臺北市政府資通安全事件通報及應變作業程序

總說明

為規範本府各機關在資通安全事件發生後之通報及應變機制，迅速完成損害及控制作業，降低資通安全事件對各機關業務之衝擊影響，本府原訂有「臺北市政府資通安全事件通報及應變作業指引」，現為持續精進相關規範，特訂定本作業程序；本作業程序共計四十一點，其重點如下:

一、 明定本作業程序訂定目的。(第一點)

二、 明定本作業程序相關之適用對象。(第二點)

三、 明定本作業程序相關之名詞定義。(第三點)

四、 明定各機關資通安全事件通報及應變程序應包含之項目。(第四點)

五、 明定各機關應指定資通安全事件通報窗口。(第五點至第九點)

六、 明定各機關知悉資通安全事件發生時應辦理事項。(第十點至第十四點)

七、 明定資訊局應於法規時限內，完成資通安全事件等級審核。(第十五點至第十六點)

八、 明定各機關若須變更資通安全事件等級，應於資通安全署國家通報應變網站提出申請。(第十七點)

九、 明定各機關知悉資通安全事件後，應完成資通安全事件通報及應變小組組成與應變會議召開。(第十八點至第二十點)

十、 明定各機關於知悉資通安全事件後，應於時限內完成損害控制或復原作業，並於資通安全署國家通報應變網站完成通知或登錄。(第二十一點至第二十三點)

十一、明定各機關於日常維運資通系統時，應保存之日誌紀錄與留存時間，並於知悉資通安全事件後，跡證保存應採行之原則。(第二十四點至第二十六點)

十二、明定各機關應保存跡證與資通安全事件調查後之辦理事項。(第二十七點至第三十點)

十三、明定各機關進行事件改善追蹤時，應視需要召開會議之相關辦理事項。(第三十一點)

十四、明定各機關應留存資通安全事件之相關紀錄，並依實際處理情形，於必要時對相關配置進行調整。(第三十二點至第三十三點)

十五、明定各機關於處理資通安全事件時，應依數位發展部資通安全署與本府規定進行情資分享。(第三十四點)

十六、明定各機關應依本府規定參與或自行辦理社交工程演練。（第三十五點至第三十六點）

十七、明定各機關應配合本府辦理之資通安全事件通報及應變演練。（第三十七點至第四十點）

十八、明定學校仍應遵循本作業程序第六點至第九點、第十二點至第十四點、第二十三點第二款、第二十四點至第二十六點規定。（第四十一點）