行政院農業委員會水產試驗所處理資通安全事件危機通報及緊急應變作業注意事項

91.10.08 行政院農業委員會農企字第 0910156761 號函同意備查

壹、 依據九十一年八月一日行政院國家資通安全會報「各機關處理資通安全事件危機通報緊急應變作業注意事項」及本所「資通安全處理小組設置要點」、「資訊安全管理作業規範」辦理。

貳、 行政院農業委員會水產試驗所（以下簡稱「本所」）為有效掌握資訊、通訊及網路系統遭受破壞、不當使用等危安或重大災害事件，能迅速通報及緊急應變處置，並在最短時間內回復，以確保公務之正常運作，特訂定本注意事項。本注意事項所稱「各單位」係指本所各組、室、研究中心。

參、 資通安全事件等級概分為四級：

「Ａ」級：影響公共安全、社會秩序、人民生命財產。

「Ｂ」級：系統停頓，業務無法運作。

「Ｃ」級：業務中斷，影響系統效率。

「Ｄ」級：業務短暫停頓，可立即修復。

肆、 資通安全事件危機通報作業注意事項：

一、 各單位應依本所「資通安全處理小組設置要點」之規定，指定資通安全危機通報聯絡人。本所企劃資訊組應彙整建立通報聯絡網人員名冊，並提報上級督導。

二、 各單位資通安全事件影響層面如災害重大，且影響層面深廣、受損程度嚴重時（如外力入侵、資通訊網路系統骨幹中斷重大突發事件等，或水、火災、地震、天然災害等涉及資通安全事件者），應儘速向本所「資通安全處理小組」通報，並轉呈上級機關。如屬一般性，僅涉及單位內、受損程度輕微時（如非伺服器、非重要系統之電腦病毒感染，且無公務資料之毀損），可由各單位自行處置，無須通報，但仍須由各單位資通安全聯絡人以通報單建檔備查。

三、 資通安全事件危機通報作業程序如下：

（一）各單位資訊或通信系統用戶端於發生危安事故時，於三十分鐘內向本所「資通安全處理小組」反應事實或請求支援，完成內部通報流程。本所「資通安全處理小組」可由上網或資料庫等查詢方式，尋求解決方案，並儘速協助用戶端進行緊急應變處置。

（二）本所「資通安全處理小組」於發生內部危安事故時，應將事件發生之事實、可能影響之範圍、損失評估、判斷支援申請、採取之應變措施等事項，於三十分鐘內填具「資通安全事件通報單」，通報至上級單位尋求技術支援，以迅速解決狀況，並降低資安事件之危害。

（三）各單位如遇資通安全事件，危及人員生命或硬體設備遭到破壞等涉及民、刑事案件時，除向本所「資通安全處理小組」通報外，並應即時向檢調單位報案，請求處理。

（四）有關通報單之災害損失評估內容應包括如下項目：作業影響情況、設備或系統損

害情況、作業延誤情況、資料受損項目、估算資通訊系統作業及資料回復所需時間、備援中心設備及人員支援狀況等。

伍、 資通安全事件緊急應變作業注意事項：

各單位應主動積極建立事前安全防護、事中預警應變、事後復原鑑識等機制。並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，編製各重要伺服器系統、行政業務或研究應用系統之預防、緊急應變暨處置復原作業程序手冊，並須演練測試無誤。

一、 事前建置安全防護機制：

（一）各單位應參照「行政院及所屬各機關資訊安全管理要點、管理規範」並依本所「資訊安全管理作業規範」，規劃建置資通系統或網路安全整體防護環境，如儲備必要之備份資料、程式或異地備援、極重要及重要文件資料檔案應採取加密方式儲存或實體隔離等防護工具或措施，並定期實施自我評審及接受外部安全稽核。而具管理獨立網域網路之單位尤應注意網路系統存取控管機制、連線紀錄資料庫、建構防火牆軟硬體、虛擬私人網路（VPN）、病毒掃描機制、身分認證授權、資料加解密、電子簽章、入侵偵測系統(IDS)、外部弱點掃描、頻寬管理、系統內部安全漏洞檢測暨資料庫建立、電磁脈衝防護、定期網路監控、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。

（二）本所企劃資訊組應針對前述各單位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，期儘早發現系統安全漏洞暨完成修復補強。

（三）各具管理獨立網域網路之單位可依資通安全防護需要，聯絡本所企劃資訊組協調「行政院國家資通安全會報」所屬技服中心支援執行入侵偵測、安全掃瞄、漏洞檢測修復等安全體檢工作，以做好事前防禦準備。平時並應建立緊急狀況時，可提供諮詢及可於二小時內迅速到達現場協助處理之相關資安廠商聯絡資料。

（四）各具管理獨立網域網路之單位可考慮本身業務需求，規劃建置資通訊網路系統骨幹實體備援能量及緊急應變機制，期於資通訊網路系統中斷時，得立即啟動緊急備援機制，儘速回復正常運作。

二、 事中主動預警緊急應變：

（一）本所企劃資訊組應依「資通安全通報聯絡網」即時轉知各單位由「行政院國家資通安全會報」危機通報分組所發出之「資通安全危害通告資訊（如最新電腦病毒疫情、漏洞、弱點及駭客攻擊等）之預警訊息、防範須知或解決方案」，妥採因應作為，並加強防範措施。

（二）各單位執行即時偵防、監測預警工作時，可藉由監測工具（如入侵偵測系統 IDS 等）或危機通告資訊等方式，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。

（三）資通安全事件緊急應變措施如下：

1 各單位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、判斷是否需要支援申請等作業項目逐一檢討與處置，並

保留被入侵或破壞等證據（如網頁置換等）。

2 透過系統弱點（病毒）資料庫、上網站、技術支援單位（或廠商）等方式，查詢獲得解決方案（如下載漏洞修補程式、解毒程式等）；或依既定之緊急應變程序，實施災害緊急應變搶修處置（如保護、救援、回復運轉、備援程序等），並持續性主動積極之監控與追蹤管制。

3 如屬無法解決之危害事件，應迅速向本所企劃資訊組（或呈轉「行政院國家資通安全會報」危機通報分組）反映，請求提供相關技術支援。

4 執行其他災害應變及防止事件擴大之措施。

（四）資通安全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、作業不甚等危安事件時，應迅速查明事件影響狀況、受損程度等，啟用備分資料、程式或啟動備援程序相關措施，期儘速回復正常運作。

2 外力入侵事件：

(1)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。

(2)駭客攻擊（或非法入侵）事件：應依本所「資訊安全管理作業規範」中之【陸、網路安全管理】條、【四、各網域遭受網路入侵之處理】款處置。

3 天然災害或重大突發事件：

(1)如遇颱風、水災、地震等天然災害或火災、爆炸、核子事故、重大建築災害等重大意外事件，應迅速攜帶重要資料及程式等離開現場，或儲存於防火保險櫃等設施內，以利爾後系統重置復原。

(2)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，執行搶修作業。

三、事後復原追蹤鑑識偵查：

（一）受損單位速依已建立之各系統緊急應變暨處置復原作業程序，實施災後復原，重建各重要伺服器系統、行政業務或研究應用系統。

（二）受損單位執行災後復原工作，首先檢驗資通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，以及運轉測試等：並俟運作正常後即進行安全備份檔案下載、資料回復、資料重置等相關事宜。

（三）當危機解除後，受損單位應將災害應變處置復原過程相關完整紀錄（如事件原因分析及檢討改善方案、解決方案、稽核軌跡及蒐集分析相關證據等資料），予以建檔管制，以利爾後查考使用。

（四）受損單位如有需要，應保留事件發生之線索，向本所企劃資訊組轉請「行政院國家資通安全會報」技術服務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：並找出防護

系統之漏洞，尋求補強保護方法，避免事件再度發生。

陸、 本所「資通安全處理小組」實施緊急應變作業注意事項：

一、 本所「資通安全處理小組」除於平時依行政體制運作外，緊急狀況通報應變或重點任務需要時由企劃資訊組負責籌劃運作，視需要邀集相關單位參與緊急應變會議，並隨時掌握各單位重要資通網路之安全狀況及採取緊急應變處置事宜。

二、 影響等級「Ｂ」級（含）以下時，由「資通安全處理小組」執行秘書視其影響程度負責簽報副召集人處理，並依需要由副召集人召集各相關單位召開緊急應變會議處理全般狀況。

三、 通報影響等級達到「Ａ」級時，由應變中心副召集人立即通報召集人，並即刻召集「資通安全處理小組」成員召開緊急應變會議處理全般狀況。企劃資訊組應於接獲通知後，於二小時內聯繫相關資安廠商列席或向「行政院國家資通安全會報」技術服務中心請求技術服務支援，以執行資通安全事件應變處置相關事宜。資安危機發生之單位主管視需要留守督導單位內危機之處理，可免於親身參與緊急應變會議，但應隨時與會議保持聯繫狀態，並提報災損最新狀況；而單位資安危機聯絡人應即時聯繫最近相關資安廠商到達現場協助處理，期於最短時間內回復系統正常運作。緊急應變會議應持續召開，直至危機解除，並須隨時通報上級機關追蹤管制。

四、 影響等級如為「Ｃ」、「Ｄ」級或未召開緊急應變會議時，企劃資訊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。

五、 企劃資訊組於事件結束後，應主動蒐整事件之處置過程紀錄、解決方案、資料存檔管制或爾後應加強之防範措施等資訊，送交各相關單位參考改善，以加強資通安全防護機制。

柒、 其他未定事項以行政院國家資通安全會報「各機關處理資通安全事件危機通報緊急應變作業注意事項」及相關規定規範之。