電腦機房緊急應變計畫

壹、依據

由於資訊通訊與網路科技的日益發達，及電子化政府之推動，本案各項業務對於網路及資訊電腦作業之依賴情況亦不容許發生長期電腦作業中斷之狀況，為使本案電腦機房之資訊作業在發生天災或人為破壞後，能依序採取緊急應變措施，儘速回復各項電腦作業，以維持本案業務之運作。

貳、目標

一、確保本案電腦機房人員、設備與資通訊及資料安全。

二、於災害發生時之及時補救及災害發生後緊急復原，以減輕天然或人為災害所造成之損失。

參、範圍

一、電腦機房所屬人員、設備及各應用系統及資料。

二、本案及各系統進駐電腦機房之設備。

三、本案對外提供服務民眾之各項設備。

肆、組織權責劃分

一、 電腦機房應依任務分配，指派人員各自負責其管理之各項資訊設備及相關之資訊安全以確保資料不被破壞或盜取，系統主管應負起機房設備安全監督之責。

二、 資通安全處理小組負責接受資安事件通報，彙整分析向上陳報，並追蹤稽核改善措施。

伍、機房環境監控及資料備份與存放（災前預防）

一、機房須配置不斷電系統(UPS)，並定期實施保養，以便於斷電或臨時跳電時暫時供應電源,避免因瞬間停電導致系統不正常關機進而造成資料及系統損毀。

二、電腦機房有關之消防設備之操作使用，應派員參加每年消防局舉辦之相關教育訓練，以熟悉操作使用方法。

三、機房值班人員應檢測機房內消防設備之使用期限，並協請管理單位派專業人員定期檢測。

四、本電腦機房值班人員每天應進行機房環境檢查及相關資料之備份工作，並依據「電腦機房管理作業要點」填具「電腦機房每日檢點表」、「電腦伺服器備援紀錄表」，並基於資料保存與安全需要將該備份媒體置於指定地點作異地

存放。

五、如發生主機資料毀損則須進行資料回復工作，並配合各應用系統需要將備份資料回存。

陸、緊急應變（災時應變）

二、 人為破壞應變

（一）人員闖入

1.機房設有門禁管制，如遇有陌生人員擅自闖入機房，應即刻予以查問其來意，引導至正確場所洽辦。

駭客入侵

2.如有來意不善人員闖入，則應通報系統主管並立刻轉請管理人員前來處理。

（二）網路入侵

1.各系統主機重要資料平時應做好備份工作，如發現有駭客侵入，應立即填具資通安全事件通報單向本案資通安全處理小組發出通報並將該主機先行隔離，隨即展開執行檢查與回復作業；事後應即時檢討改進並將處理情況填具資通安全事件解除通報單逐級陳報。

2.電腦機房值班人員得運用相關網路稽核軟體不定期監控網路使用概況，遇有疑似駭客入侵，應立即報告系統主管並填具資通安全事件通報單向本案資通安全處理小組發出通報，且得配合相關工具予以監控、追綜、查察，必要時得以予以斷訊，並針對受入侵主機採取相關之檢查措施如系統與資料已遭竄改則除須保留入侵證據外，事後應依災後復原程序辦理回復工作，檢討改進並將處理情況填具資通安全事件解除通報單逐級陳報。

（三）病毒風暴

1.如因病毒事件造成網路風暴，應立即運用本案購置防毒軟體或至相關防毒網站下載最新病毒碼進行解毒處理並做好相關系統漏洞之修補，以設法排除網路障礙恢復正常。

2.如無法自行排除應緊急與廠商連繫尋求支援。

3.進行相關資通安全事件通報作業。

三、停電時緊急應變

（一）因 UPS 可供之電源有限，值班人員應於停電前（若須長時間停電）或發現停電時（估算所需停電時間），以正常程序將主機關閉，待來電時再將主機開啟。

（二）若台電將於下班期間限電，因 UPS 可供應之電源有限，故除有特殊任務而無法關機之伺服器或網路設備外，其餘應於下班前關閉，隔日上班時再行開機。

（三）因台電停電而造成機房空調系統無法運作，則須將機房門窗打開保持空氣流暢以降低溫度，俟台電恢復供電後關閉門窗並啟動空調系統。

設備當機

四、一般當機及服務中斷之應變

（一）主機及其他設備當機或中斷服務：

1.如屬硬體問題則設法排除問題，再重新開機；如屬應用系統問題則需會同業務權責系統及廠商處理。

2.與使用系統連繫，告知當機情況及預定修復時刻。

3.視事件影響程度得進行資通安全事件通報作業。

（二）網際網路服務中斷：

1.查明網路中斷處並設法排除問題。

2.如屬政府服務網路(GSN)或其他網際網路中斷，應積極聯繫中華電信促其儘速修復。

3.與使用系統連繫，告知中斷情況及預定修復時刻。

4. 視事件影響程度得進行資通安全事件通報作業。

五、針對以上之應變，各系統所屬機房須成立任務編組以依序因應處理緊急事件。

六、緊急應變處理過程中，對外一切資訊之發佈應指定專人負責，他人不得擅自為之。

具體防範與應變處理設施

柒、軟硬體之修復與資料回復（災後重建）

一、如有上開災變發生，短期間資訊設備當機或資料漏失無法回復正常，各業務系統負責人員應洽各業務系統相關作業人員，改採人工處理程序辦理，並將人工表單資料妥善保存，以供修復完畢後補正資料之需。

二、災害發生過後，應先行檢測主機系統及硬體受損程度並依下列程序處理：

（一）由本案各系統負責人員研判故障類型，並先行設法排除，如無法解決時，應詳細記錄當時狀況及顯示之訊息後，立即就故障問題通知相關人員及維護廠商前來維修。

（二）如主機硬體嚴重受損時，應與維修人員連絡，並詳述損壞情形，以減少維修人員修復之時間，並於最短時間內回復硬體設備，如短時間無法回復硬體設備時，應協調商借主機暫時使用。

（三）如遇系統受損或資料毀損無法回復時，應由平時備份之磁帶中回復資料，將損壞減低到最小之程度。

（四）如逾一小時無法修復時，應廣播通知各系統，並督促相關廠商儘快修復。

（五）系統修復完畢後應提出資通安全事件解除通報單核判。

三、回復時間視資料或設備毀損情況而定，概分下列幾種情況：

（一）資料檔案輕微損害：作部份回存，約需幾分鐘至半小時。

（二）資料檔案嚴重毀損：作全部回存，約需一至二小時。

（三）機器硬體設備受損：視損害情形，約半小時至十二小時。

（四）單一機器設備全毀：需安裝新機（含軟硬體）並回儲備份資料，約需兩天。

（五）機房重建：包括安裝軟硬體及通訊設備，需一星期以上。

四、設備與資料恢復正常後應盡快通知相關作業人員，檢查並補正漏失資料以便繼續作業，以免影響居住及參建系統之績效。

捌、狀況通報

一、電腦機房主機之操作，如有安全異常事件除由值班操作員及時處理並向上反映外，視影響程度得依「資通安全處理小組作業手冊」規定之程序

向本案管理系統資訊安全處理小組通報。

二、資通安全處理小組接獲通報，應協助處理或監控系統廠商轉通報請求支援協助。

玖、演練

本計畫之緊急應變措施，至少每年應選定狀況舉辦一次演練，並檢討演練結果作為改善參考。

拾、附則：

本計畫奉核定後實施，如有未盡事宜，得以補充並公佈。