高雄市政府法制局資通安全事件緊急應變作業計畫

一、目的：

為掌握本局之資通設備及網路系統遭受破壞、不當使用等危安或重大災害事件，並能迅速通報及有效緊急應變處理，在最短時間內回復，以確保業務正常運作。

二、依據：

高雄市政府九十一年八月二十三日高市府主資字第〇九一〇〇三九一八四號書函辦理。

三、本緊急應變對象及時機：

（一）對象：本局資通訊及網路系統，進行電子化作業之所有人員。

（二）時機：本處於發生重大資通安全事件或其他災害涉及資通安全事件時，應立即依本計畫辦理。

四、組織：

為有效處理緊急事件，特設置「高雄市政府法制局資通安全處理小組」（以下簡稱「處理小組」），由本局主任秘書、專門委員及各科（室）主管組成，主任秘書擔任召集人、專門委員擔任副召集人，秘書室負責處理相關作業。

五、資通安全事件等級分為四級：

『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。

六、資通安全事件危機防護機制作業處理程序如下：

（一）事前安全防護機制作業處理程序：

1.定期備份資料：本處網站、公文系統及人事管理資訊系統定期備份資料，避免人為或外力之破壞。

2.管制密碼使用：本處各項系統之密碼由專人管理維護，定期變更設定密碼，人員異動時必須交接並更新密碼。

3.配備專屬位址：各項網路資訊設備，配備專屬網際網路位址(IP address)，不可重複或共用，並由專人維護保管。

4.強化防毒措施：定期更新防毒軟體病毒碼及執行掃毒程式，避免系統因中毒而癱瘓整體作業。

5.宣導資通安全：定期宣導資通安全常識，加強防毒及防止駭客入侵觀念，維護本處資通安全。

（二）事中安全防護機制作業處理程序： 依「資通安全事件等級」及「入侵管道分類」採行處理程序。

1.依「資通安全事件等級」採行處理程序：

(1)等級『A』、『B』級：立即陳報本府資通安全處理小組並請求本府資訊中心協助處置，啓動本處處理小組採行應變措施。

(2)等級『C』級：啓動本處處理小組採行應變措施，於最短時間內排除問題恢復業務作業。

(3)等級『D』級：由承辦科（四科）儘速排除問題。

2.依「入侵管道分類」採行處理程序：

(1)內部危安事件：發現（或疑似）遭人爲惡意破壞毀損、作業不慎等危安事件時，迅速查明事件影響狀況、受損程度等，啓用事前備分資料、程式或啓動備援計畫相關措施，儘速回復正常運作。

(2)外力入侵事件：

A、病毒感染事件：遭受病毒入侵後，立刻中斷受感染之設備，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：發現（或）被入侵時，立即中斷本處網路之實體連線，拒絕入侵者任何存取動作，修補安全漏洞定等具體改善補救措施；若爲本處網站者，立刻通知本府資訊中心（本局網站係建置於本府網站公用主機）協助排除。

（三）事後安全防護機制作業處理程序：

1.首先檢驗資通安全環境及硬體設備是否可以正常運作，並執行系統復原及掃描作業，並俟運作正常後即進行安全備份檔案事宜。

2.當危機解除後，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、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。

3.如有需要應保留事件發生之線索，向本府資通安全處理小組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。