經濟部標準檢驗局
資通安全事件通報及應變處理作業程序修正對照表

修正規定	現行規定	說明
一、經濟部標準檢驗局(以下簡稱本局)為確保於發生資通安全事件時，依資通安全管理法(以下簡稱本法)及資通安全事件通報及應變辦法相關規定即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對本局業務之衝擊影響，並確保資通安全事件發生時之跡證保存，特訂定本作業程序。	一、經濟部標準檢驗局(以下簡稱本局)為確保於發生資通安全事件時，依資通安全管理法(以下簡稱本法)及資通安全事件通報及應變辦法相關規定即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對本局業務之衝擊影響，並確保資通安全事件發生時之跡證保存，特訂定本作業程序。	本點未修正。
二、本局資通安全事件通報及應變小組(以下簡稱本小組)於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。 本小組成員代表(如附件一)及任務如下： (一)事件指揮官：為本小組總召集人，綜理全般業務，直接督導各單位聯絡人員及新聞發言人。 (二)新聞發言人：為資通安全事件對外發布新聞或說明之單一窗口，綜整與定期更新訊息。 (三)執行秘書：為事件指揮官幕僚，負責督辦本小組各項業務。 本小組成員由本局資通安全專職人員、資通安全事件通報人員、資訊室相關主管及人員、事件發生單位相關主管及人員與委外廠商組成，得視情況納入政風單位或外部專家等，並視需要申請經濟部派員協助。	二、本局資通安全事件通報及應變小組(以下簡稱通報應變小組)組成如附件一，於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。 通報應變小組各分組代表如附件二，其任務如下： (一)事件指揮官：為通報應變小組總召集人，綜理全般業務，直接督導各單位聯絡人員及新聞發言人。 (二)新聞發言人：為資通安全事件對外發布新聞或說明之單一窗口，綜整與定期更新訊息。 (三)執行秘書：為事件指揮官幕僚，負責督辦通報及應變小組各項業務。 (四)情資及計畫組： 1.本分組負責辦理下列事宜： (1)資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式 IoC(Indicators of Compromise)等。 (2)應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損	一、整併情資及計畫組與應變執行組為本小組，並刪除附件一，原附件二改列附件一，原第四款第二目移列修正規定第三項並修正小組成員。 二、原第四款第一目及第五款之辦理事項合併移列第三點，爰予刪除。 三、其餘酌作文字修正。

	害控制、復原作業及跡證保存計畫。 2.本分組由本局資通安全專職人員、資訊人員、業務單位及委外廠商或外部專家組成，經濟部或相關機關得視情況納入政風單位派員參與，以提供必要之協助。 (五)應變執行組： 1.本分組負責辦理下列事宜： (1)執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。 (2)復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。 (3)跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。 (4)事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。 (5)提出改善建議：依據事件調查根因，提出短、中、長期改善建議。 (6)彙整改善報告。 (7)撰寫調查、處理及改善報告。 (8)追蹤管考：針對機關單位已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。 2.本分組由本局資通安全專職人員、資訊人員、業務單位及委外廠商或外部專家組成，並視需要申請經濟部派員參與，以提供必要之協助。	
三、本小組負責辦理下列事宜： (一)資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡	第二點第四款第一目及第五款 (四)情資及計畫組： 1.本分組負責辦理下列事宜： (1)資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並	序文及第一款與第二款由原第二點第四款第一目移列，第三款至第七款由原第二點第五款第一目之第一次目至第五次目移列，第八款由原第二點第六次目及第七次目合併移列，第九款由原第二點第八

意程式入侵指標 IoC(Indicators of Compromise)等。 (二)應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。 (三)執行損害控制：依據計畫調度人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。 (四)執行復原作業：依據計畫執行系統重建、弱點掃描或漏洞修補等事宜。 (五)跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。 (六)事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。 (七)提出改善建議：依據事件調查根因，提出短、中、長期改善建議。 (八)彙整與撰寫調查、處理及改善報告。 (九)追蹤管考：針對單位已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。	清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式 IoC(Indicators of Compromise)等。 (2)應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。 (五)應變執行組： 1.本分組負責辦理下列事宜： (1)執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。 (2)復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。 (3)跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。 (4)事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。 (5)提出改善建議：依據事件調查根因，提出短、中、長期改善建議。 (6)彙整改善報告。 (7)撰寫調查、處理及改善報告。 (8)追蹤管考：針對機關單位已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。	次目移列，並酌作文字修正。
四、資通安全事件通報及應變程序應包含通報資通安全事件、召開事件應變會議、損害控制或復原作業、事件根因分析及改善追蹤等項目(如附件二)，並依本法施行細則第六條第一項第九款規定納入資通安全維護計畫中，各程序內容如下： (一)通報資通安全事件： 1.本局資通安全事件通報人員	三、資通安全事件通報及應變程序應包含通報資通安全事件、組成通報應變小組與召開事件應變會議、損害控制或復原作業、事件根因分析及改善追蹤等項目(如附件三)，並依本法施行細則第六條第一項第九款規定納入資通安全維護計畫中。 前項各程序如下：	一、點次變更。 二、配合原附件一刪除，原序文附件三改列附件二，為精簡文字，將現行規定第二項併入第一項，另配合情資及計畫組與應變執行組整併，刪除現行規定第二項各款之組別名稱，並酌作文字修正。

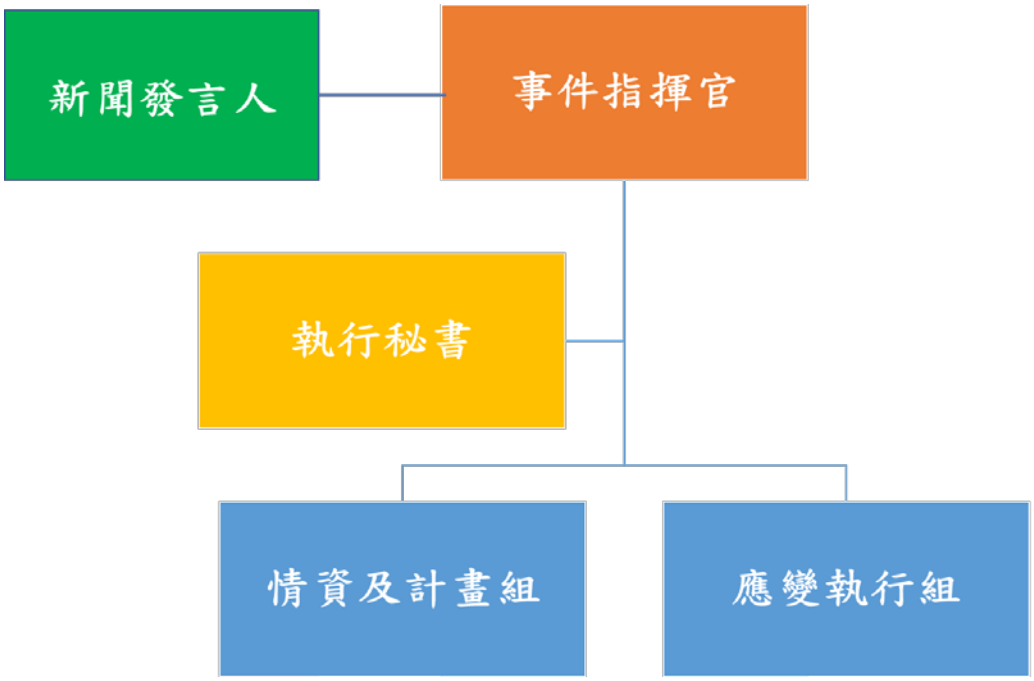
應依本法及資通安全事件通報及應變辦法規定，依主管機關及經濟部指定方式完成事件通報，並通知相關事件處理人員。 2. 第一級或第二級資通安全事件須通知新聞發言人。 3. 第三級或第四級資通安全事件除依前二目規定辦理外；另須填寫「經濟部及轄管機關(構)資通安全事件速報單」通報經濟部。 (二)召開事件應變會議：第三級或第四級資通安全事件應於完成初步損害控制後，召開事件應變會議，會議形式不拘，由事件指揮官主持討論下列事項，並視情況邀請經濟部或主管機關派員出席： 1. 資通安全事件概況。 2. 評估受影響範圍。 3. 其他必要之討論事項。 (三)損害控制或復原作業： 1. 執行損害控制或復原作業，並辦理下列事項： (1)確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。 (2)評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。 (3)於完成損害控制或復原作業後，依主管機關及經濟部指定之方式完成通知作業。 2. 第三級或第四級資通安全事件，除依前目規定辦理外，並應辦理下列事項： (1)定時向事件指揮官及經濟部回報控制措施成效。 (2)倘涉及個人資料外洩，應依個人資料保護法第十二條規定辦理。 (四)事件根因分析：執行事件根因分析，依資通安全事件等級，辦理事項如下：	(一)通報資通安全事件： 1. 本局應依本法及資通安全事件通報及應變辦法規定，由情資及計畫組依主管機關及經濟部指定方式完成事件通報，並通知相關事件處理人員。 2. 第一級或第二級資通安全事件須通知單位新聞發言人。 3. 第三級或第四級資通安全事件除依前二目規定辦理外；另須填寫「經濟部及轄管機關(構)資通安全事件速報單」通報經濟部。 (二)組成通報應變小組與召開事件應變會議：第三級或第四級資通安全事件應於完成初步損害控制後，召開事件應變會議，會議形式不拘，由事件指揮官主持討論下列事項，並視情況邀請經濟部或主管機關派員出席： 1. 資通安全事件概況。 2. 評估受影響範圍。 3. 其他必要之討論事項。 (三)損害控制或復原作業： 1. 由應變執行組執行損害控制或復原作業，並辦理下列事項： (1)確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。 (2)評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。 (3)於完成損害控制或復原作業後，依主管機關及經濟部指定之方式完成通知作業。 2. 第三級或第四級資通安全事件，除依前目規定辦理外，並應辦理下列事項： (1)定時向事件指揮官、通報及應變小組成員及經濟部回報控制措施成效。 (2)倘涉及個人資料外洩，應	

1.除設備故障外，應依第五點規定辦理跡證保存，並督導委外廠商或外部專家進行根因調查，提出紀錄分析；如有發現惡意程式，應提出惡意程式分析。 2.依第五點規定辦理跡證保存時，如發現惡意程式，得請防毒軟體或資安服務公司檢測，並上傳至Virus Check網站(https://viruscheck.tw/)分析，以更新或強化相關偵測及聯防機制，不宜上傳至其他平臺。 3.依據事件調查根因分析結果，本小組應評估短、中、長期資安管理改善策略，其內容如下： (1)短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。 (2)中期：依據事件根因提出三個月至六個月內完成之強化作為，例如盤點老舊設備，並訂定汰換期程。 (3)長期：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如培養本局資安人員能力等。 4.第三級或第四級資通安全事件之調查根因及改善策略應由事件指揮官核定，並由資通安全專職人員彙整送交經濟部。 (五)改善追蹤：進行事件改善追蹤時，得視需要由執行秘書或其授權之人召開會議，並辦理下列事項： 1.評估改善作為期程。 2.評估執行成效，並據以調整改善策略。 3.配合經濟部辦理相關改善作為。 4.由執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善措施為	依個人資料保護法第十二條規定辦理。 (四)事件根因分析：由應變執行組執行事件根因分析，依資通安全事件等級，辦理事項如下： 1.除設備故障外，應依第四點規定辦理跡證保存，並由組長督導委外廠商或外部專家進行根因調查，提出紀錄分析；如有發現惡意程式，應提出惡意程式分析。 2.依第四點規定辦理跡證保存時，如發現惡意程式，得請防毒軟體或資安服務公司檢測，並上傳至Virus Check網站(https://viruscheck.tw/)分析，以更新或強化相關偵測及聯防機制，不宜上傳至其他平臺。 3.依據事件調查根因分析結果，應評估短、中、長期資安管理改善策略，其內容如下： (1)短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。 (2)中期：依據事件根因提出三個月至六個月內完成之強化作為，例如盤點老舊設備，並訂定汰換期程。 (3)長期：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如培養本局資安人員能力等。 4.第三級或第四級資通安全事件，由執行秘書將事件調查根因及改善策略提報事件指揮官核定，並由資通安全專職人員彙整送交經濟部。 (五)改善追蹤：由應變執行組進行事件改善追蹤時，應視需要召開會議，並辦理下列事項： 1.評估改善作為期程。 2.評估執行成效，並據以調整	

止，並由資通安全專職人員彙整送交經濟部。 5. 依主管機關或經濟部指定之方式，送交調查、處理及改善報告；第三級或第四級資通安全事件，應另以密件公文將該報告送交經濟部。 6. 本局送交調查、處理及改善報告後，相關改善事項應納入定期追蹤管考機制。	改善策略。 3. 配合經濟部辦理相關改善作為。 4. 由執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善措施為止，並由資通安全專職人員彙整送交經濟部。 5. 依主管機關或經濟部指定之方式，送交調查、處理及改善報告；第三級或第四級資通安全事件，應另以密件公文將該報告送交經濟部。 6. 本局送交調查、處理及改善報告後，相關改善事項應納入定期追蹤管考機制。	
五、為確保資通安全事件發生時，所保有跡證足以進行事件根因分析，委外辦理資通系統或服務之單位應依資通安全事件等級辦理下列事項，且於資通系統或服務之委外契約中定明紀錄保存及備份規定，並應視事件情形辦理其他必要之跡證保存事項： (一)於日常維運資通系統時，應依附件三保存日誌(log)，並定期備份至與原稽核系統不同之實體系統或外部設備/媒體。 (二)發生資通安全事件時，應依下列原則進行跡證保存： 1. 進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。 2. 若系統無備援機制，應備份受害系統儲存媒介(例如硬碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。 3. 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供	四、跡證保存 為確保資通安全事件發生時，所保有跡證足以進行事件根因分析，應依資通安全事件等級辦理下列事項，並應視事件情形辦理其他必要之跡證保存事項： (一)於日常維運資通系統時，應依附件四保存日誌(log)，並定期備份至與原稽核系統不同之實體系統或外部設備/媒體。 (二)發生資通安全事件時，應依下列原則進行跡證保存： 1. 進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。 2. 若系統無備援機制，應備份受害系統儲存媒介(例如硬碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。 3. 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。 4. 若備援設備亦為受害範圍，	一、點次變更。 二、現行規定第三款修正移列納入序文，並酌作文字修正。 三、配合原附件一刪除，第一款原附件四改列附件三。

服務。 4. 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。	於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。 (三)於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中定明紀錄保存及備份規定。	

附件一、資通安全事件通報及應變小組組成(修正前)

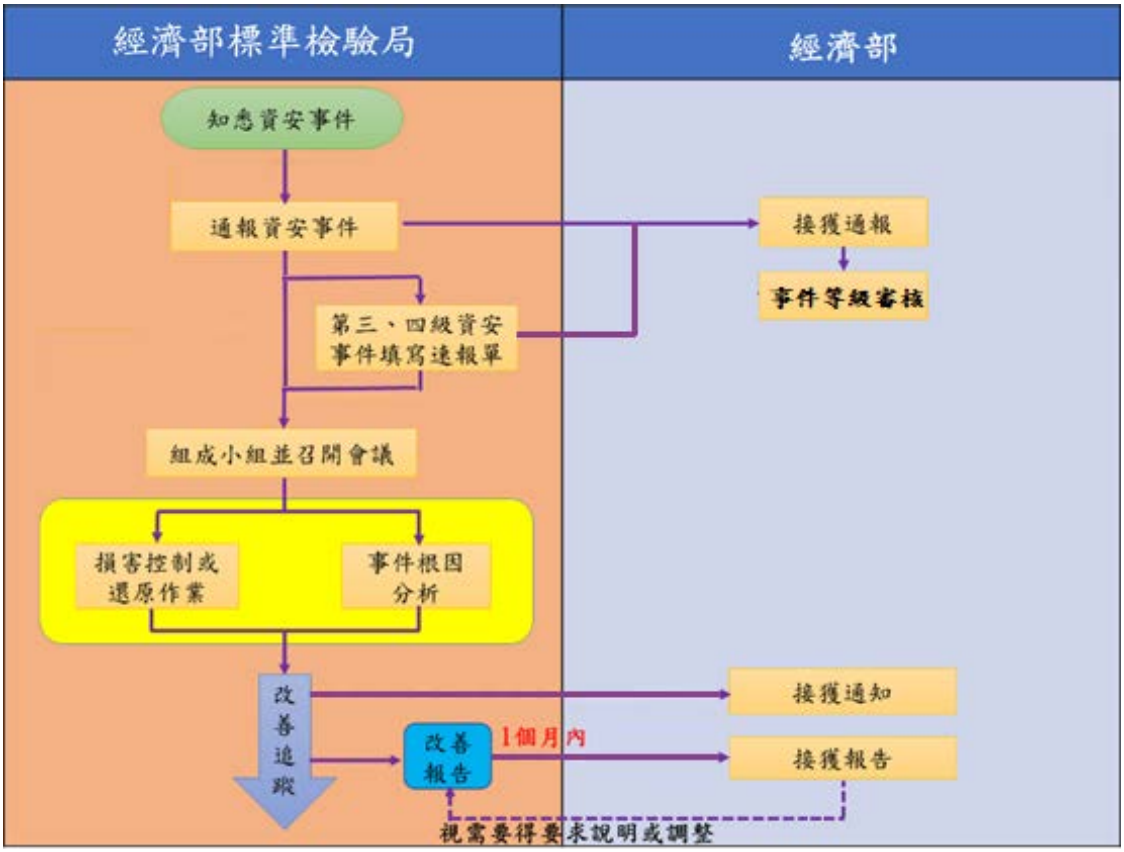


附件二、資通安全事件通報及應變小組各分組代表(修正前)

	第一級、第二級 資通安全事件	第三級、第四級 資通安全事件
事件指揮官	資訊室主任	資通安全長
新聞發言人	資訊室主任	資訊室主任
執行秘書	資訊室第二科科長	資訊室主任
情資及計畫組組長	資訊室第二科科長	資訊室第二科科長
應變執行組組長	事件發生單位之 權責主管(註)	資訊室第二科科長

註：權責主管係指維運(護)資通系統或設備管理單位之主管人員

附件三、資通安全事件通報及應變程序(修正前)



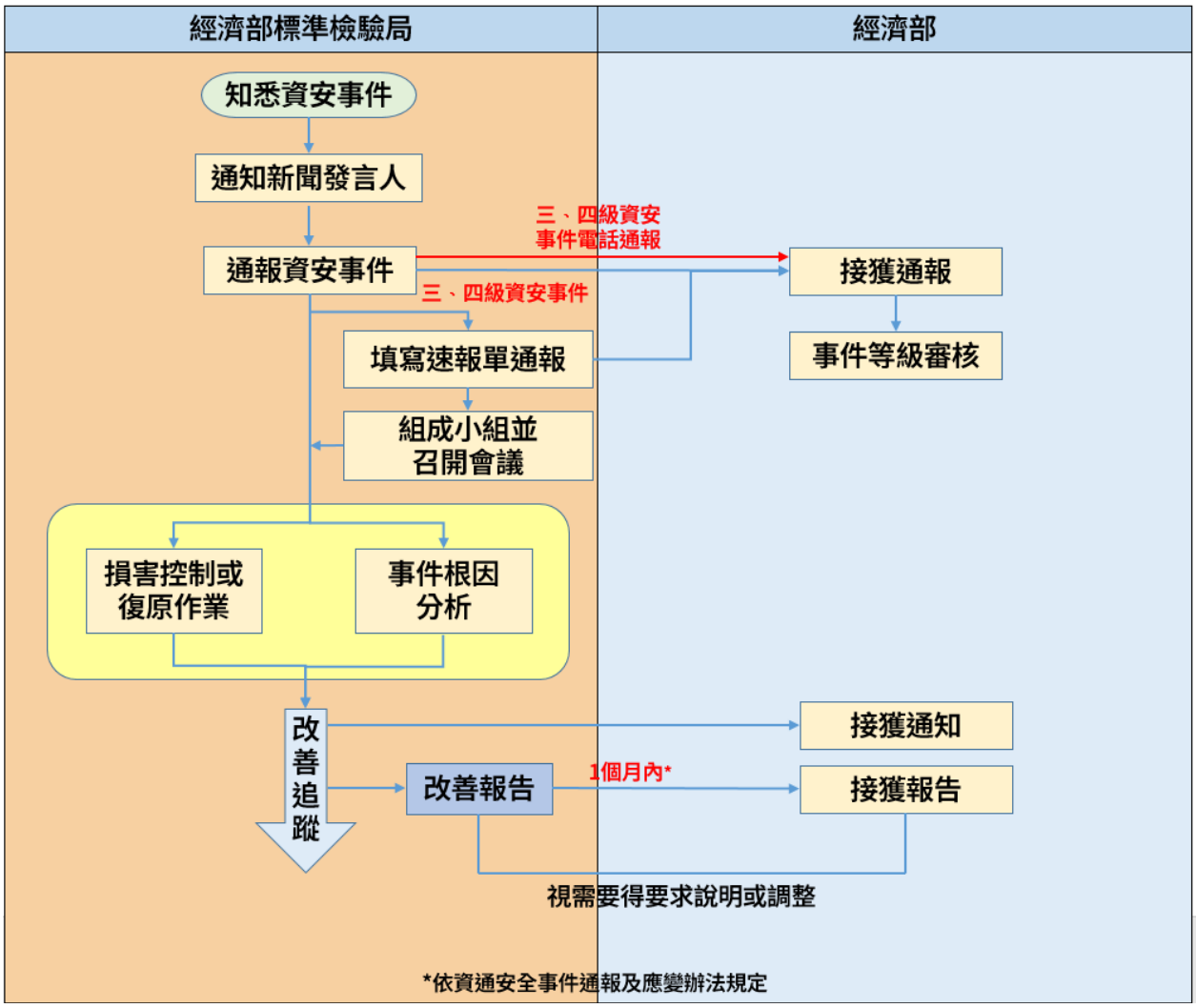
附件四、日誌保存範圍及項目(修正前)

保存範圍	保存項目
全部核心資通系統最近六個月之日誌紀錄。	1.作業系統日誌(OS event log) 2.網站日誌(Web log) 3.應用程式日誌(AP log) 4.登入日誌(Logon log)

附件一、資通安全事件通報及應變小組代表(修正後)

	第一級、第二級 資通安全事件	第三級、第四級 資通安全事件
事件指揮官	資訊室主任	資通安全長
新聞發言人	資訊室主任	資訊室主任
執行秘書	資訊室資通服務科科長	資訊室簡任技正

附件二、資通安全事件通報及應變程序(修正後)



附件三、日誌保存範圍及項目(修正後)

保存範圍	保存項目
資通系統最近六個月之日誌紀錄。	作業系統日誌(OS event log) 網站日誌(Web log) 應用程式日誌(AP log) 登入日誌(Logon log)