之流程及權責

本機關之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報應變及演練辦法」之資通安全事件等級判斷：

1. 事件若涉及洩漏資訊，其內容是否涉及核心業務或關鍵基礎設施業務，是否屬國家或一般公務機密，及影響程度，屬嚴重或輕微。
2. 事件若導致業務之資訊或資通系統遭竄改，遭竄改內容是否涉及核心業務或關鍵基礎設施業務之資訊，是否屬國家或一般公務機密，及影響程度，屬嚴重或輕微。
3. 機關業務運作若遭影響或資通系統停頓，其影響是否涉及核心業務或關鍵基礎設施業務之資訊，是否於可容忍中斷時間內能回復正常運作。
4. 事件其他足以影響資通安全事件等級之因素。

（二）除事件之等級外，權責人員或緊急處理小組亦應對資通安全事件之影響範圍、損害程度及本機關因應之能力進行評估。

（三）本機關權責人員或緊急處理小組於完成資通安全事件等級之判斷及相關評估後，應儘速報資通安全管理代表核准。

（四）權責人員應於知悉資通安全事件後一小時內依中央目的事業主管機關所指定或認可之方式，進行事件通報。

（五）本機關因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於知悉資通安全事件後一小時內以電話或其他適當方式，將該次資安事件應通報之內容及無法依規定方式通報之事由，分別告知所屬之中央目的事業主管機關，並於事由解除後，依原方式補行通報。

（六）資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。

（七）本機關於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向本機關之權責人員或窗口，以指定之方式進行通報。

（八）本機關執行通報應變作業時，得視情形向中央目的事業主管機關提出技術支援或其他協助之需求。

陸、 應變程序

一、事件發生前之防護措施規劃

本機關應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

（一）負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 資安事件相關鑑識及其他調查作業。
4. 資安事件之調查與處理及改善報告之方式。
5. 資安事件後續發展及與其他事件關聯性之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
7. 其他資通安全事件應變之相關事項。

（二）對於第一級、第二級資通安全事件，本機關應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本機關應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

（三）本機關完成通報及應變程序之辦理後，應依中央目的事業主管機關所指定或認可之方式進行結案登錄。

（四）本機關於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、 資安事件後之復原、鑑識、調查及改善機制

一、本機關完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、資通安全事件調查、處理及改善報告應包括以下項目：

（一）事件發生、完成損害控制或復原作業之時間。

（二）事件影響之範圍及損害評估。

（三）損害控制及復原作業之歷程。

（四）事件調查及處理作業之歷程。

（五）為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

（六）前款措施之預定完成時程及成效追蹤機制。

三、本機關應向中央目的事業主管機關提出前項之報告，以供監督與檢討。

捌、 紀錄留存及管理程序之調整

一、本機關應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「資通安全事件通報紀錄

單」上留存完整之紀錄，該文件並應經承辦之權責人員、資通安全管理代表簽核。

二、本機關於完成資通安全事件之通報及應變程序後，應依據「資通安全事件通報紀錄單」之內容及實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、 演練作業

本機關應配合中央目的事業主管機關依資通安全事件通報應變及演練辦法之規定規劃或辦理之資通安全演練作業。