經濟部電子資料遭竊事故處理作業程序修正對照表

修正名稱	現行名稱	說明
經濟部電子資料遭竊事件處理作業程序	經濟部電子資料遭竊事故處理作業程序	依資通安全管理法第十四條，名稱酌作修正。
修正規定	**現行規定**	**說明**
壹、目的： 經濟部（以下簡稱本部）為處理駭客入侵導致電子資料遭竊事件之作業程序標準化，以提升本類事件處理速度、保存事件相關資訊及強化本部資訊安全，特訂定本作業程序（以下簡稱本作業處理程序）。	壹、目的： 經濟部（以下簡稱本部）為處理駭客入侵導致電子資料遭竊事故之作業程序標準化，以提升本類事故處理速度、保存事故相關資訊及強化本部資訊安全，特訂定本作業程序（以下簡稱本作業處理程序）。	依資通安全管理法第十四條，文字酌作修正。
貳、適用對象及時機： 一、適用對象：本部部次長室、主任秘書室、參事室及所屬幕僚單位。 二、適用時機：本部因駭客入侵導致電子資料遭竊時，依本作業處理程序辦理。	貳、適用對象及時機： 一、適用對象：本部部次長室暨所屬幕僚單位（不含中部辦公室、中區聯合服務中心及南區聯合服務中心）。 二、適用時機：本部因駭客入侵導致電子資料遭竊時，依本作業處理程序辦理。	依資通安全管理法修正適用對象。
參、作業程序： 一、於本部資訊安全監控中心（以下簡稱監控中心）處理資通安全事件且發現有資料遭竊跡象時，依下列程序處理： （一）資安通報作業 依「經濟部資通安全事件通報及應變管理程序」陳	參、作業程序： 一、於本部資訊安全監控中心（以下簡稱監控中心）處理資訊安全事件且發現有資料遭竊跡象時，依下列程序處理： （一）資安通報作業 依「經濟部資通安全事件緊急應變計畫暨作業處理	一、經濟部資通安全事件緊急應變計畫暨作業處理程序已於一百零八年二月一日

報並於「國家資通安全通報應變網站」進行通報作業。 （二）事件處理作業 依設備類別（個人電腦或主機）及現場環境綜合評估。為避免揮發性資料因電源關閉影響事件調查，於狀況許可下，先將設備網路斷線並採擷揮發性資料。 1.個人電腦 (1)取得使用者電腦 如該部電腦於事件調查時為開機狀態，則應先將記憶體資料轉存（Memory Dump）後，再將該部電腦取回資訊中心，以盡量保持其原始狀態之完整性，俾利後續調查處理作業。 (2)電腦硬碟映像檔製作 取回之個人電腦硬碟由監控中心作業人員進行一對一（Bit-Stream）完全複製（一式三份），一份作為事件調查用；一份作為歸還使用者備份資料用；另一份留存備用。	程序」（附件一）陳報並於「國家資通安全通報應變網站」進行通報作業。 （二）事故處理作業 依設備類別（個人電腦或主機），進行以下處理作業。 1.個人電腦 1.1 取得使用者電腦 將該部電腦取回資訊中心，以盡量保持其原始狀態之完整性，俾利後續調查處理作業。 1.2 電腦硬碟映像檔製作 取回之個人電腦硬碟由監控中心作業人員進行一對一（Bit-Stream）完全複製（一式三份），一份作為事故調查用；一份作為歸還使用者備份資料用；另一份留存備用。 1.3 原始電腦硬碟封存 原始電腦硬碟以公文袋封存，標示後置於資訊中心機房防火保險櫃內（標示格式如附件二）。 1.4 電腦歸還使用者	停止適用，本部並於同日訂定經濟部資通安全事件通報及應變管理程序，而本點為配合前揭規範變更，爰修正第一款第一目及第八目之一。 二、經濟部資通安全處理小組設置要點已於一百零八年一月二十二日停止適用，本部並於同日訂定經濟部資通安全推動小組設置要點，而本點為配合前揭規範

(3)原始電腦硬碟封存 原始電腦硬碟以公文袋封存，標示後置於資訊中心機房防火保險櫃內（標示格式如附件一）。 (4)電腦歸還使用者 將其中一份複製硬碟中之惡意程式清除後，安裝回使用者電腦，歸還使用者，並請使用者變更相關帳號之密碼。 (5)電腦使用者備份資料 使用者進行檔案資料檢視，將確屬於個人之公私務資料部分進行備份作業。 (6)電腦重新安裝 為確保使用者電腦環境之安全，俟電腦使用者備份作業完成後，再由資訊中心進行電腦重新安裝作業。 2.主機 (1)主機映像檔製作及封存 ①如屬虛擬主機，則由監控中心作業人員直接複製該虛擬主機檔案二份，並註記複製檔案建立日期時間。 ②如屬實體主機，則由監控中心作業人員於	將其中一份複製硬碟中的惡意程式清除後，安裝回使用者電腦，歸還使用者，並請使用者變更相關帳號之密碼。 1.5 電腦使用者備份資料 使用者將屬於個人的公私務資料部分進行備份作業。 1.6 電腦重新安裝 為確保使用者電腦環境之安全，俟電腦使用者備份作業完成後，再由資訊中心進行電腦重新安裝作業。 2.主機 2.1 主機映像檔製作及封存 (1)如屬虛擬主機，則由監控中心作業人員直接複製該虛擬主機檔案二份。 (2)如屬實體主機，則由監控中心作業人員針對本機硬碟部分進行一對一（Bit-Stream）完全複製（一式二份）。 (3)複製品一份作為事	變更，爰將第一款第八目之一「本部資通安全『處理』小組修正為「資通安全『推動』小組」，其餘文字亦配合前揭規定變更，酌作文字修正。 三、本點其餘款次或目次等為配合實務辦理需要，文字酌作修正。

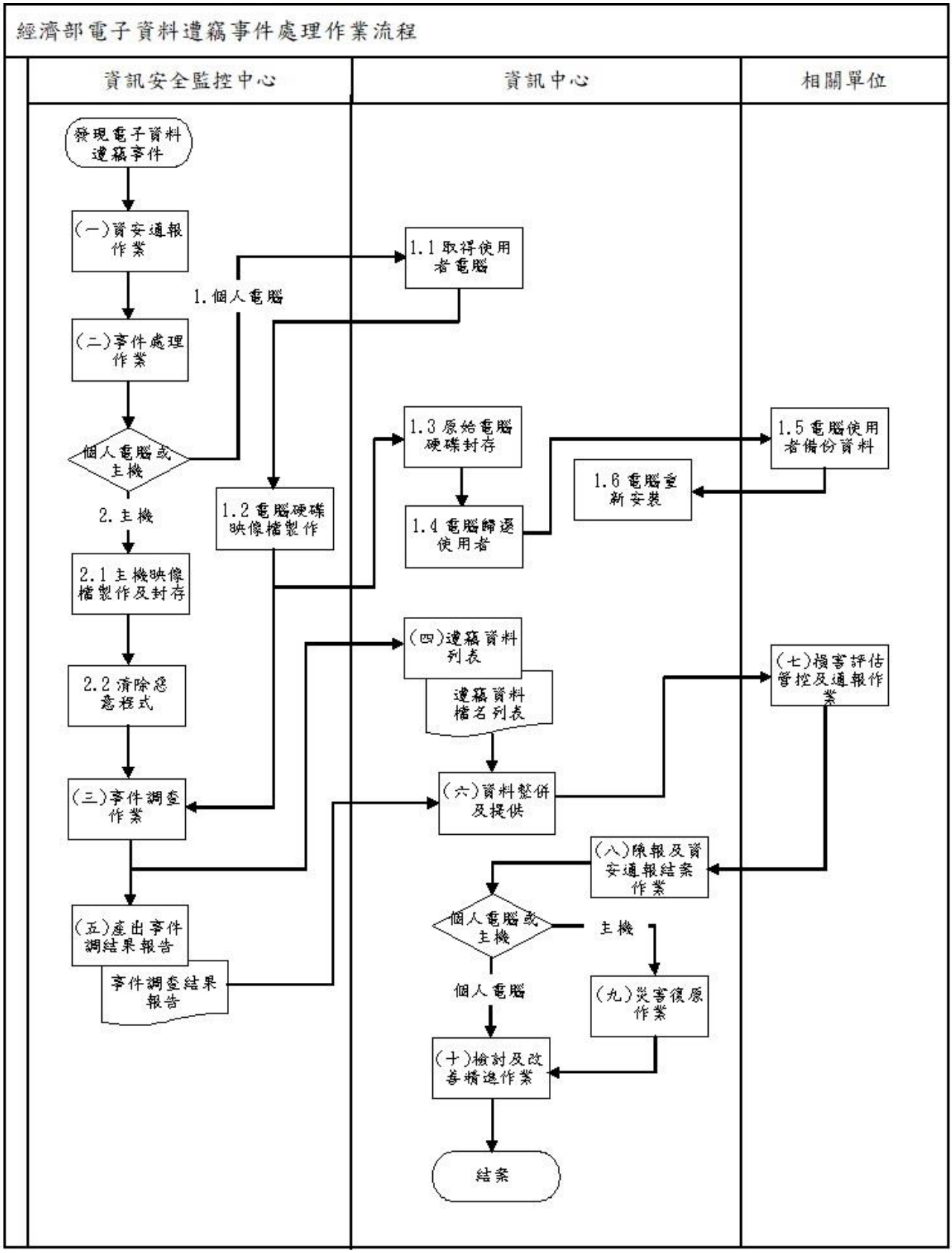
確認系統服務可中斷後，先將記憶體資料轉存（Memory Dump），再將主機電源關閉，並針對本機硬碟部分進行一對一（Bit-Stream）完全複製（一式二份）。 ③複製品一份作為事件調查用；另一份封存備用。 (2)清除惡意程式 清除主機上之惡意程式，以防駭客續以利用。 （三）事件調查作業 1. 監控中心針對複製品進行調查分析作業，檢查項目包含使用者電腦登入紀錄、系統機碼、處理程序及應用程式、檔案異動紀錄、USB 使用紀錄、上網紀錄、E-mail 紀錄、軟體使用紀錄以及記憶體暫存資料等項目，並依事件發生時間、惡意程式、惡意網路連線關係、攻擊手法及利用之系統漏洞等進行整體關聯分析作業。 2. 於調查當時發現可立即進行之損害管控動作，資訊	故調查用；另一份封存備用。 2.2 清除惡意程式 清除主機上之惡意程式，以防駭客續以利用。 （三）事故調查作業 1. 監控中心針對複製品進行調查分析作業，檢查使用者電腦登入紀錄痕跡、系統機碼、文件開啟痕跡、USB 使用痕跡、上網痕跡、E-mail 痕跡、軟體使用痕跡、記憶體等項目，並進行發生時間、惡意程式、惡意網路連線關係、運用手法及運用系統漏洞等整體分析作業。 2. 於調查當時發現可立即進行之損害管控動作，資訊中心得先進行處理，如當下發現惡意程式連往之駭客中繼站位置，立即於安全設備上進行連線阻擋，或停用遭利用之帳號等，以降低損害。 （四）遭竊資料列表 疑似遭竊之資料檔由資訊中心進行檔名列表作業，以供資料所屬單位進行損害評估及管控之用。	

中心得先進行處理，如當下發現惡意程式連往之駭客中繼站位置，立即於安全設備上進行連線阻擋，或停用遭利用之帳號等，以降低損害。 （四）遭竊資料列表 疑似遭竊之資料檔由資訊中心進行檔名列表作業，以供資料所屬單位進行損害評估及管控之用。 （五）產出事件調查結果報告 監控中心進行事件調查暨處理作業後，產出「經濟部資通安全事件調查結果報告」（格式如附件二，不含「資料檔案檔名列表」部分）。 （六）資料整併及提供 1. 將前開之事件調查結果報告與檔名列表資料，合併成完整報告。 2. 將報告中之「資料檔案檔名列表」部分提供資料所屬單位進行損害評估及管控作業。 （七）損害評估管控及通報作業 1. 資料所屬單位針對遭竊資料進行損害評估及後續之損害管控作業。 2. 資料所屬單位須填具「經	（五）產出事故調查結果報告 監控中心進行事故調查暨處理作業後，產出「經濟部資通安全事故調查結果報告」（格式如附件三，不含「資料檔案檔名列表」部分）。 （六）資料整併及提供 1. 將前開之事故調查結果報告與檔名列表資料，合併成完整報告。 2. 將報告中之「資料檔案檔名列表」部分提供資料所屬單位進行損害評估及管控作業。 （七）損害評估管控及通報作業 1. 資料所屬單位針對遭竊資料進行損害評估及後續之損害管控作業。 2. 資料所屬單位須填具「經濟部遭竊電子資料機敏等級評估單」（附件四）回報資訊中心。 3. 如遭竊資料內含機敏資訊，資料所屬單位須向政風處通報。 （八）陳報及資安通報結案作業 1. 遭竊資料如內含機敏資訊，資訊中心須依「經濟部資通安全事件緊急應變計畫暨作業處理程序」向	

濟部遭竊電子資料機敏等級評估單」（附件三）回報資訊中心。 3. 如遭竊資料內含機敏資訊，資料所屬單位須向政風處通報；如遭竊資料內含個人資料，資料所屬單位須依經濟部及所屬機關個人資料保護管理要點第二十二點規定通報至本部個人資料保護推動執行小組。 （八）陳報及資安通報結案作業 1. 遭竊資料如內含機敏資訊，資訊中心須依「經濟部資通安全事件通報及應變管理程序」向本部資通安全推動小組召集人（資通安全長）陳報。 2. 依前述程序於「國家資通安全通報應變網站」進行資訊作業面之結案作業。 3. 封存之硬碟併同完整報告以密件公文歸檔專用資料袋封存，標示後置於資訊中心機房防火保險櫃內。（標示格式如附件一） （九）災害復原作業（主機） 應變更該主機及系統相關使用之帳號及密碼，並依主機及系統復原程序進行	本部資通安全處理小組召集人（資訊安全長）陳報。 2. 依前述程序於「國家資通安全通報應變網站」進行資訊作業面之結案作業。 3. 封存之硬碟併同完整報告以密件公文歸檔專用資料袋封存，標示後置於資訊中心機房防火保險櫃內。（標示格式如附件二） （九）災害復原作業（主機） 應變更該主機及系統相關使用之帳號及密碼，並依主機及系統復原程序進行災害復原作業。 （十）檢討及改善精進作業 檢討遭入侵原因後，進行後續改善精進作業。 二、封存之證物，於資安通報結案作業完成日二年後銷毀，調查結果報告循公文程序歸檔。	

災害復原作業。 （十）檢討及改善精進作業 檢討遭入侵原因後，進行後續改善精進作業。 二、封存之證物，於資安通報結案作業完成日二年後銷毀，調查結果報告循公文程序歸檔。		
肆、經濟部電子資料遭竊事件處理作業流程如附圖。	肆、經濟部電子資料遭竊事故處理作業流程如附圖。	文字及附圖酌作修正。

修正後附圖


經濟部電子資料遭竊事件處理作業流程
資訊安全監控中心
資訊中心
相關單位
發現電子資料遭竊事件
(一)資安通報作業
(二)事件處理作業
個人電腦或主機
1.個人電腦
2.主機
1.1 取得使用者電腦
1.2 電腦硬碟映像檔製作
1.3 原始電腦硬碟封存
1.4 電腦歸還使用者
1.5 電腦使用者備份資料
1.6 電腦重新安裝
2.1 主機映像檔製作及封存
2.2 清除惡意程式
(三)事件調查作業
(四)遭竊資料列表
遭竊資料檔名列表
(五)產出事件調結果報告
事件調查結果報告
(六)資料整併及提供
(七)損害評估管控及通報作業
(八)陳報及資安通報結案作業
個人電腦或主機
主機
個人電腦
(九)災害復原作業
(十)檢討及改善精進作業
結案

修正後附件一

經濟部電子資料遭竊事件證物/調查結果報告封存封

事件編號	（同「經濟部資通安全事件調查結果報告」）
封存內容及數量	
封存日期	年　　月　　日
設備使用者	**單位：** **姓名：**
封存人員	
資安通報單 ID	（國家資通安全通報應變作業發配之編號）
資安通報結案日期	年　　月　　日
※封存內容於通報結案作業完成日 2 年後銷毀	

修正後附件二

經濟部資通安全事件調查結果報告

事件說明		
事件編號	(MOEA-AIR-西元年-流水號 3 碼，流水號每年由 001 開始累計，AIR：Accident investigation report)	
事件發現日期	年　　月　　日　　時　　分	
作業人員		
事件描述		
通報單 ID	（國家資通安全通報應變作業發配之編號，無則免填）	
通報作業日期	通 報 日 期 ：　　年　　月　　日 通報結案日期：　　年　　月　　日	
設備及證物(硬碟)資訊		
設備資訊	IP：	OS：
設備使用者或用途	主機名稱： 主機用途：	
設備 Patch 狀態	OS:	Office：
防毒軟體版本		
證物廠牌	（未保留證物則不需要）	
證物型號	（未保留證物則不需要）	
證物容量	（未保留證物則不需要）	
證物外觀	（證物照片，未保留證物則不需要）	
調查暨處理過程描述		
使用工具	調查時使用之軟硬體工具	
檢查項目	使用者電腦登入紀錄、系統機碼、處理程序及應用程式、檔案異動紀錄、USB 使用紀錄、上網紀錄、E-mail 紀錄、軟體使用紀錄以及記憶體暫存資料等	
發現狀況說明	遭植入惡意程式、有被打包資料殘留等	
疑有資料遭竊	□是　□否	
處理作業	停用網路服務、清除惡意程式等	

說明			
惡意程式或工具樣本分析			
檔名			
存在路徑			
日期資訊	建立：	修改：	存取：
擁有者			
檔案大小(Bytes)			
MD5			
連線標的			
防毒軟體掃描結果			
行為描述			
檢討及建議事項			

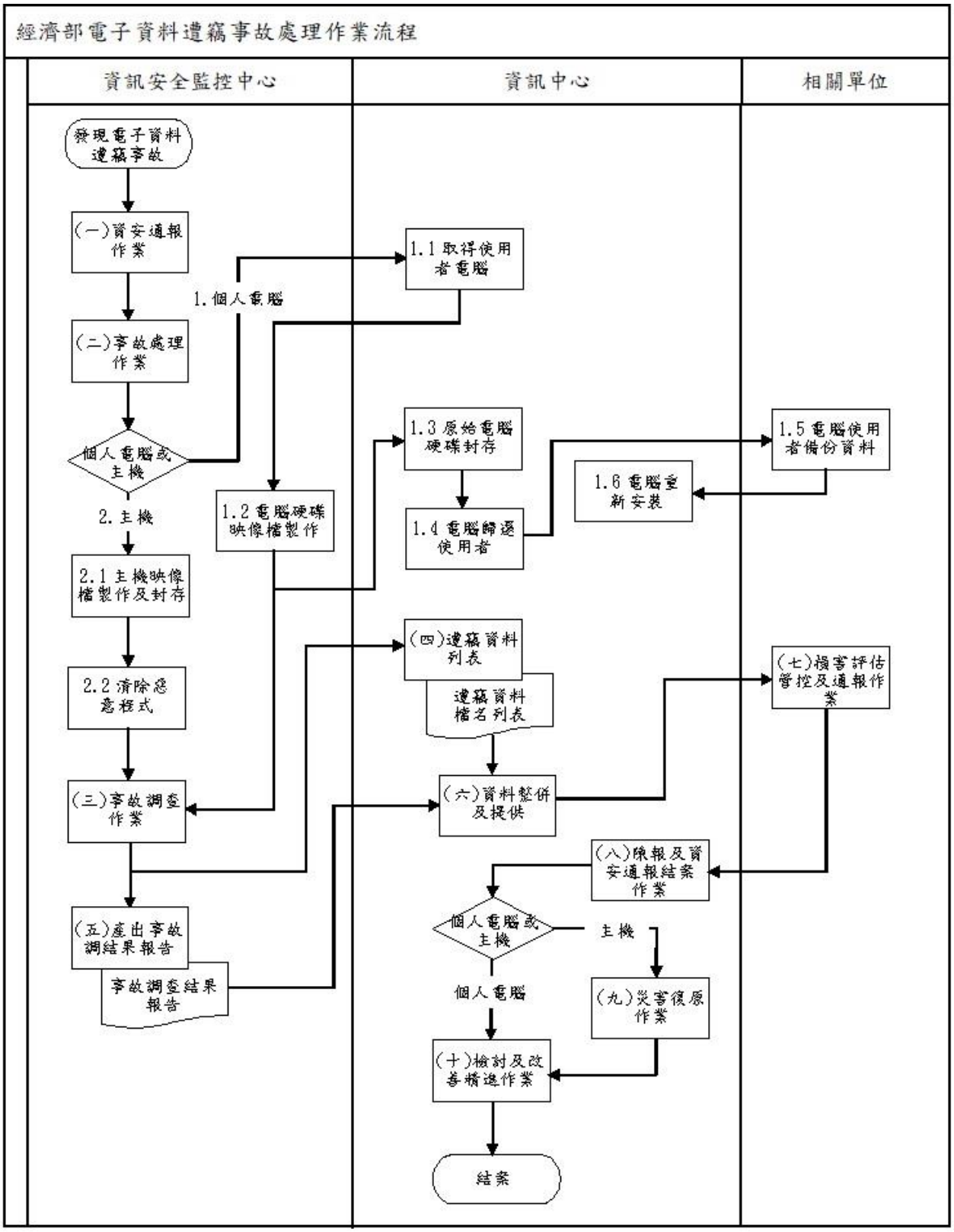
資料檔案檔名列表					
序號	檔名	檔案大小(Bytes)	建立日期	修改日期	擁有者

修正後附件三

經濟部遭竊電子資料機敏等級評估單

※以下由「資訊中心」填列	
事件編號	
事件發現時間	年　　月　　日
※以下由「資料所屬單位」填列	
填列日期	年　　月　　日
遭竊資料 最高機敏等級	□絕對機密等級公務資料 □極機密等級公務資料 □機密等級公務資料 □密等級公務資料 □敏感等級公務資料 □非屬密級以上或敏感之核心業務資料 □非核心業務資料
是否已通報政風處	□是　□否
填報人員： 填報人員主管： 填報單位主管：	
本評估單請於資料送達後 2 日內回擲資訊中心	

修正前附圖


經濟部電子資料遭竊事故處理作業流程
資訊安全監控中心
資訊中心
相關單位
發現電子資料遭竊事故
(一)資安通報作業
(二)事故處理作業
個人電腦或主機
1.個人電腦
2.主機
1.1 取得使用者電腦
1.2 電腦硬碟映像檔製作
1.3 原始電腦硬碟封存
1.4 電腦歸還使用者
1.5 電腦使用者備份資料
1.6 電腦重新安裝
2.1 主機映像檔製作及封存
2.2 清除惡意程式
(三)事故調查作業
(四)遭竊資料列表
遭竊資料檔名列表
(五)產出事故調結果報告
事故調查結果報告
(六)資料整併及提供
(七)損害評估管控及通報作業
(八)陳報及資安通報結案作業
個人電腦或主機
主機
個人電腦
(九)災害復原作業
(十)檢討及改善精進作業
結案

修正前附件一

經濟部資通安全事件緊急應變計畫及作業處理程序

一、 經濟部（以下簡稱本部）為有效掌握本部及所屬行政機關、事業機構（以下簡稱本部及所屬機關（構））之資通訊、網路系統或其他重大災害事件，俾迅速辦理資通安全事件（以下簡稱資安事件）通報及緊急應變處置，並在最短時間內回復，以確保本部作業之正常運作，特依行政院訂頒之國家資通訊發展方案及行政院國家資通安全會報函頒之國家資通安全通報應變作業綱要訂定本作業處理程序。

二、 本作業處理程序適用對象及時機：

（一）適用對象：本部及所屬機關（構）。

（二）適用時機：本部及所屬機關（構）於發生資安事件或其他災害涉及資安事件時，應立即依本作業處理程序辦理。

三、 資安事件影響等級：

資安事件影響等級分為四級別，由重至輕分別為四級、三級、二級及一級：

（一）符合下列情形之一者，屬四級事件：

1. 國家機密資料遭洩漏。
2. 關鍵資訊基礎設施系統或資料遭嚴重竄改。
3. 關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

（二）符合下列情形之一者，屬三級事件：

1. 密級或敏感公務資料遭洩漏。
2. 核心業務系統或資料遭嚴重竄改、關鍵資訊基礎設施系統或資料遭輕微竄改。
3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作、關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

（三）符合下列情形之一者，屬二級事件：

1. 核心業務（含關鍵資訊基礎設施）一般資料遭洩漏。
2. 非核心業務系統或資料遭嚴重竄改、核心業務系統或資料遭輕微竄改。
3. 非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作、核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

（四）符合下列情形之一者，屬一級事件：

1. 非核心業務一般資料遭洩漏。
2. 非核心業務系統或資料遭輕微竄改。
3. 非核心業務運作遭影響或系統停頓,於可容忍中斷時間內回復正常運作。

四、 資安人員指派及資訊登錄，應依下列規定辦理：

（一）本部及所屬機關（構）均應設資安長，由機關（構）之副首長兼任(無副首長者由首長指派)，並指派二位以上之資安聯絡人員，本部另需指派資安審核人員。

（二）資安聯絡人員、資安審核人員、資訊主管及本部資安長之相關資訊，均需登錄於國家資通安全通報應變網站（以下簡稱通報應變網站)，如有異動應立即更新。

（三）通報應變網站聯繫資訊如下：

1. 網址：https://www.ncert.nat.gov.tw
2. 聯絡電話：(02) 2733-9922（二十四小時專線電話）
3. 傳真：(02) 2733-1655
4. 電子郵件：service@nccst.nat.gov.tw

五、 資安事件危機通報作業應依下列規定辦理：

（一）本部及所屬機關（構）

1. 通報範圍應包含自建或委外之資通訊系統,及委託民間興建營運後轉移(Build-Operate-Transfer, BOT)之關鍵資訊基礎設施。
2. 發現資安事件後除應循內部程序向上陳報外，並須於一小時內，至通報應變網站登錄資安事件細節、影響等級及支援申請等資訊，並評估該事件是否影響其他政府機關（構）或關鍵資訊基礎設施運作，需橫向通知行政院國家資通安全會報政府資通安全組(以下簡稱行政院會報政府資通安全組）相關分組。
3. 本部所屬機關（構）發生四級、三級資安事件時，應成立臨時之資通安全處理小組，負責執行危機通報及緊急應變處理相關措施。
4. 如因網路或電力中斷等事由，致無法上網填報資安事件，須於發現資安事件後一小時內，與行政院國家資通安全會報技術服務中心(以下簡稱技服中心）聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。
5. 進行資安事件處理，四級、三級事件須於三十六小時內完成復原或損害管制；二級、一級事件須於七十二小時內完成復原或損害管制。
6. 完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件

處理辦法及完成時間。

（二）經濟部資通安全處理小組

1. 經濟部資通安全處理小組在接獲所屬機關（構）通報後，應主動掌握事件狀況、協助所屬機關（構）進行資安事件應變處理，並督導事件處理過程。

2. 經濟部資通安全處理小組須至通報應變網站審核所屬機關（構）資安事件通報，並評估該事件是否影響其他政府機關（構）或關鍵資訊基礎設施運作以及事件影響等級之合理性，視需要申請技術支援。如資安事件屬四級、三級事件，須於通報後二小時內完成審核；二級、一級事件，須於通報後八小時內完成審核。

3. 如資安事件屬四級、三級事件，經濟部資通安全處理小組接獲所屬機關（構）結案申請後，須至通報應變網站審核結案內容，並填寫所配合辦理或規劃相關作業。

六、 本部及所屬機關（構）應主動積極建立資安事件之事前安全防護、事中緊急應變及事後復原作業之具體機制：

（一）事前安全防護

1. 為確保機關組織功能正常運作，依據組織風險評估界定，針對遭遇內部危安（如人為破壞）、外力入侵（如病毒感染、駭客攻擊、非法入侵）、天然災害或重大突發（如水災、火災、地震、資通訊網路系統骨幹中斷）等事件，訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。

2. 應規劃建置資通安全整體防護環境，做好機關（構）及 BOT 廠商內部資料存取控制，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。

3. 應依資通安全防護需要，執行入侵偵測、安全掃描及弱點檢測等安全檢測工作，並訂定系統與資料備份管理規定，以做好事前防禦準備。

4. 制訂資通安全管理政策、制度及作業規範等相關措施，定期實施安全檢測、網路監控、人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。

5. 應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核工作項目，定期實施內部稽核。

6. 應保留資安紀錄與備份,如資訊系統屬委外(含 BOT)建置管理者，應於合約內要求承商保留相關資安紀錄。

7. 應依資訊系統分級相關作業規定，判定資訊系統安全與防護等級，

並據以落實資安防護基準。

8. 應每年定期規劃辦理資安認知教育訓練。

9. 無論自建或委外資安監控（Security Operation Center, SOC）服務，應配合建立監控情蒐傳送機制，定期傳送技服中心。

10. 應建置並保存相關設備之系統日誌。

（二）事中緊急應變

1. 資安業務承辦人於接獲技服中心及各單位所屬 SOC 監控中心之資安事件通報時，應依本作業處理程序第五點規定辦理。

2. 於接獲技服中心之共通性資安警訊通告，應就有關資安建議防護措施配合落實與防範，並請單位主管加強控管，直到矯正及預防措施完成為止；若有需要應轉知各同仁提高警覺。

3. 應將技服中心發布之中繼站黑名單於DNS伺服器或防火牆等設備攔阻，並監控是否有異常連線紀錄，納入上述資安事件通報流程管控處理暨追蹤。

4. 於執行即時偵防、監測預警工作時，可藉由二十四小時之監測機制或透過經濟部資通安全處理小組危機通告等方式，以掌握最新的預警訊息，並適時對單位內發布警告訊息及控制發展趨勢，以降低受損程度。

5. 資安事件緊急應變措施如下：

(1) 應就資通安全危害事件之徵兆，查明事件原因、安全等級區分、判定可能影響範圍、評估可能損失、判斷是否需要申請支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。

(2) 可透過查詢通報應變網站、系統弱點（病毒）資料庫或聯絡技術支援單位（或廠商）等方式，尋求解決方案（如下載漏洞修補程式、解毒程式等），如無法解決，應迅速向經濟部資通安全處理小組或技服中心反應，請求提供相關技術支援。

(3) 依既定之緊急應變計畫，實施災害緊急應變搶修處置（如保護、救援、回復運轉等），並持續性監控與追蹤管制。

(4) 視資安事件損壞程度，遵循單位內部及 BOT 廠商備份管理規定，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。

(5) 評估資安事件對業務運作造成之衝擊，並進行損害管制。

(6) 資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工作，以聯繫檢警調單位協助偵查。

(7)如發生重大(四級、三級)資安事件，應主動提供相關設備系統日誌予技服中心，利其提供本部及所屬機關（構）相關協助。

6. 資安事件分類應變步驟如下：

(1)內部危安事件：

發現（或疑似）遭人為惡意破壞毀損、作業不慎等危安事件時，應迅速查明事件影響狀況、受損程度等，啟用備份資料、程式或啟動備援計畫相關措施，以期儘速回復正常運作。

(2)外力入侵事件：

A.病毒感染事件：病毒入侵後，隨時掌握電腦病毒感染最新動態，隔離病毒避免疫情擴散；同時儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。

B.駭客攻擊（或非法入侵）事件：

(a)發現（或）被入侵時，立即隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並迅速啟動備援系統或程序。

(b)如入侵者已被嚴密監控暨不危害內部（含ＤＭＺ非軍事區）網路安全時，可考慮讓入侵者作有條件的連接，適度允許其繼續動作，並請求技服中心協助追查入侵者 IP 位置；並利用稽核檔案或系統指令、聯合ＩＳＰ公司等方式，追蹤入侵者行蹤。惟一旦入侵者危害到內部（含ＤＭＺ非軍事區）網路安全，則應立即切斷入侵者之實體連線。

(c)全面檢討網路安全措施、修補安全漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情事再度發生。

(d)正式記錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考，並向主管機關或檢警單位反應。

(3)天然災害或重大突發事件：

A.為防備颱風、水災、地震等天然害或火災、爆炸、核子事故、重大建築災害等重大意外事件，應將重要資料採異地存放措施，或儲存於防火保險櫃等設施內，以利爾後系統重置復原。

B.如遇資通訊網路系統骨幹（主幹頻寬）中斷事件，應立即查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶救作業。

（三）事後復原作業

1. 受損單位應速依應變（回復）計畫，實施災後復原重建。

2. 受損單位執行災後復原重建工作，首先應檢驗資通安全環境及硬體設備是否可以正常運作，並執行環境重建、系統復原及掃描作業，其步驟包含軟硬體設備重新取得建置、重置作業系統及應用系統，執行運轉測試等；並俟系統正常運作後即進行安全備份、資料復原等相關事宜。

3. 在完成復原重建工作後，受損單位應將災害應變處置復原過程相關完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制（如建立資安事件資料庫或列入更新解決方案資料庫等），供爾後查考使用。

4. 受損單位如有需要，應保留事件發生之線索，向技服中心或檢警單位申請追蹤鑑識、偵查支援，藉研析稽核紀錄或入侵活動偵測等相關資料，以釐清事件發生的原因與責任。

5. 全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。

6. 資安事件結束後，應彙整事件之歷程概述、損害情形、後續可能影響、應變措施及強化作為等資訊，並提送經濟部資通安全處理小組及行政院會報政府資通安全組檢討，以強化資通安全防護機制。

七、 經濟部資通安全處理小組實施緊急應變作業注意事項：

（一）經濟部資通安全處理小組於接獲四級、三級之資安事件通報時，應陳報召集人及副召集人,並視需要召集各分組及相關單位召開緊急應變會議，處理全盤狀況。

（二）影響等級如為二級、一級或未召開緊急應變會議時，經濟部資通安全處理小組仍應自事件通報開始至應變處置結束期間，全程主動追蹤掌握狀況暨管制回報。

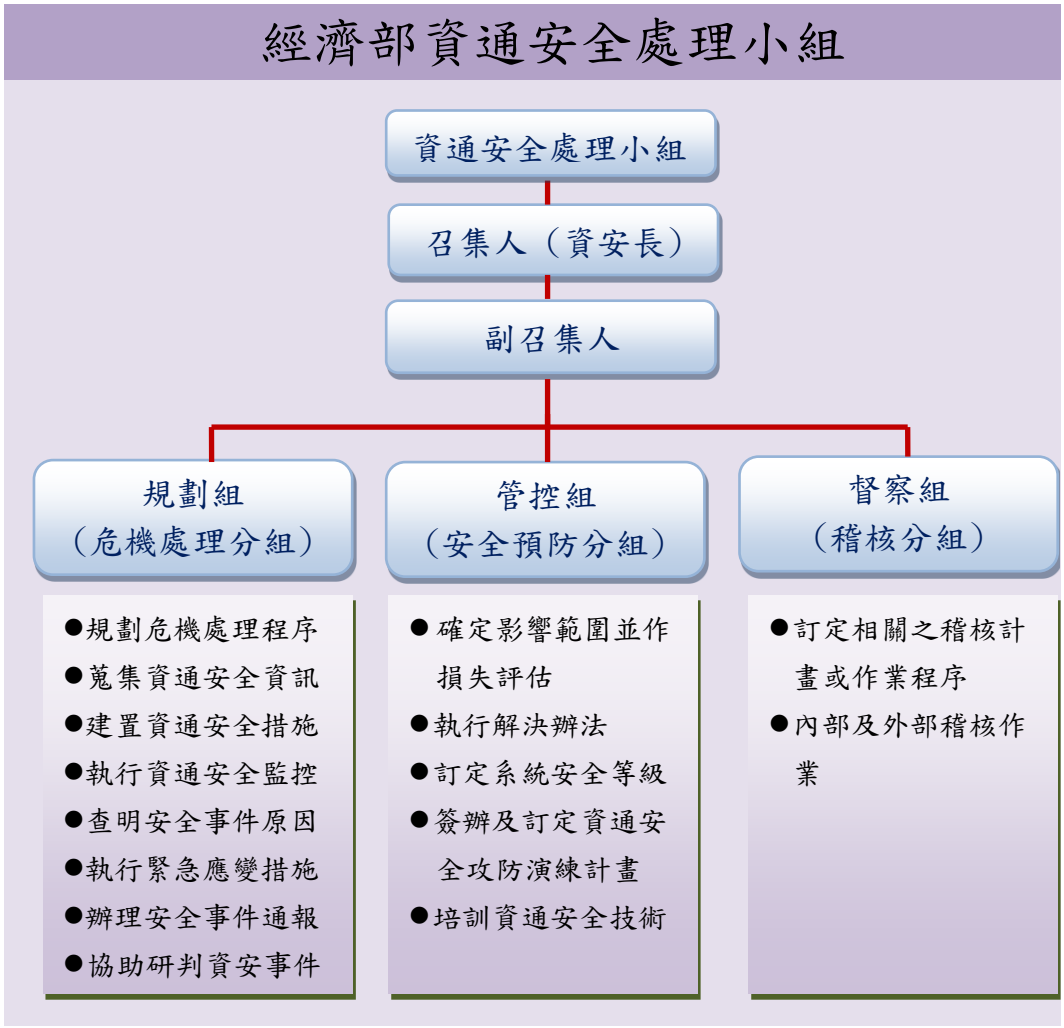
八、 經濟部資通安全處理小組演練作業規定如下：

（一）本部及所屬機關（構）資通安全通報演練：

1. 為檢驗本部及所屬機關(構)之資安通報機制及應變能力,由經濟部資通安全處理小組於每年九月底前辦理完成本部及所屬機關（構）資通安全通報演練作業。

2. 演練程序如下：

(1) 經濟部資通安全處理小組在本項演練作業中，應分組分工執行各項任務。分規劃組（危機處理分組）負責規劃演練之各種模擬狀況及選出演練單位；管控組（安全預防分組）負責通知參演單位及支援處理作業；督察組（稽核分組）負責保管模擬狀況題庫及登錄各階段演練時間，組織架構如下：



(2) 演練計畫應簽奉經濟部資通安全處理小組之召集人（資安長）核定後實施。

(3) 演練實施前，應向本部及所屬機關（構）實施作業說明並知會行政院國家資通安全會報。

(4) 遴選演練對象方式，由經濟部資通安全處理小組之規劃組以無預警隨機方式選取所屬三分之一（含以上）之單位為演練對象。

(5) 演練前經濟部資通安全處理小組之規劃組需事先規劃資安影響等級一級、二級、三級、四級各種模擬演練狀況(至少十種以上)，用隨機選取方式，分配予所選出之參與演練單位，密封交督察組保管。

(6) 各種模擬狀況中，明定該狀況是係由經濟部資通安全處理小組支援解決或須由技服中心支援解決，以檢驗不同流程的處理方式。

(7) 演練完成後將演練成果報告併演練時間紀錄表，於一個月內送行政院會報政府資通安全組備查。

(8) 演練成果報告、演練時間紀錄表及支援處理及回覆單等相關表單請至通報應變網站下載。

（二）本部及所屬機關（構）防範惡意電子郵件社交工程演練：

1. 為提高本部及所屬機關（構）對社交工程防制認知，各機關（構）應每年不定期至少辦理二次(分別於四月及九月底前辦理)防範惡意電子郵件社交工程演練作業。

2. 演練程序如下：

(1) 每次演練須（含）四分之一以上人員具有公務電子郵件人員參與演練。

(2) 演練實施前須訂定演練計畫，簽奉該機關（構）資安長核定。

(3) 完成演練作業後，應召開檢討會議，檢討辦理情形及演練結果；演練報告須經資安長核定，並分別於五月及十月中旬前送經濟部資通安全處理小組彙整。

(4) 經濟部資通安全處理小組須分別於五月及十月底前，將演練成果送行政院會報政府資通安全組備查。

九、 獎懲及減責標準

依行政院會報政府資通安全組主責機關(單位)之建議，對具以下事蹟或情事之一之單位所屬人員予以適度之獎勵或懲處：

（一）獎勵標準

1. 所通報之資安事件資料完整且具時效性，足以警示其他機關（構）及早防範，防止資安事件擴大。

2. 完成資安事件處理後,通報結案時所提供解決辦法,可供其他機關(構)及時採用，防止資安事件擴大。

3. 於資安事件通報後，積極辦理相關回復工作，降低對機關（構）影響程度，績效顯著。

4. 提供技服中心分析之紀錄，有效預防機關(構)內發生資安事件，並可供其他機關(構)事前應對及預防之用。

5. 積極推動資通安全防護及通報至所屬單位，績效卓著。

（二）懲處標準

1. 通報之資安事件資料，經查明不實。

2. 未遵循本作業處理程序落實資安事件通報應變作業及提供資安紀錄等，致國家或社會受有重大損害時，依法追訴行為人涉及湮滅證據等相關刑事責任，另追究行為人、其主責機關（構）資安長及相關人員之行政責任。

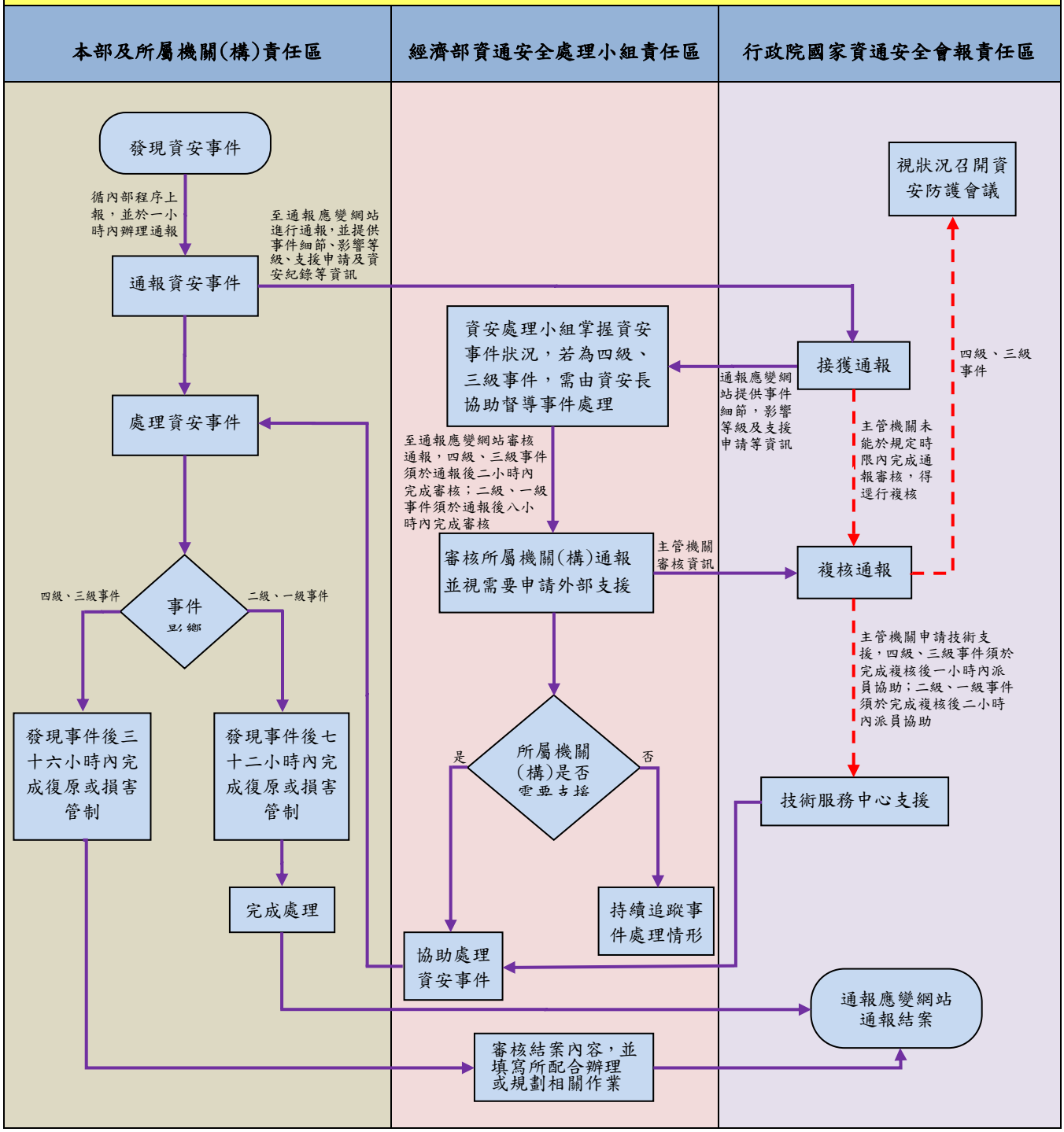
3. 各受委託資安業者未依程序通報，建議解除合約。

（三）減責標準

遵循本作業處理程序規定確實辦理資安事件通報及應變作業並提供資安紀錄，仍致政府或民眾權益受損時，依行政院會報政府資通安全組主責機關(單位)提供之資料減輕其責。

十、 本部及所屬機關（構）資通安全事件通報與應變作業流程詳如附圖。

本部及所屬機關（構）資通安全事件通報及應變作業流程



修正前附件二

經濟部電子資料遭竊事故證物/調查結果報告封存封

事故編號	（同「經濟部資通安全事故調查結果報告」）
封存內容及數量	
封存日期	年　　月　　日
設備使用者	單位： 姓名：
封存人員	
資安通報單 ID	（國家資通安全通報應變作業發配之編號）
資安通報結案日期	年　　月　　日
※封存內容於通報結案作業完成日 2 年後銷毀	

修正前附件三

經濟部資通安全事故調查結果報告

事故說明	
事故編號	(MOEA-AIR-西元年-流水號3碼，流水號每年由001開始累計，AIR：Accident investigation report)
事故發現日期	年　　月　　日　　時　　分
作業人員	
事故描述	
通報單ID	（國家資通安全通報應變作業發配之編號，無則免填）
通報作業日期	通報日期：　　年　　月　　日 通報結案日期：　　年　　月　　日
設備及證物(硬碟)資訊	
設備IP	
設備使用者	
設備Patch狀態	
防毒軟體版本	
證物廠牌	（未保留證物則不需要）
證物型號	（未保留證物則不需要）
證物容量	（未保留證物則不需要）
證物外觀	（證物照片，未保留證物則不需要）
調查暨處理過程描述	
使用工具	調查時使用之軟硬體工具
檢查項目	使用者登入紀錄痕跡、系統機碼分析、文件開啟痕跡、USB使用痕跡、上網痕跡、E-mail痕跡、WebMail痕跡、IM聊天痕跡、軟體使用痕跡、記憶體分析、關鍵字搜尋等
發現狀況說明	遭植入惡意程式、有被打包資料殘留等
疑有資料遭竊	□是　□否
事故原因及手	發生時間分布圖、惡意網路連線關係圖、運用手法及運用系統漏

法分析	洞等
處理作業說明	停用網路服務、清除惡意程式等
惡意程式或工具分析	
檔名	
存在路徑	
建立日期	
修改日期	
存取日期	
擁有者	
檔案大小(Bytes)	
MD5	
防毒軟體掃描結果	
行為描述	
檢討及建議事項	

資料檔案檔名列表					
序號	檔名	檔案大小(Bytes)	建立日期	修改日期	擁有者

修正前附件四

經濟部遭竊電子資料機敏等級評估單

※以下由「資訊中心」填列	
事故編號	
事故發現時間	年　　月　　日
※以下由「資料所屬單位」填列	
填列日期	年　　月　　日
遭竊資料 最高機敏等級	□絕對機密等級公務資料（4級） □極機密等級公務資料（4級） □機密等級公務資料（4級） □密等級公務資料（3級） □敏感等級公務資料（3級） □非屬密級以上或敏感之核心業務資料（2級） □非核心業務資料（1級）
是否已通報政風處	□是　□否
填報人員： 填報人員主管： 填報單位主管：	
本評估單請於資料送達後2日內回擲資訊中心	