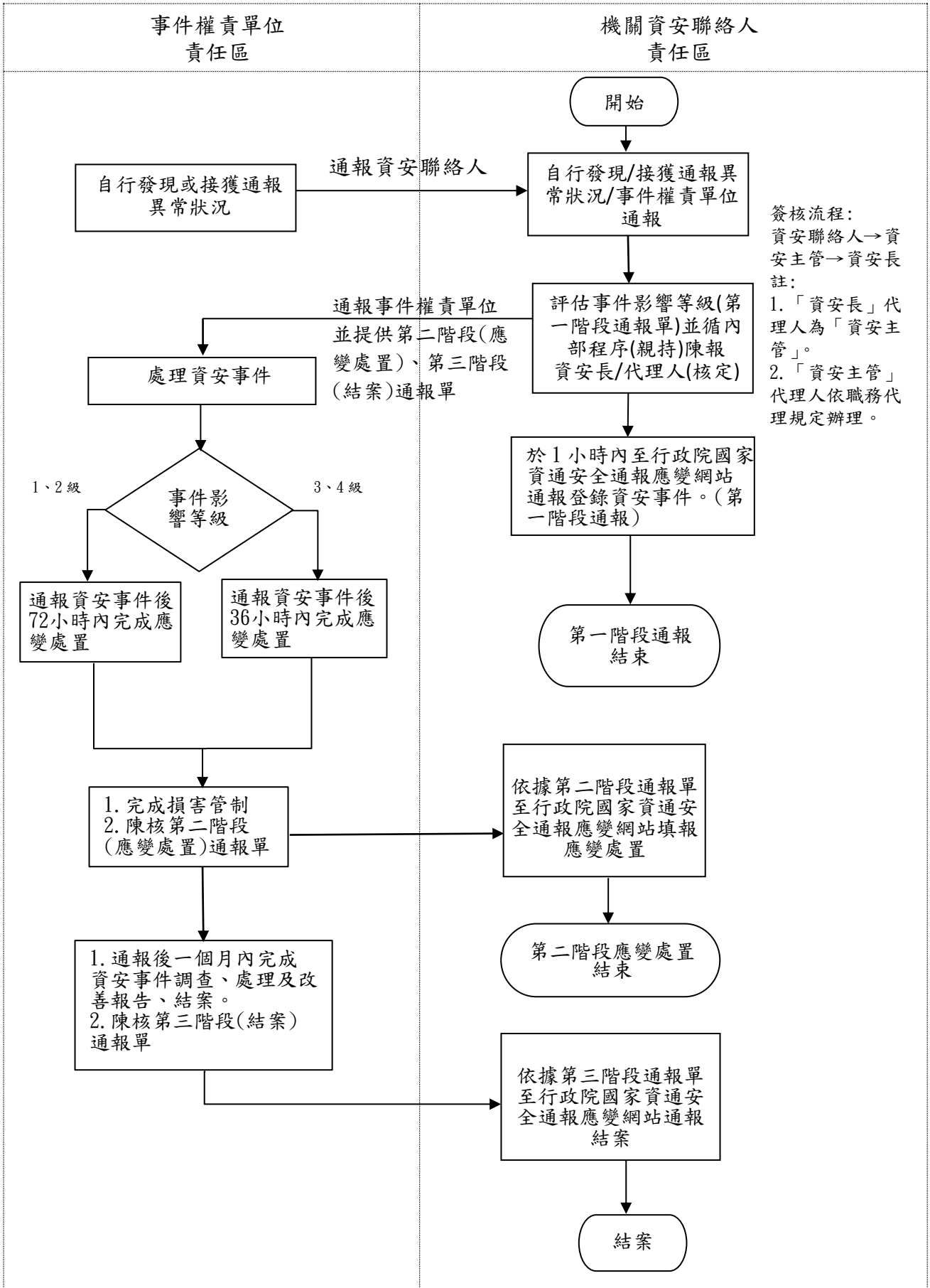
臺中市政府(機關名稱)(單位)作業程序說明表

項目編號	KC01
項目名稱	資通安全事件通報作業
承辦單位	資訊室(股)或負責資訊業務之單位
作業程序說明	一、事件權責單位自行發現，或接獲通報資通安全事件(以下簡稱資安事件)或異常事件時，應立即通報機關資安聯絡人。 二、 機關資安聯絡人(含資安專案)自行發現或接獲技服通知、事件權責單位通知後，應評估事件影響等級並循內部程序(親持)第一階段資安事件通報單陳報(資安長或代理人)。 三、經資安長/代理人核定後，由資安聯絡人通報事件權責單位，並須於 1 小時內至「國家資通安全通報應變網站」(https://www.ncert.nat.gov.tw)通報登錄資安事件細節、影響等級及支援申請等資訊,並評估該事件是否影響其他政府機關（構）或重要民生設施運作，進行橫向通報。 四、如因網路或電力中斷等事由，致使無法上網填報資安事件，應依行政院指定方式及時間先行提供事件細節,待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。 五、如屬「1」、「2」級資安事件，須於通報後 72 小時內完成應變處置;「3」、「4」級資安事件，須於通報後 36 小時內完成應變處置。 六、資安事件倘危及人員生命，或設備遭到破壞等涉及民、刑事案件時，經請示資安長/代理人後，應由資安聯絡人立即通報警檢調單位協助。如引發重大災害時，應向災害防救體系提報，請求支援處理。 七、完成應變處置後,事件權責單位應依第二階段應變處置通報單(資安事件緊急應變處理單)陳核資安長，再移請資安聯絡人至「國家資通安全通報應變網站」通報第二階段應變處置。 八、完成資安事件處理後,事件權責單位應依第三階段結案通報單(資安事件調查結案處理單)陳核資安長，再移請資安聯絡人至「國家資通安全通報應變網站」通報第三階段結案，始完成事件調查、改善報告及結案等程序。
控制重點	一、機關於發生資安事件時，應依行政院指定方式，於通報作業程序規定的期限內，至「國家資通安全通報應變網站」完成第一階段事件通報登錄。 二、機關於發生資安事件時，應於規定的期限內，完成應變處置之損害管制。

法令依據	資通安全管理法第14條及資通安全事件通報及應變辦法
使用表單	資通安全事故通報單(紙本通報使用)

KC01

臺中市政府(機關名稱)(單位)作業流程圖
資通安全事件通報作業



臺中市政府(機關名稱)(單位)內部控制制度控制作業自行評估表

○年度

評估單位：資訊室(股)或負責資訊業務之單位

風險項目：1.C1 資安事件未進行管理

2.C2 確認資安事件後未立即進行通報

作業類別(項目)：KC01 資通安全事件通報作業

評估期間：○年○月○日至○年○月○日

評估日期：　　年　　月　　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	未發生	不適用	
一、機關於發生資安事件時，是否依通報作業程序，於規定的期限內，至「國家資通安全通報應變網站」完成第一階段事件通報登錄。						
二、機關於發生資安事件時，是否於規定的期限內，完成損害管制。						
填表人：　　複核：						

註：

1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

附件

資通安全事件通報

一、 為利本機關遭遇資通安全事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保各項業務之正常運作。

二、 資通安全事件發生時，需將資安事故之評估資訊(如事件分類、影響程度、說明事件發生狀況、可能影響範圍及影響等級等)確實填報，相關內容參照行政院國家資通安全會報「資安事件通報單(紙本通報單)」，並依國家資通安全通報應變網站之三階段流程將通報單修訂為資安事件通報單、資安事件緊急應變處理單、資安事件調查結案處理單等三張，依三階段通報流程陳核資安長。資安事件影響等級之評斷如下：

（一）符合下列情形之一者，屬「1 級」事件：

(1) 非核心業務資訊遭輕微洩漏。

(2) 非核心業務資訊或非核心資通系統遭輕微竄改。

(3) 非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

（二）符合下列情形之一者，屬「2 級」事件：

(1) 非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

(2) 非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

(3) 非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

（三）符合下列情形之一者，屬「3 級」事件：

(1) 未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

(2) 未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

(3) 未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

（四）符合下列情形之一者，屬「4 級」事件：

(1) 一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

(2) 一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

(3) 涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。