文 件 編 號
AISAC－009

教育機構資安通報應變手冊
第一版

教育學術資安資訊分享與分析中心(ISAC)研發專案

委託機關(單位)：教育部

研　究　單　位：崑山科技大學

中華民國　　99　年　6　月　29　日

目　錄

壹、 前言

I. 緣起

我國資安通報應變之最高單位為行政院國家資通安全會報，舉凡重大資安事件不僅各級學校、區縣市網資安人員、教育機構資安通報應變小組及教育部主管人員需列管追蹤資安事件之處理，更必須回報至行政院國家資通安全會報。為使教育機構各級人員能快速掌握處理原則，本手冊遵循行政院國家資通安全會報於 98 年 2 月 5 日所頒訂之國家資通安全通報應變作業綱要，並參酌教育部所屬機關學校需求，特別增修不同流程以規範各級教育機構資安通報應變之處理。

II. 簡介

教育機構資安通報應變手冊（以下簡稱「本手冊」）為教育部為求有效掌握我國教育部所屬之各級教育機構之資通訊及網路系統遭受破壞、不當使用等資通安全事件(以下簡稱「資安事件」)，能迅速通報及緊急應變處置，並在最短時間內回復，以確保各級教育機構之正常運作，特訂定通報應變作業流程，以提供各級學校進行資安通報應變之準則。

III. 重要名詞定義:

本版之通報應變流程之分層架構規劃為三層架構(詳見第二章說明)，通報與應變流程需分開處理(詳見第二章說明)，且每一階段不同階層所完成的處理時間平台皆需記錄。在回報行政院與教育部之管理報表上逾時統計資料需明確定義完成時間，因此本節就手冊中使用之重要名詞加以定義。

(1)通報完成時間：

- 本通報完成時間指【第一線人員】於教育機構資安通報平台上完成通報流程的時間。
- 其他【區縣市網人員】與【教育機構資安通報應變小組】所完成審核分別稱之為【區縣市審核完成時間】與【教育機構資安通報應變小組審核完成時間】，記錄這些時間目的是讓上層機關了解資安事件處理所需之時程。

(2)應變完成時間：

- 本應變完成時間指【第一線人員】於教育機構資安通報平台上完成通報流程動作後，並完成應變流程，此僅包含填寫完畢緊急應變措施。
- 【第一線人員】應變流程可與通報流程同時進行，若同時完成，對於 0-1-2 級資安事件此通報完成時間即為應變完成時間。

(3)正式結案完成時間：

- 正式結案完成時間之設定，目的有二:(1)回覆行政院之資安回報中之逾時處理計算需使用，(2)提供給資安統計報表進行統計分析用。
- 正式結案完成時間需區分 0-1-2 級與 3-4 級的情況。
- 0-1-2 級的正式結案完成時間是【第一線人員】完成(通報與)應變流程後之時間
- 3-4 級的正式結案完成時間係指當教育機構資安通報應變小組完成應變審核動作，當【教育機構資安通報應變小組】審核完成後，此時間即為正式結案完成時間。

附記:回覆行政院之資安回報中需回報之時間有二:上述說明之 (1)通報完成時間，與(2)應變完成時間。

貳、 通報應變流程之規劃原則

一、 通報應變流程之分層架構及其職掌範圍

➢通報應變流程之分層架構:

本通報應變流程之分層架構依照教育部需求，規劃成三層架構，架構圖如下所示:

➢參與人員與職掌範圍:

不同單位依照其所管轄之職掌範圍與上述分層架構可分為:

- 【第一線人員】:第一線人員指的是各級學校之網管、資安人員，其負責範圍為其所管轄單位之資安事件的通報與處理。教育部規範第一線人員需列兩名人員以求資安事件處理之有效。
- 【區縣市網人員】: 區縣市網人員指的是 25 個縣(市)教育網路中心與 13 個區域網路中心之網管、資安人員，其職掌範圍為審核連線單位資安事件、協助第一線人員資安事件的處理，並可透過平台檢閱所屬連線單位的處理事件報表。教育部規範區縣市網人員需列兩名人員以求資安事件處理之有效。
- 【教育機構資安通報應變小組】: 其職掌範圍為負責教育機構資安通報平台之營運，審核所有資安事件，協調資安事件通報、處理與支援事項。
- 【教育部人員】: 教育部人員指的是教育部電算中心之各級長官與資安負責人員，教育部人員職掌範圍為指揮與監督重大資安事件之通報應變，並透過平台檢閱全國各級學校的事件處理報表。

二、 通報應變流程之規劃要點:

1. 為使通報應變流程更有效掌握，資安通報平台之流程劃分為通報流程與應變流程。
2. 所有通報應變流程都必須先完成通報流程(不管是 0、1、2 級或是 3、4 級,詳見下段落說明），且都必須審核過後才是正式結束通報流程。如此規劃著眼於不同層級之資安人員可充分掌握所發生之資安事件，並能依輕重等級啟動不同對應之處理機制。
3. 但為使通報應變流程更加有效率,【第一線人員】所完成的通報流程之時間即為通報完成時間，但後續仍需進行審核以確保正確，因此審核通過才是正式結束通報流程。
4. 應變流程則視事件等級不同有所不同。對於 0、1、2 級資安事件,【第一線人員】所完成的通報流程之時間即為應變完成時間，同時也是正式結案完成時間，後續應變流程無需進行審核。對於 3、4 級資安事件,【第一線人員】所完成的通報流程之時間為應變完成時間，但後續仍需進行審核以確保正確，因此審核通過才是正式結案完成時間。
5. 另外，為求快速阻絕入侵與攻擊，避免災害擴大，各級單位可先進行資安事件之應變處理(例如先行使受害之系統離線)，待通報流程結束後，緊接著進行的應變流程再填寫所處理的解決方法。
6. 通報應變流程依照不同資安情報來源又可畫分為:(1)自行通報(2)告知通報。
   甲、自行通報係由各單位(可以是【第一線人員】、【區縣市網人員】或是【教育機構資安通報應變小組】)自行發現問題時必主動向上級報告。不管是哪一級資安事件，當發現事件時須於 1 小時內登入通報平台完成通報此事件。所不同的是 3-4 級因事態嚴重，因此尚須電話通知上層管理，落實緊急通報。
   乙、 告知通報係由其他單位(本版的單位來源包括 ICST 與 A-SOC，99 年度將會有其他來源)所告知教育部所屬單位所發生之資安事件，依據分享原則與主動告知原則寄發資安通知。

三、 不同等級之處理原則

為了配合與行政院 ICST 之事件等級一致，且避免全國 4 千多所學校與教育部所屬單位需重新學習新規範，本版之事件等級分類比照行政院 ICST 之事件等級，僅新添 0 級事件。根據行政院 ICST 之事件等級之定義資安事件影響等級分為 4 個級別，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」。

底下針對教育部所使用的事件等級加以說明。

（一）4 級事件:

符合下列任一情形者，屬 4 級事件：

1. 國家機密資料遭洩漏。
2. 國家重要資訊基礎建設系統或資料遭竄改。
3. 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

附註:目前於國家資通應變平台上尚未有 4 級事件(資料來源於國家資通安全應變平台，在 2009 年 2 月 12 日起變更資安影響等級評定標準後，於 2009/2/12 後迄今 2010/6/20，未有 4 級事件)。

（二）3 級事件

符合下列任一情形者，屬 3 級事件：

1. 密級或敏感公務資料遭洩漏。
2. 核心業務系統或資料遭嚴重竄改。
3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

案例 1：98 年 x 月 y 日某中學，發現兩名學生撬開教務處窗戶入侵，盜用各辦公室電腦，利用燒片、拷貝等方式，竊走全校學生詳細個資及全校教職員個資與帳號密碼，並利用此帳號密碼入侵學務系統，竄改學籍資料與成績，犯罪行為持續年餘，因該生已影響學校學務系統並涉及個資法，具符合上述條款(1).密級或敏感公務資料遭洩漏範圍擴及全校與(2).核心業務系統或資料遭嚴重竄改，故判定為 3 級資安事件

案例 2：96 年 x 月 y 日某大學，因空調水塔缺水，使得機房溫度升高，造成伺服器及網路設備當機，機房營運中斷，此符合上述條款(3)核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作，故判定為 3 級資安事件。

（三）2 級事件

符合下列任一情形者，屬 2 級事件：

1. 非屬密級或敏感之核心業務資料遭洩漏。
2. 核心業務系統或資料遭輕微竄改。
3. 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

案例 1: 99 年 x 月 y 日某大學資料庫主機中教職員工帳號資料表，疑似遭 SQL Injection 值入 javascript 字串，導致部份系統無法正常登入，調用備份之資料，還原資料表，僅影響數筆資料，此符合上述(2).核心業務系統或資料遭輕微竄改與(3).核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作，故判定為 2 級資安事件。

案例 2:98 年 9 月 12 日某大學，遭到入侵並安裝惡意程式，得暫時關閉 web，影響部份網頁收信功能，此符合上述(3).核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作，故判定為 2 級資安事件。

（四）1 級事件

符合下列任一情形者，屬 1 級事件：

1. 非核心業務資料遭洩漏。
2. 非核心業務系統或資料遭竄改。
3. 非核心業務運作遭影響或短暫停頓。

案例 1: 99 年 x 月 y 日某國小，發現科任教室教學電腦被植入惡意程式，經修復後移除惡意程式無損失，此符合(2).非核心業務系統或資料遭竄改，故判定為 1 級資安事件。

案例 2: 99 年 x 月 y 日某大學，發現學務處一般行政用主機，使用者電腦有異常的情形發生且無法使用防毒軟體移除病毒，於資料備份後重新安裝作業系統，已上線使用中，此符合上述條件(1).非核心業務資料遭洩漏、(2).非核心業務系統或資料遭竄改與(3).非核心業務運作遭影響或短暫停頓，故判定為 1 級資安事件。

（五）0 級事件(資安預警)

凡屬於下列工單皆屬於 0 級事件

- 未確定事件或待確認工單:來自不同計畫所使用新型技術(A-SOC，miniSOC,…)所產生之工單，但其正確性有待確認。
- 其他單位所告知教育部所屬單位所發生未確定之資安事件。
- 教育部及區、縣網路中心檢舉信箱通告之資安事件。

上述皆屬於有待受駭(害)單位進行確認之資安事件。

0 級事件的設立目的在於:

- 提供資安預警的功能:未必每個單位會遭受到 0 級攻擊事件，但可提請各單位加強檢查所負責之伺服器或設備是否有遭受攻擊的可能性。
- 協助不同計畫所使用新型技術(A-SOC，miniSOC,…)並加強其正確性。
- 確認與處理其他單位所告知教育部所屬單位所發生未確定之資安事件。
- 確認與處理教育部及區、縣網路中心檢舉信箱通告之資安事件。

在通報應變流程中，需特別注意下列規範：

1.通報作業：【第一線人員】所屬單位若發現資安事件後需於 1 小時內通報完成。

2.應變處理作業：

(1)事件級別為 0、1、2 級資安事件需於 72 小時內處理完成並結案(包括通報流程與應變流程)。

(2)事件級別為 3、4 級資安事件需於 36 小時內處理完成並結案(包括通報流程與應變流程)。

四、 分層負責

為減輕【區縣市網人員】與【教育機構資安通報應變小組】的工作負擔及同時貫徹分層負責的精神，事件應變處理流程依等級規劃不同處理原則:

(1)事件級別為 0、1、2 級資安事件需於 72 小時內處理完成並結案，0、1、2 級影響範圍係限制於各單位，因此由各單位逕自處理並自行結案。其上層主管須就是否逾時進行輔導與協助。

(2)事件級別為 3、4 級資安事件因影響範圍擴大，因此需於 36 小時內處理完成並結案，三級單位都必須以主動積極的態度加以處理。應變流程須待三級審核後才可結案。

參、 自行通報流程

本節旨在說明 TANet 自行通報處理流程之標準作業程序，首先自行通報係由各單位(可以是【第一線人員】、【區縣市網人員】或是【教育機構資安通報應變小組】)自行發現問題時必主動向上級報告。不管是那一級資安事件，當第一線人員發現事件時須於 1 小時內登入通報平台完成通報此事件。所不同的是 3-4 級因事態嚴重，因此尚須電話通知上層管理，落實緊急通報。

一、 【自行通報】(1、2 級)處理流程(通報應變同時進行)

本情境所規範之處理流程圖如下：

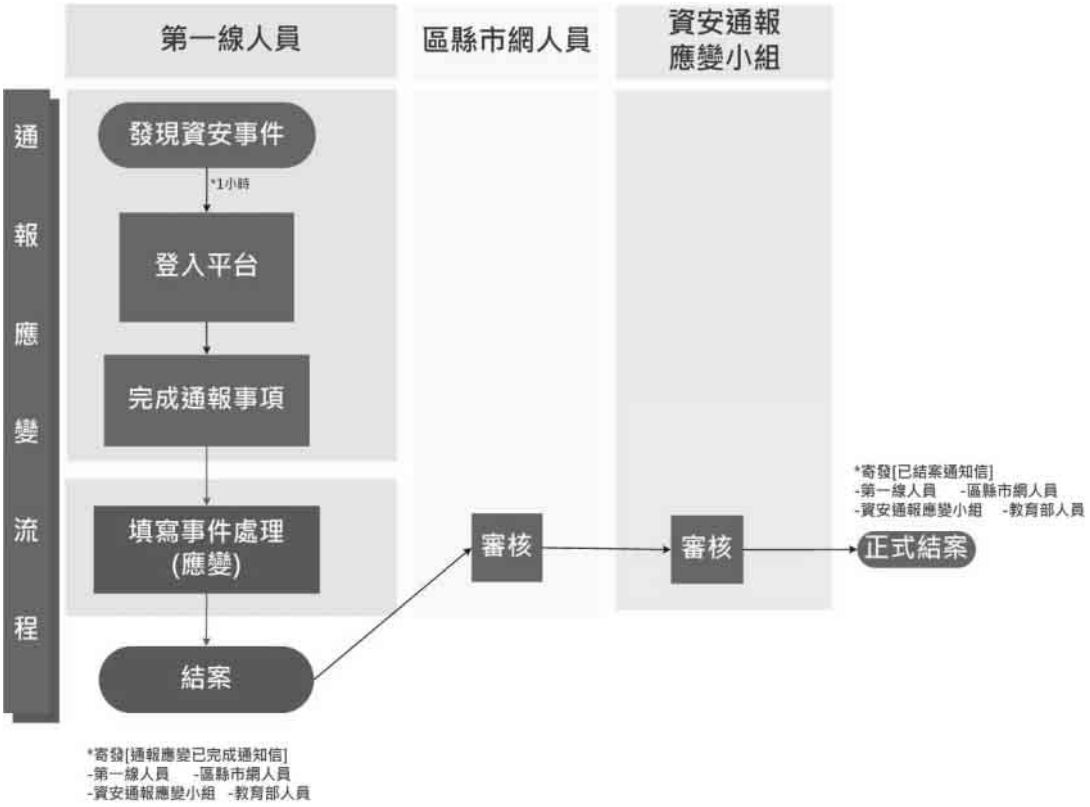
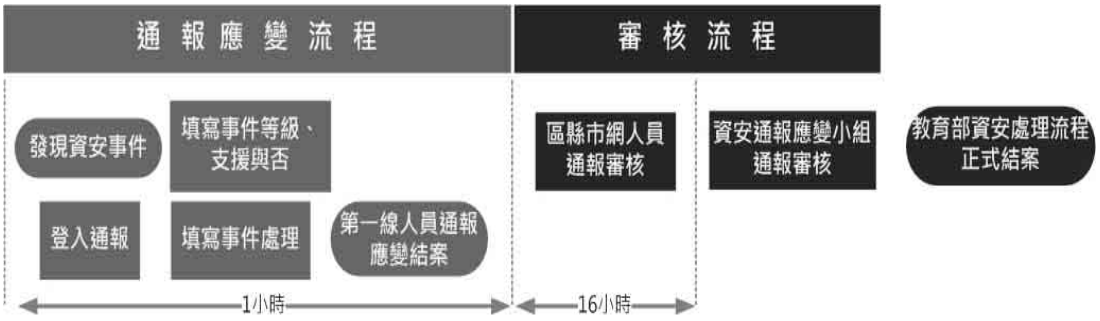


圖 1、2 級自行通報（通報應變同時進行）處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I.通報流程說明：

I.1【第一線人員】登入通報平台進行通報應變作業

【第一線人員】自行發現資安事件時，本於主動求是精神，登入通報平台進行資安處理作業。

▶注意事項

1. 第一線人員發現資安事件時，須於 1 小時內登入通報平台完成通報此資安事件。

▶說明事項

1. 資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫
   (1)事件等級: 因係 1-2 級通報，故無須電話告知【區縣市網人員】。
   (2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2. 【第一線人員】填完成通報流程後，繼續填寫應變流程，按發佈通報結案，便已完成【第一線人員】之通報應變，此時間即為通報應變完成時間。
3. 完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▶【第一線人員】完成處理後，平台接續處理事項:

➡平台會自動產生◎**工單編號與** ◎**完成時間**：

【第一線人員】可於後續**工單處理狀態**檢視得知◎**工單編號與** ◎**完成時間**

⇨【第一線人員】完成通報應變流程之時間即為回報給行政院之通報完成時間與應變完成時間(兩時間相同)。

➡平台會自動產生下列**工單**(已知:事件等級=1、2級)

(1)一**通報待審核工單(相同工單編號)**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。

(2)產生一處理狀態**工單(相同工單編號)**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列Email:（已知:事件等級=1、2級)

⇨平台寄發相同格式的【通報應變已完成】Email分別通知

(1)【第一線人員】: 目的在確認確實有發通告。。

(2)【區縣市網人員】: 目的在提醒有**通報待審核，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發SMS簡訊通知(已知:事件等級=1、2級)

(1)【第一線人員】:無。

(2)【區縣市網人員】: 目的在提醒有**通報待審核，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

附註: 【第一線人員】在此無逾時產生。

I.2【區縣市網人員】登入平台進行通報審核作業

▶注意事項

1. (1、2級)資安事件，區縣市網人員僅需審核通報流程，毋需審核應變流程。
2. 【區縣市網人員】須於收到**通報審核工單**後16小時內登入通報平台完成審核。若未能於收到**通報審核工單**後16小時內完成審核，則為逾時處理。

3. 平台逾時處理流程:

- 平台將於收到審核工單超過4小時後寄發第一次【審核已逾時】Email給【區縣市網人員】。
- 之後每12小時寄發【審核已逾時】Email給【區縣市網人員】。

▶(通報)審核作業說明事項

1.【區縣市網人員】將特別注意事件等級與是否需支援:
(1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。
2.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▶【區縣市網人員】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已審核通報作業。
(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供Email通知(已知:事件等級=1、2級)。

➡平台在此並沒有提供SMS簡訊通知(已知:事件等級=1、2級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】進行審核作業

▸注意事項

1.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。

▶(通報)審核作業說明事項

1.(1、2級)資安事件，教育機構資安通報應變小組僅需審核通報流程，毋需審核應變流程。
2.【教育機構資安通報應變小組】須特別注意事件等級與是否需支援:

(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。

(2)審核事件等級若是通過則按同意，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

3.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個教育部規範之通報流程正式完成。

▶【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單:**

(1) 當教育機構資安通報應變小組審核完畢，代表該工單已正式完成結案，所以會產生一**歷史工單**到【所有人員】歷史通報目錄。

✉平台會自動寄發下列 Email:（已知:事件等級=1、2 級)。

⇨平台寄發相同格式的【通報已審核】Email 分別通知

(1)【第一線人員】: 目的在告知該通報已正式完成結案。

(2)【區縣市網人員】: 目的在告知該通報已正式完成結案。

(3)【教育機構資安通報應變小組】: 目的告知在該通報已正式完成結案。

(4)【教育部人員】: 目的在告知該通報已正式完成結案。

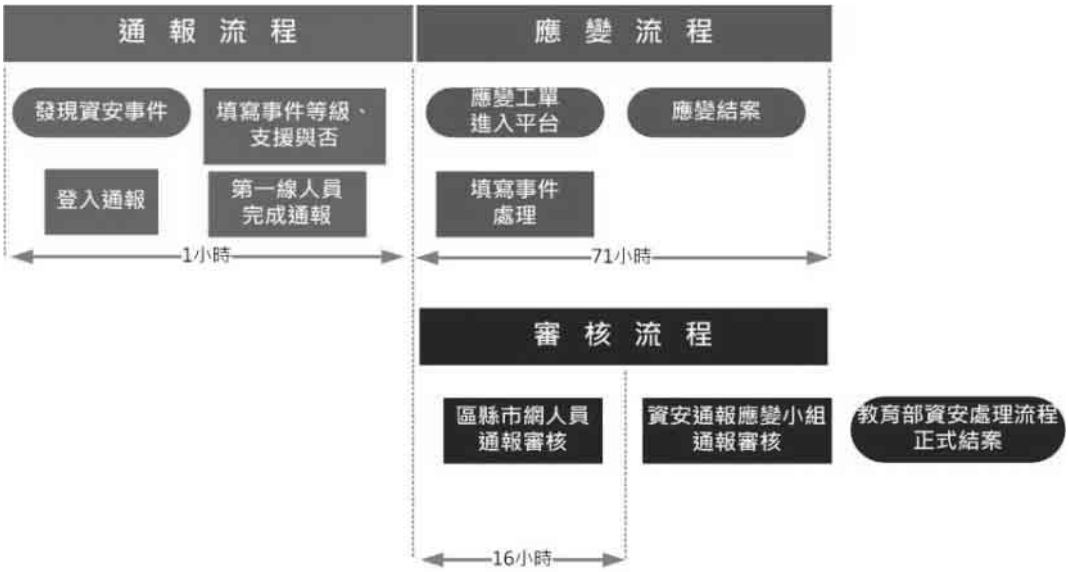
➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2 級)。

二、 【自行通報】(1、2級)處理流程(通報應變分開進行)

本情境所規範之處理流程圖如下：

圖 1、2級自行通報(通報應變分開進行)處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I. 通報流程說明：

I.1【第一線人員】登入通報平台進行通報應變作業

【第一線人員】自行發現資安事件時，本於主動求是精神，登入通報平台進行資安處理作業。

▶注意事項

1. 第一線人員發現資安事件時，須於 1 小時內登入通報平台完成通報此資安事件。

▶說明事項

1. 資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫
   (1)事件等級: 因係 1-2 級通報，故無須電話告知【區縣市網人員】。
   (2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

   ⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2【第一線人員】填完成通報流程後，按發佈通報結案，便已完成【第一線人員】之通報

應變，此時間即為通報完成時間。【第一線人員】需於後續 71 小時內再次登入平台完成應變流程。否則則為逾時，平台會進行逾時處理流程。

3.完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▶【第一線人員】完成處理後，平台接續處理事項:

➡平台會自動產生◎**工單編號與** ◎**完成時間**：

【第一線人員】可於後續**工單處理狀態**檢視得知◎**工單編號與** ◎**完成時間**

⇨【第一線人員】完成通報流程之時間即為回報給行政院之通報完成時間

➡平台會自動產生下列**工單**(已知:事件等級=1、2 級)

(1)送一**待處理工單(相同工單編號)**到【第一線人員】應變待處理目錄。

(2)一**通報待審核工單(相同工單編號)**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。

(3)產生一處理狀態**工單(相同工單編號)**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列 Email:（已知:事件等級=1、2 級）

⇨平台寄發相同格式的【通報已完成】Email 分別通知

(1)【第一線人員】: 目的在確認確實有發通告。

(2)【區縣市網人員】: 目的在提醒有**通報待審核工單，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發 SMS 簡訊通知(已知:事件等級=1、2 級)

(1)【第一線人員】:無。

(2)【區縣市網人員】: 目的在提醒有**通報待審核工單，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

I.2【區縣市網人員】登入平台進行通報審核作業

▶注意事項

1. (1、2 級)資安事件，區縣市網人員僅需審核通報流程，毋需審核應變流程。

2.【區縣市網人員】須於收到**通報審核工單**後 16 小時內登入通報平台完成審核。若未能於收到**通報審核工單**後 16 小時內完成審核，則為逾時處理。

3. 平台逾時處理流程:
   - 平台將於收到審核工單超過 16 小時後寄發第一次【審核已逾時】**Email** 給【區縣市網人員】。
   - 之後每 12 小時寄發【審核已逾時】**Email** 給【區縣市網人員】。

▶(通報)審核作業說明事項

1.【區縣市網人員】將特別注意事件等級與是否需支援:
(1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

2.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▶【區縣市網人員】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**(已知:事件等級=1、2 級)

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已通報審核作業。

(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=1、2 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】進行審核作業

▸注意事項

1.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。

▸(通報)審核作業說明事項

1.(1、2級)資安事件，教育機構資安通報應變小組僅需審核通報流程，毋需審核應變流程。

2.【教育機構資安通報應變小組】須特別注意事件等級與是否需支援:

(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。

(2)審核事件等級若是通過則按同意，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

3.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個教育部規範之通報流程正式完成。

▶【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**(已知:事件等級=1、2級)

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【教育機構資安通報應變小組】已通報審核作業。

✉平台會自動寄發下列Email:（已知:事件等級=1、2級)。

⇨平台寄發相同格式的【通報已審核】Email分別通知

(1)【第一線人員】: 目的在告知該通報已正式完成結案。

(2)【區縣市網人員】: 目的在告知該通報已正式完成結案。

(3)【教育機構資安通報應變小組】: 目的在告知該通報已正式完成結案。

(4)【教育部人員】: 目的在告知該通報已正式完成結案。

➡平台在此並沒有提供SMS簡訊通知(已知:事件等級=1、2級)。

II.應變流程說明：

應變流程開始於應變待處理工單進入到平台的【第一線人員】應變待處理目錄。

II.0 平台會自動檢查是否逾時

▶說明事項

1.1、2級資安事件【第一線人員】需於71小時內處理完成應變並送出審查。

2.3、4級資安事件【第一線人員】需於35小時內處理完成應變並送出審查。

▶平台處理事項:

1.平台會每1小時自動檢查是否逾時。若過程(通報流程+應變流程)中處理已逾時，平台會進行應變逾時處理流程。

2. 1、2級應變逾時處理流程

✉平台將會自動寄發下列Email:（已知:事件等級=1、2級）

(1)逾時前1小時寄發【應變逾時處理通知】Email通知【第一線人員】。
(2)逾時後每12小時寄發【應變逾時處理通知】Email通知【第一線人員】。

➡平台在此並沒有提供SMS簡訊通知。(已知:事件等級=1、2級)

II.1【第一線人員】登入平台並進行應變處理

▸注意事項

1.當【第一線人員】於一小時內完成通報後，須在於71小時內登入平台完成應變處理。

▸說明事項

1.當第一線人員處理完畢後，需進入通報平台填寫事件處理情況。
2.第一線人員於填寫緊急應變措施、解決辦法與解決時間後，按發佈應變通報送出結案。
3. 1、2級資安事件【區縣市網人員】、【教育機構資安通報應變小組】無需進行應變審核。

教育部規範之完整通報與應變流程正式完成結案。

▸【第一線人員】完成處理後，平台接續處理事項:

➡平台將會自動更新【所有人員】歷史通報目錄夾,
【所有人員】可於歷史通報目錄夾看到最新完成與更新後之所有紀錄。

✉平台會自動寄發下列Email:（已知:事件等級=1、2級）

⇨平台寄發相同格式的【應變已完成】Email分別通知

(1)【第一線人員】: 目的在告知與備查。
(2)【區縣市網人員】: 目的在告知與備查。
(3)【教育機構資安通報應變小組】: 目的在告知與備查。
(4)【教育部人員】: 目的在告知與備查。

➡平台在此並沒有提供SMS簡訊通知。(已知:事件等級=1、2級)

三、 【自行通報】(3、4級)處理流程(通報應變同時進行)

本情境所規範之處理流程圖如下：

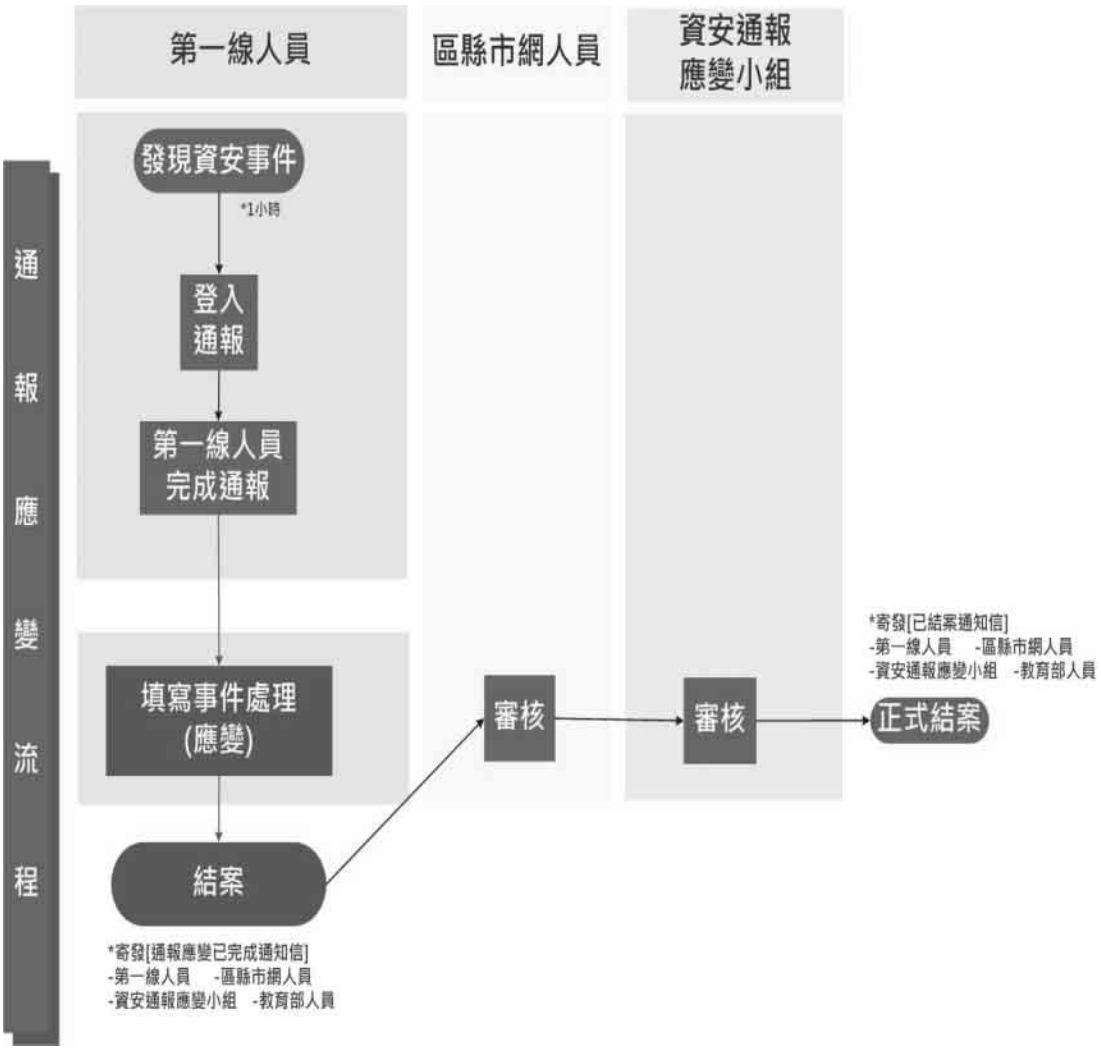
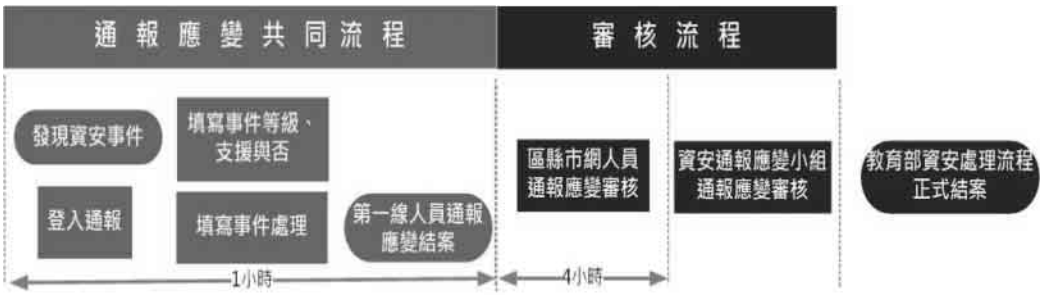


圖 3、4級自行通報(通報應變同時進行)處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I.通報流程說明：

I.1【第一線人員】登入通報平台進行通報應變作業

【第一線人員】自行發現資安事件時，本於主動求是精神，登入通報平台進行資安處理作業。

▸注意事項

1.第一線人員發現資安事件時，須於 1 小時內登入通報平台完成通報此資安事件。

▸說明事項

1.資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫
(1)事件等級: 因係 3-4 級通報須電話告知【區縣市網人員】及【教育機構資安通報應變小組】。
(2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2.【第一線人員】填完成通報流程後，繼續填寫應變流程，按發佈通報結案，便已完成【第一線人員】之通報應變，此時間即為通報應變完成時間。

⇨【第一線人員】完成通報應變流程之時間即為回報給行政院之通報完成時間與應變完成時間(兩時間相同)

3.完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▸【第一線人員】完成處理後，平台接續處理事項:

➡平台會自動產生◎**工單編號與** ◎**完成時間**：

【第一線人員】可於後續**工單處理狀態**檢視得知◎**工單編號與** ◎**完成時間**

➡平台會自動產生下列**工單**

(1)一**待審核工單**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。

(2)產生一處理狀態**工單**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列 Email:（已知:事件等級=3、4 級）

⇨平台寄發相同格式的【通報應變已完成】Email 分別通知

(1)【第一線人員】: 目的在確認確實有發通告。

(2)【區縣市網人員】: 目的在提醒有**通報應變待審核工單，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發 SMS 簡訊通知(已知:事件等級=3、4 級)

(1)【第一線人員】:無。

(2)【區縣市網人員】: 目的在提醒有**通報待審核工單，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡**【教育機構資安通報應變小組】發現通報 3、4 級資安事件，應即時判斷資安事件內容確認為 3、4 級事件後，電話通報【教育部人員】，並全程追蹤至結案審核完成。**

I.2【區縣市網人員】登入平台進行通報應變審核作業

▸注意事項

1.【區縣市網人員】收到**通報應變審核工單**後，須於 4 小時內登入通報平台完成審核，若未能於收到**通報應變審核工單**後 4 小時內完成審核，則為逾時處理。

2.逾時處理流程:

- 平台將於發送審核工單超過 4 小時後寄第一次【審核已逾時】**Email** 給【區縣市網人員】
- 之後每 12 小時寄發【審核已逾時】**Email** 給【區縣市網人員】。

▸審核作業說明事項:通報與應變流程皆需審核

1.(3、4級)資安事件,【區縣市網人員】需審核通報流程和應變流程。
2.通報流程審核:【區縣市網人員】需特別注意事件等級與是否需支援。
(1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
(2)審核事件等級若是通過則按通過,若是不通過(也就是說,事件等級填寫錯誤)則按不通過,並填寫(1)建議等級,與(2)原因。
3.應變流程審核:【區縣市網人員】需特別注意解決辦法是否合適。
若是通過(解決辦法合適)則按通過,若是不通過(也就是說,解決辦法不合適)則按不通過,並填寫(1)原因。【區縣市網人員】需主動告知(視難易度,採Email或電話告知方式)【第一線人員】合適之建議措施並請【第一線人員】進行後續處理。
4.當【區縣市網人員】按確定時,代表【區縣市網人員】審核流程已完成。

▸【區縣市網人員】完成處理後,平台接續處理事項:

➡平台會自動產生(更新)下列**工單**
(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**,顯示【區縣市網人員】已通報審核作業。
(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄,提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供Email通知(已知:事件等級=3、4級)。

➡平台在此並沒有提供SMS簡訊通知(已知:事件等級=3、4級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】登入平台進行通報審核作業

▸注意事項

1.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。

▸審核作業說明事項:通報與應變流程皆需審核

1.(3、4級)資安事件,【教育機構資安通報應變小組】需審核通報流程和應變流程。
2.通報流程審核:【教育機構資安通報應變小組】需特別注意事件等級與是否需支援。

(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。

(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

3.應變流程審核：【教育機構資安通報應變小組】需特別注意解決辦法是否合適。

3、4 級資安事件【教育機構資安通報應變小組】需主動聯絡【區縣市網人員】,就【第一線人員】之解決辦法是否合適進行瞭解。若是通過(解決辦法合適)則按通過，若是不通過(也就是說, 解決辦法不合適)則按不通過，並填寫(1)原因。【教育機構資安通報應變小組】需主動告知(視難易度，採 Email 或電話告知方式) 【區縣市網人員】與【第一線人員】合適之建議措施並請【第一線人員】進行後續處理，請【區縣市網人員】協助【第一線人員】處理。

4.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個通報流程正式完成。

▶【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 產生一**歷史工單**到【所有人員】歷史通報目錄，顯示通報已正式完成。

✉ 平台會自動寄發 Email 通知：

⇨平台寄發相同格式的【通報應變已審核】Email 分別通知

(1)【第一線人員】: 目的在告知該工單已正式結案。

(2)【區縣市網人員】目的在告知該工單已正式結案。

(3)【教育機構資安通報應變小組】: 目的在告知該工單已正式結案與備查。

(4)【教育部人員】: 目的在告知該工單已正式結案與備查。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

四、 【自行通報】(3、4級)處理流程(通報應變分開進行)

本情境所規範之處理流程圖如下：

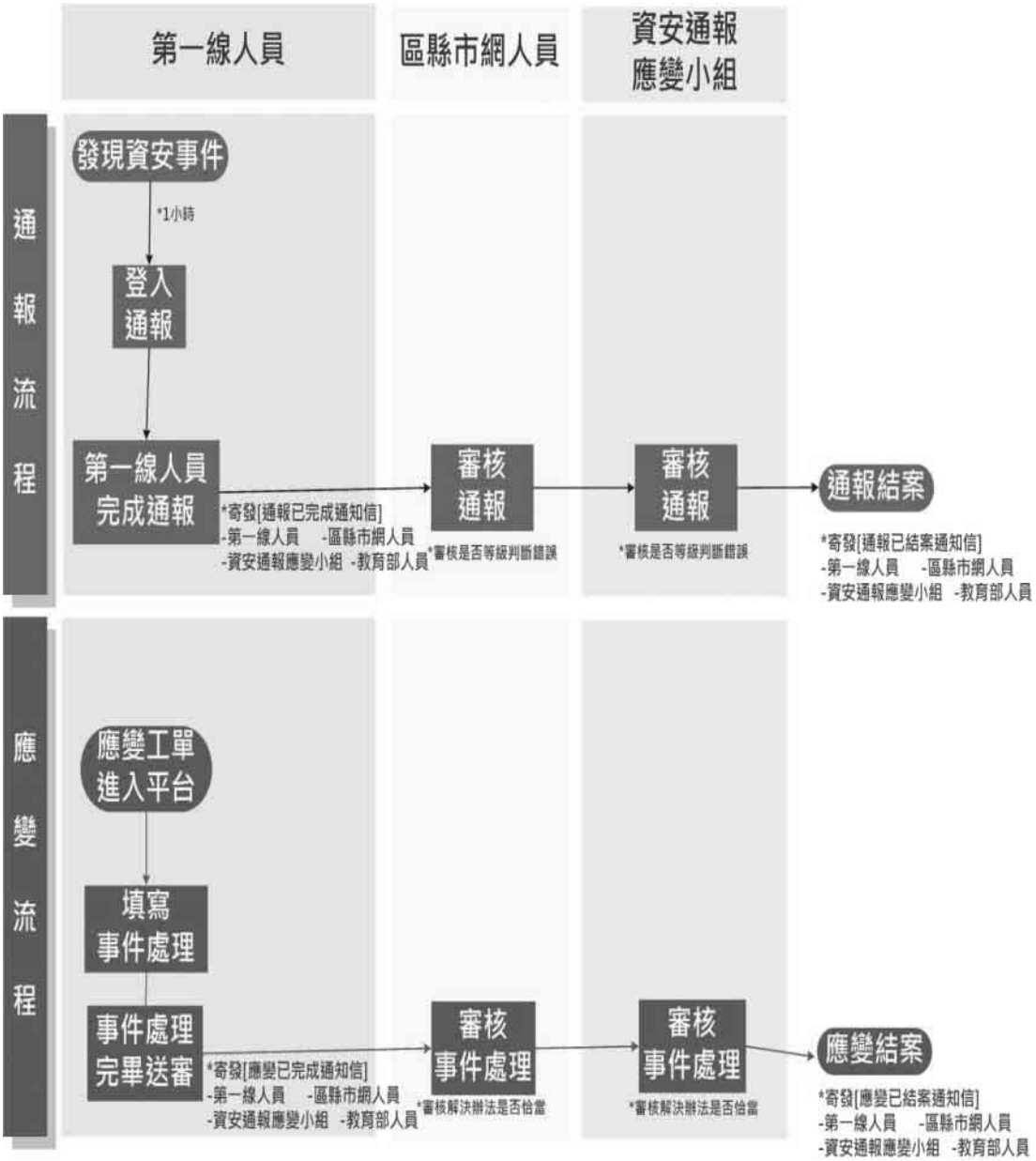
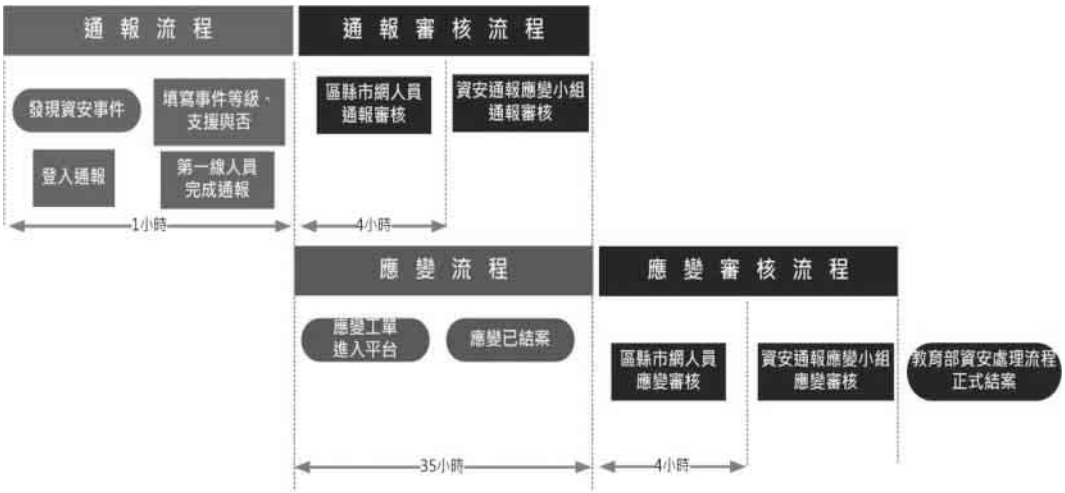


圖 3、4級自行通報(通報應變分開進行)處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I.通報流程說明：

I.1【第一線人員】登入通報平台進行通報應變作業

【第一線人員】自行發現資安事件時，本於主動求是精神，登入通報平台進行資安處理作業。

▸注意事項

1. 第一線人員發現資安事件時，須於 1 小時內登入通報平台完成通報此資安事件。

▸說明事項

1. 資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫
   (1)事件等級: 因係 3-4 級通報須電話告知【區縣市網人員】及【教育機構資安通報應變小組】。
   (2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

   ⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2.【第一線人員】完成通報時，按送出結案，便已完成【第一線人員】之通報流程，此時間即為通報完成時間。【第一線人員】需於後續 35 小時內再次登入平台完成應變流程。否則則為逾時，平台會進行逾時處理流程。

3.完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▸**【第一線人員】完成處理後，平台接續處理事項:**

➡平台會自動產生**◎工單編號與 ◎完成時間：**

【第一線人員】可於後續**工單處理狀態**檢視得知**◎工單編號與 ◎完成時間**

⇨【第一線人員】完成通報流程之時間即為回報給行政院之通報完成時間

➡平台會自動產生下列**工單**

(1)送一**應變待處理工單**到【第一線人員】應變待處理目錄。

(2)一**通報待審核工單**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。

(3)產生一處理狀態**工單**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列 Email:（已知:事件等級=3、4 級）

⇨平台寄發相同格式的【通報已完成】Email 分別通知

(1)【第一線人員】: 目的在確認確實有發通告。。

(2)【區縣市網人員】: 目的在提醒有**通報待審核工單，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發 SMS 簡訊通知(已知:事件等級=3、4 級)

(1)【第一線人員】:無。

(2)【區縣市網人員】: 目的在提醒有**通報待審核工單，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡**【教育機構資安通報應變小組】發現通報 3、4 級資安事件，應即時判斷資安事件內容確認為 3、4 級事件後，電話通報【教育部人員】，並全程追蹤至結案審核完成。**

I.2【區縣市網人員】登入平台進行通報審核作業

▸注意事項

1.【區縣市網人員】收到**通報待審核工單**後，須於 4 小時內登入通報平台完成審核，若未能於收到**通報應變審核工單**後 4 小時內完成審核，則為逾時處理。

2.逾時處理流程:

- 平台將於發送審核工單超過 4 小時後寄第一次【審核已逾時】**Email** 給【區縣市網人員】
- 之後每 12 小時寄發【審核已逾時】**Email** 給【區縣市網人員】。

▸(通報)審核作業說明事項

1.【區縣市網人員】將特別注意事件等級與是否需支援:
(1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

2.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▸【區縣市網人員】完成(通報)審核作業後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已通報審核作業。

(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=3、4 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】登入平台進行通報審核作業

▸注意事項

1.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。

▸(通報)審核作業說明事項

1.【教育機構資安通報應變小組】須特別注意事件等級與是否需支援:
(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。
(2)審核事件等級若是通過則按同意，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。
2.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個教育部規範之通報流程正式完成。

▶【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**
(1) 當教育機構資安通報應變小組審核完成表示通報流程已正式完成，更新到所有人員】的工單處理狀態目錄。

✉平台會提供 Email 通知(已知:事件等級=3、4 級)。

⇨平台寄發相同格式的【通報已審核】Email 分別通知

(1)【第一線人員】: 目的在告知。
(2)【區縣市網人員】: 目的在告知。
(3)【教育機構資安通報應變小組】: 目的在告知與備查。
(4)【教育部人員】: 目的在告知與備查。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

II.應變流程說明：

應變流程開始於應變待處理工單進入到平台的【第一線人員】應變待處理目錄。

II.0 平台會自動檢查是否逾時

▶說明事項

1.1、2 級資安事件【第一線人員】需於 71 小時內處理完成應變並送出審查。
2.3、4 級資安事件【第一線人員】需於 35 小時內處理完成應變並送出審查。

▶平台處理事項:

1.平台會每 1 小時自動檢查是否逾時。若過程(通報流程+應變流程)中處理已逾時，平台會進行應變逾時處理流程。

2.3、4 級應變逾時處理流程

✉平台會自動寄發下列 Email:（已知:事件等級=3、4 級）

(1)逾時前 1 小時寄發【將逾時】Email 通知【第一線人員】。
(2)逾時後每 12 小時會再寄發【已逾時】Email 提醒【第一線人員】。

➡平台在此並沒有提供 SMS 簡訊通知。(已知:事件等級=3、4 級)

II.1【第一線人員】登入平台並進行應變處理

▸注意事項

1.當【第一線人員】於一小時內完成通報後，須在於 35 小時內登入平台完成應變處理。

▸說明事項

1.當第一線人員處理完畢後，需進入通報平台填寫事件處理情況。
2.第一線人員於填寫緊急應變措施、解決辦法與解決時間後，按發佈應變通報送出結案。
3.教育部規範之完整通報仍待區縣市網與教育機構資安通報應變小組審核結果。

▸【第一線人員】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單:**
(1)送一**應變待審核工單(相同工單編號)**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。
(2)產生一處理狀態**工單(相同工單編號)**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列 Email:（已知:事件等級=3、4 級）

⇨平台寄發相同格式的【應變已完成】Email 分別通知

(1)【第一線人員】: 目的在告知與備查。
(2)【區縣市網人員】:目的在提醒【區縣市網人員】須登入平台處理【應變待審核】。
(3)【教育機構資安通報應變小組】: 目的在告知與備查。
(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發 SMS 簡訊通知（已知:事件等級=3、4 級）
平台寄發【待審核】簡訊通知【區縣市網人員】,提醒【區縣市網人員】須登入平台處理。

II.2【區縣市網人員】登入平台進行應變審核作業

▸注意事項

1.【區縣市網人員】收到**應變審核工單**後須於 4 小時內登入通報平台完成審核。若未能於收到**應變審核工單**後 4 小時內完成審核，則為逾時處理。
2.逾時處理流程:
- 平台將於發送審核工單超過 4 小時後寄發第一次【審核已逾時】Email 給【區縣市網人員】
- 之後每 12 小時會再寄發【審核已逾時】Email 給【區縣市網人員】。

▸(應變)審核作業說明事項:

1.【區縣市網人員】需特別注意解決辦法是否合適。
2.若是通過(解決辦法合適)則按通過，若是不通過(也就是說, 解決辦法不合適)則按不通過，並填寫(1)原因。【區縣市網人員】需主動告知(視難易度，採 Email 或電話告知方式)【第一線人員】合適之建議措施並請【第一線人員】進行後續處理。
3.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▸【區縣市網人員】完成(應變)審核作業後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已完成(應變)審核作業。

(2)一應變**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=3、4 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

II.3【教育機構資安通報應變小組】登入平台進行應變審核作業

▸注意事項

1.【教育機構資安通報應變小組】須於收到**待審核工單**後，需登入通報平台完成審核。

▸(應變)審核作業說明事項:

1.【教育機構資安通報應變小組】需特別注意解決辦法是否合適。
2.3、4級資安事件【教育機構資安通報應變小組】需主動聯絡【區縣市網人員】，就【第一線人員】之解決辦法是否合適進行瞭解。
3.若是通過(解決辦法合適)則按通過，若是不通過(也就是說, 解決辦法不合適)則按不通過，並填寫(1)原因。
4.【教育機構資安通報應變小組】需主動告知(視難易度，採 Email 或電話告知方式)【區縣市網人員】與【第一線人員】合適之建議措施並請【第一線人員】進行後續處理，請【區縣市網人員】協助【第一線人員】處理。
5.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個通報流程正式完成。

▸【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台將會平台會自動更新【所有人員】歷史通報目錄夾
【所有人員】可於歷史通報目錄夾看到最新完成與更新後之所有紀錄。

✉平台會自動寄發下列 Email:（已知:事件等級=3、4級）

⇨平台寄發相同格式的【應變已審核】Email 分別通知

(1)【第一線人員】: 目的在告知與備查
(2)【區縣市網人員】: 目的在告知與備查
(3)【教育機構資安通報應變小組】:目的在告知與備查
(4)【教育部人員】:目的在告知與備查

➡平台在此並沒有提供 SMS 簡訊通知。(已知:事件等級=3、4級)

教育部規範之完整資安處理流程正式結案。

肆、 告知通報流程

本節旨在說明 TANet 告知通報處理流程之標準作業程序。首先告知通報係由其他單位(本版的單位來源包括 ICST ,A-SOC 與 ABUSE 檢舉信箱…，99 年度將會有其他來源)所告知教育部所屬單位所發生之資安事件，依據分享原則與主動告知原則寄發資安通報。不管是那一級資安事件，當第一線人員接獲通報時須於 1 小時內登入通報平台完成通報處理此事件。所不同的是 3-4 級因為重要事件，因此尚須電話通知上層管理，落實緊急通報。

告知通報流程起始於有新進資安事件工單(來自【A-SOC】或【G-SOC】)進入通報平台。由於新進資安事件工單並未附有資安事件等級(需由後續【第一線人員】加以填寫)，因此平台處理流程會有不同作法。

不管是那一級資安告知工單，平台都會自動化處理下列事項:

1.平台將自動把外部通報資訊帶入工單。

2.平台會自動產生工單編號。

3.平台會自動產生下列**工單**(條件:事件等級尚未得知，**相同工單編號**)

(1)送一**告知通報工單**到【第一線人員】新進告知通報目錄夾。

(2)送一**告知通報工單**到【區縣市網人員】新進告知通報目錄夾。

(3)送一**告知通報工單**到【教育機構資安通報應變小組】新進通報目錄夾。

(4)送一**告知通報工單**到【教育部人員】新進告知通報目錄夾。

4.平台會自動寄發下列 Email:（事件等級尚未得知）

(1)【第一線人員】: 目的在告知與提醒登入平台進行通報。

(2)【區縣市網人員】: 目的在告知與備查。

(3)【教育機構資安通報應變小組】:目的在告知與備查。

(4)【教育部人員】:目的在告知與備查。

5.平台會自動寄發 SMS 簡訊通知(事件等級尚未得知)

(1)【第一線人員】: 目的在告知與提醒登入平台進行通報。

(2)【區縣市網人員】:目的在告知與備查。

(3)【教育機構資安通報應變小組】:目的在告知與備查。

(4)【教育部人員】:目的在告知與備查。

➨Email 提供詳盡的資安事件說明及相關處理建議，SMS 簡訊則在及時告知相關人員資安事件的發生，提醒相關人員需盡快收發 Email 並進行後續處理作業。

➡【教育機構資安通報應變小組】發現可成為 3、4 級資安事件，應立即聯絡【第 1 線人員】進行事件初步了解，並通知【教育部人員】及【縣市網人員】告知相關事件狀況，並全程追蹤事件處理流程與進度。

一、 【告知通報】(1、2 級)處理流程(通報應變同時進行)

本情境所規範之處理流程圖如下：

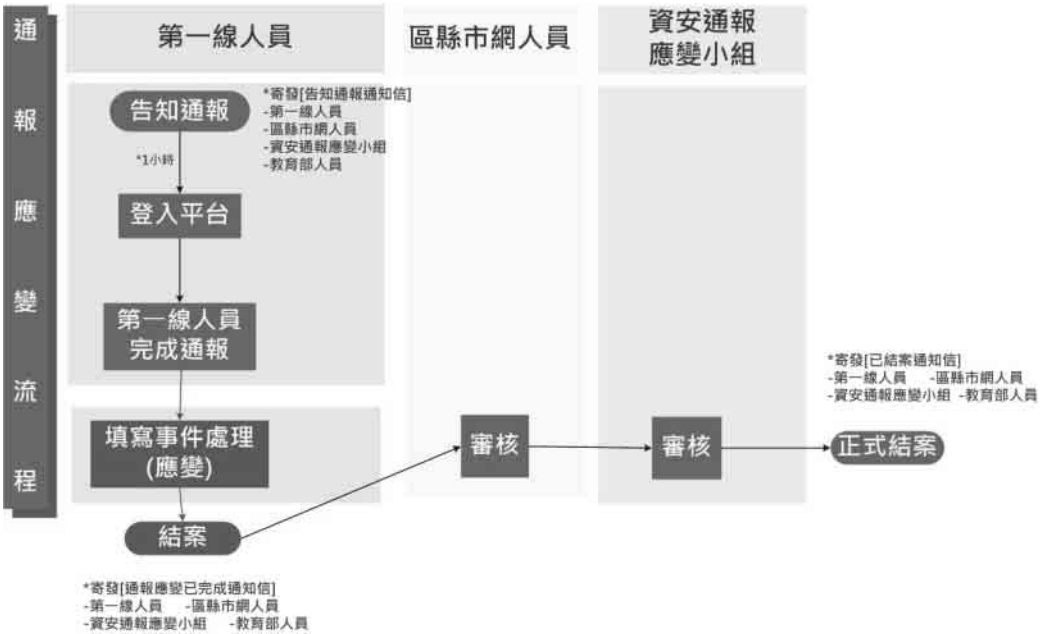
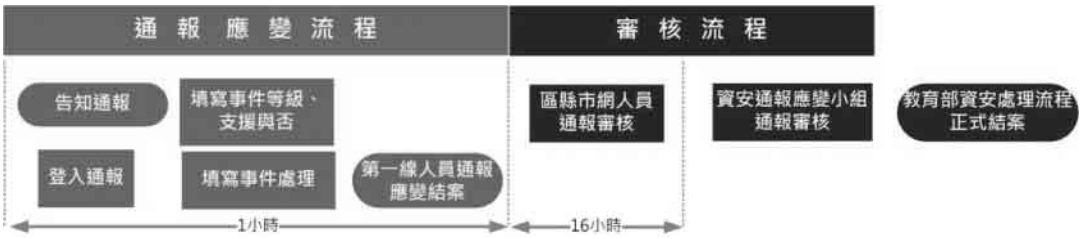


圖 1、2 級告知通報(通報應變同時進行)處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I.通報流程說明：

I.1【第一線人員】登入通報平台進行(通報應變)作業

【第一線人員】於收到【告知通報】之 Email 或 SMS 簡訊，須於 1 小時內登入通報平台完成通報此資安事件。

▸說明事項

1.資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫
(1)事件等級: 因係 1-2 級通報，故無須電話告知【區縣市網人員】。
(2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2.【第一線人員】填完成通報流程後，繼續填寫應變流程，按發佈通報結案，便已完成【第一線人員】之通報應變，此時間即為通報應變完成時間。

⇨【第一線人員】完成通報應變流程之時間即為回報給行政院之通報完成時間

3.完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▸【第一線人員】完成處理後，平台接續處理事項:

➡平台會自動產生◎**完成時間**：(**工單編號於發送工單時就已經產生**)
【第一線人員】可於後續**工單處理狀態**檢視得知◎**工單編號與**◎**完成時間**
➡平台會自動產生下列**工單**
(1)一**通報待審核工單(相同工單編號)**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。
(2)產生一處理狀態**工單(相同工單編號)**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列 Email:（已知:事件等級=1、2 級）

⇨平台寄發相同格式的【通報應變已完成】Email 分別通知

(1)【第一線人員】: 目的在確認確實有發通告。
(2)【區縣市網人員】: 目的在提醒有**通報待審核，**區縣市網需進行審核。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2 級)。

I.2【區縣市網人員】登入平台進行(通報)審核作業

▸注意事項

1. (1、2 級)資安事件，區縣市網人員僅需審核通報流程，毋需審核應變流程。
2. 【區縣市網人員】須於收到**通報審核工單**後 16 小時登入通報平台完成審核。若未能於收到**通報審核工單**後 16 小時內完成審核，則為逾時處理。
3. 逾時處理流程:
   - 平台將於發送審核工單超過 16 小時後寄發第一次【審核已逾時】**Email** 給【區縣市網人員】。
   - 之後每 12 小時寄發【審核已逾時】**Email** 給【區縣市網人員】。

▸(通報)審核作業說明事項

1. 【區縣市網人員】將特別注意事件等級與是否需支援:
   (1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
   (2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。
2. 當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▸【區縣市網人員】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已審核通報作業。

(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=1、2 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】登入平台進行通報審核作業

▸注意事項

1.(1、2級)資安事件，教育機構資安通報應變小組僅需審核通報流程，毋需審核應變流程。

2.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。

▸(通報)審核作業說明事項

1.【教育機構資安通報應變小組】須特別注意事件等級與是否需支援:

(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。

(2)審核事件等級若是通過則按同意，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

2.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個教育部規範之通報流程正式完成。

▸【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 當教育機構資安通報應變小組審核完畢，代表該工單已正式完成結案，所以會產生一**歷史工單**到【所有人員】歷史通報目錄。

✉平台會自動寄發下列 Email:（已知:事件等級=1、2級)。

⇨平台寄發相同格式的【通報已審核】Email 分別通知

(1)【第一線人員】: 目的在告知該通報已正式完成結案。

(2)【區縣市網人員】: 目的在告知該通報已正式完成結案。

(3)【教育機構資安通報應變小組】: 目的告知在該通報已正式完成結案。

(4)【教育部人員】: 目的在告知該通報已正式完成結案。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2級)。。

二、 【告知通報】(1、2 級)處理流程(通報應變分開進行)

本情境所規範之處理流程圖如下：

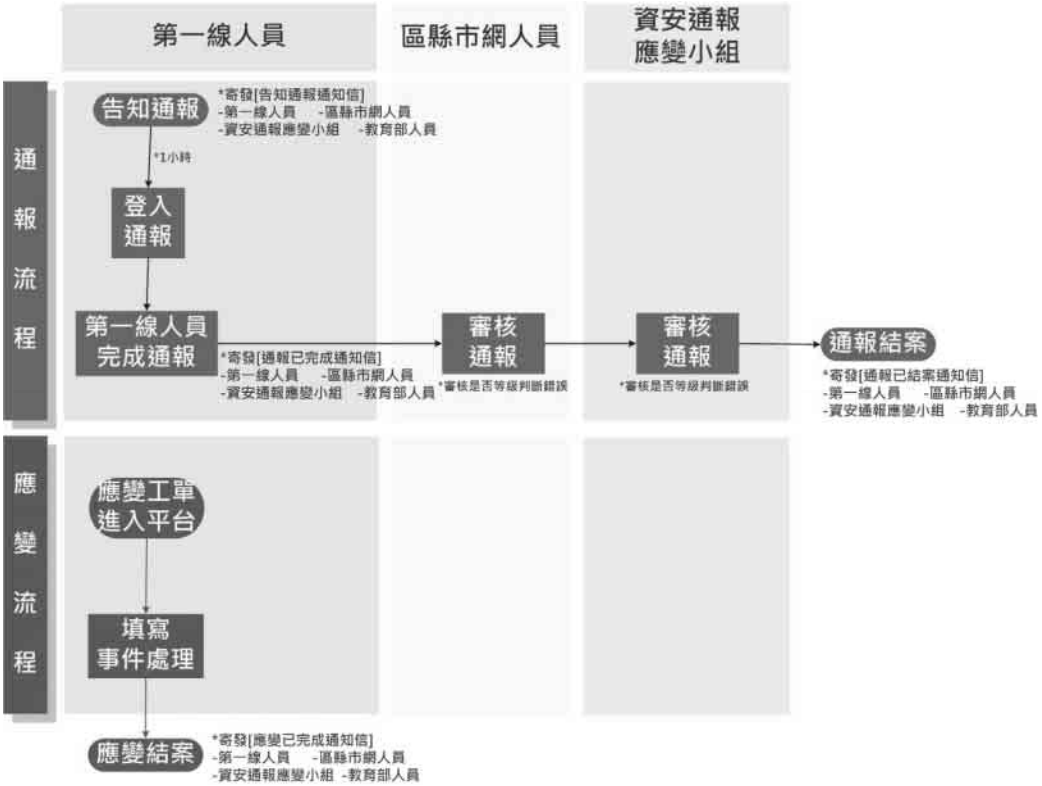
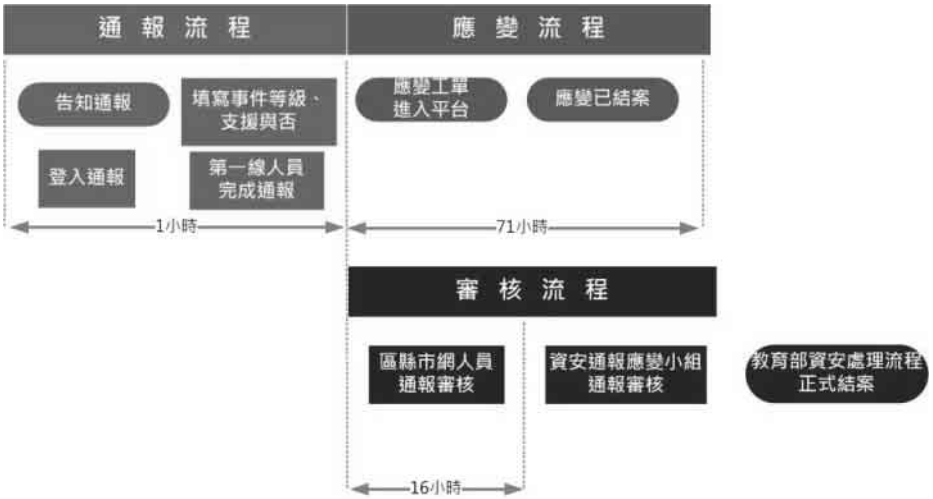


圖 1、2 級告知通報(通報應變分開進行)處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I.通報流程說明：

I.1【第一線人員】登入通報平台進行(通報)作業

【第一線人員】於收到【告知通報】之 Email 或 SMS 簡訊，須於 1 小時內登入通報平台完成通報此資安事件。

▶說明事項

1.資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫
(1)事件等級: 因係 1-2 級通報，故無須電話告知【區縣市網人員】。
(2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2.【第一線人員】完成通報時，按送出結案，便已完成【第一線人員】之通報，此時間即為通報完成時間。

⇨【第一線人員】完成通報流程之時間即為回報給行政院之通報完成時間。

3.完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▶**【第一線人員】完成處理後，平台接續處理事項:**

➡平台會自動產生◎**完成時間：(工單編號於發送工單時就已經產生)**
【第一線人員】可於後續**工單處理狀態**檢視得知◎**工單編號**與◎**完成時間**
➡平台會自動產生下列**工單**
(1)送一**待處理工單(相同工單編號)**到【第一線人員】應變待處理目錄。
(2)一**通報待審核工單(相同工單編號)**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。
(3)產生一處理狀態**工單(相同工單編號)**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列 Email:（已知:事件等級=1、2 級）

⇨平台寄發相同格式的【通報已完成】Email 分別通知

(1)【第一線人員】: 目的在確認確實有發通告。
(2)【區縣市網人員】: 目的在提醒有**通報待審核工單，**區縣市網需進行審核。
(3)【教育機構資安通報應變小組】: 目的在告知與備查。
(4)【教育部人員】: 目的在告知與備查。
➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2 級)。。

I.2【區縣市網人員】登入平台進行(通報)審核作業

▶注意事項

1. (1、2 級)資安事件，區縣市網人員僅需審核通報流程，毋需審核應變流程。
2.【區縣市網人員】須於收到**通報審核工單**後 16 小時內登入通報平台完成審核。
若未能於收到**通報審核工單**後 16 小時內完成審核，則為逾時處理。
3.逾時處理流程:
- 平台將於發送審核工單超過 16 小時後寄發第一次【審核已逾時】Email 給【區縣市網人員】。
- 之後每 12 小時寄發【審核已逾時】Email 給【區縣市網人員】。

▶(通報)審核作業說明事項

1.【區縣市網人員】將特別注意事件等級與是否需支援:
(1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯

誤)則按不通過，並填寫(1)建議等級，與(2)原因。

2.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▶**【區縣市網人員】完成處理後，平台接續處理事項:**

➡平台會自動產生(更新)下列**工單**

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已審核通報作業。

(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=1、2 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】進行(通報)審核作業

▶**注意事項**

1.(1、2 級)資安事件，教育機構資安通報應變小組僅需審核通報流程，毋需審核應變流程。

2.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。

▶**(通報)審核作業說明事項**

1.【教育機構資安通報應變小組】須特別注意事件等級與是否需支援:

(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。

(2)審核事件等級若是通過則按同意，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

2.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個教育部規範之通報流程正式完成。

▶**【教育機構資安通報應變小組】完成處理後，平台接續處理事項:**

➡平台會自動產生(更新)下列**工單**

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【教育機構資安通報應變小組】已完成通報審核作業。

✉平台會自動寄發下列 Email:（已知:事件等級=1、2 級)。

⇨平台寄發相同格式的【通報已審核】Email 分別通知

(1)【第一線人員】: 目的在告知該通報已正式完成結案。
(2)【區縣市網人員】: 目的在告知該通報已正式完成結案。
(3)【教育機構資安通報應變小組】: 目的告知在該通報已正式完成結案。
(4)【教育部人員】: 目的在告知該通報已正式完成結案。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=1、2 級)。

II.應變流程說明：

應變流程開始於應變待處理工單進入到平台的【第一線人員】應變待處理目錄。

II.0 平台會自動檢查是否逾時

▸說明事項

1.1、2 級資安事件【第一線人員】需於 71 小時內處理完成應變並送出審查。
2.3、4 級資安事件【第一線人員】需於 35 小時內處理完成應變並送出審查。

▸平台處理事項:

1.平台會每 1 小時自動檢查是否逾時。若過程(通報流程+應變流程)中處理已逾時，平台會進行應變逾時處理流程。
2. 1、2 級應變逾時處理流程

✉平台將會自動寄發下列 Email:（已知:事件等級=1、2 級）

(1)逾時前 1 小時寄發【將逾時】Email 通知【第一線人員】。
(2)逾時後每 12 小時寄發【已逾時】Email 通知【第一線人員】。

➡平台在此並沒有提供 SMS 簡訊通知。(已知:事件等級=1、2 級）

II.1【第一線人員】登入平台並進行應變處理

▸注意事項

1.當【第一線人員】於一小時內完成通報後，須在於 71 小時內登入平台完成應變處理。

▶說明事項

1.當第一線人員完成通報後，需進入通報平台填寫事件處理情況(應變處理)。
2.第一線人員於填寫緊急應變措施、解決辦法與解決時間後，按發佈應變通報送出結案。
3. 1、2 級資安事件【區縣市網人員】、【教育機構資安通報應變小組】無需進行應變審核。

教育部規範之完整通報與應變流程正式完成結案。

▶【第一線人員】完成處理後，平台接續處理事項:

➡平台將會自動更新【所有人員】歷史通報目錄夾,
【所有人員】可於歷史通報目錄夾看到最新完成與更新後之所有紀錄。

✉平台會自動寄發下列 Email:（已知:事件等級=1、2 級）

⇨平台寄發相同格式的【應變已完成】Email 分別通知

(1)【第一線人員】: 目的在告知與備查。
(2)【區縣市網人員】: 目的在告知與備查。
(3)【教育機構資安通報應變小組】: 目的在告知與備查。
(4)【教育部人員】: 目的在告知與備查。

➡平台在此並沒有提供 SMS 簡訊通知。(已知:事件等級=1、2 級)

三、 【告知通報】(3、4)級通報處理流程(通報應變同時進行)

本情境所規範之處理流程圖如下：

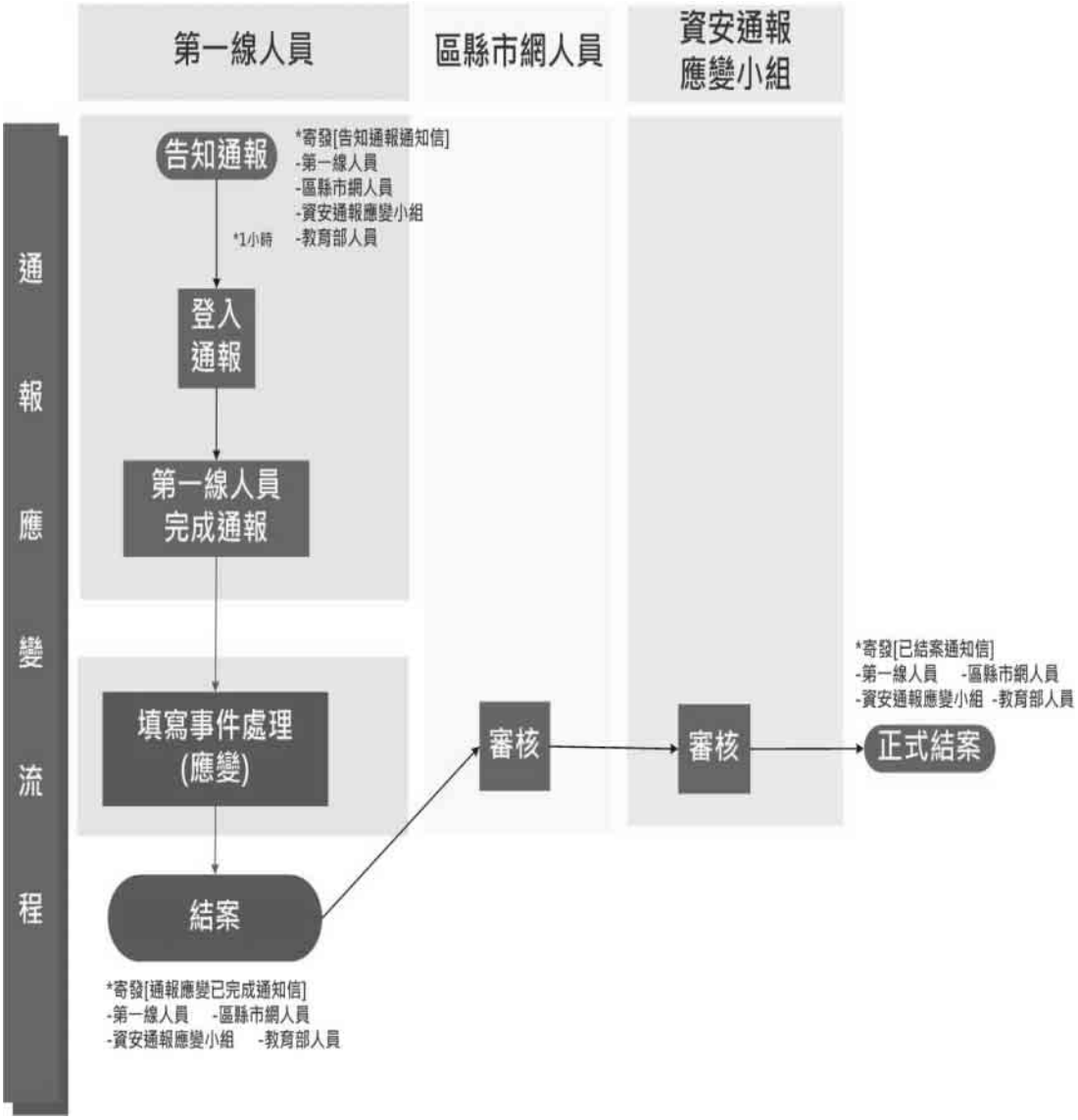
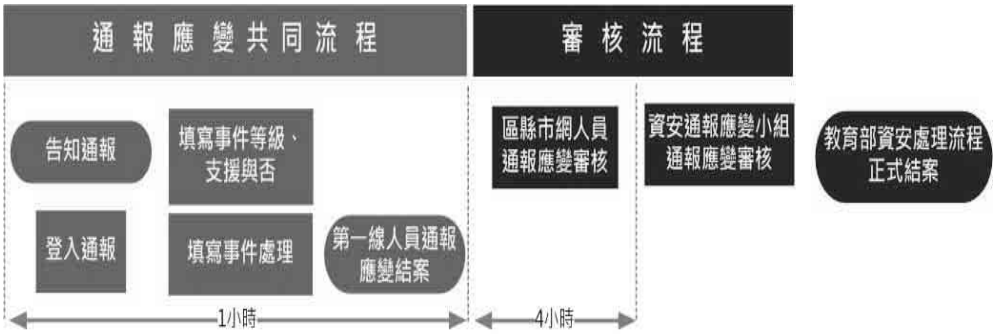


圖 3、4 級告知通報(通報應變同時進行)處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I.通報流程說明：

I.1【第一線人員】登入通報平台進行(通報應變)作業

【第一線人員】於收到【告知通報】之 Email 或 SMS 簡訊，須於 1 小時內登入通報平台完成通報此資安事件。

▶說明事項

1.資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫

(1)事件等級: 因係 3-4 級通報須電話告知【區縣市網人員】及【教育機構資安通報應變小組】。

(2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2.【第一線人員】填完成通報流程後，繼續填寫應變流程，按送出結案，便已完成【第一線人員】之通報應變，此時間即為通報應變完成時間。

⇨【第一線人員】完成通報應變流程之時間即為回報給行政院之通報完成時間

3.完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▶**【第一線人員】完成處理後，平台接續處理事項:**

➡平台會自動產生◎**完成時間：(工單編號於發送工單時就已經產生)**
【第一線人員】可於後續**工單處理狀態**檢視得知◎**工單編號**與◎**完成時間**

➡平台會自動產生下列**工單**
(1)一**通報應變待審核工單**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。
(2)產生一處理狀態**工單**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列 Email:（已知:事件等級=3、4 級）

⇨平台寄發相同格式的【通報應變已完成】Email 分別通知

(1)【第一線人員】: 目的在確認確實有發通告。
(2)【區縣市網人員】: 目的在提醒有**通報應變待審核工單，**區縣市網需進行審核。
(3)【教育機構資安通報應變小組】: 目的在告知與備查。
(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發 SMS 簡訊通知(已知:事件等級=3、4 級)
平台寄發【待審核】簡訊通知【區縣市網人員】，目的在提醒有**通報待審核工單，**區縣市網需進行審核。

I.2【區縣市網人員】登入平台進行通報應變審核作業

▶**注意事項**

1.（3、4 級)資安事件，區縣市網人員需審核通報流程和應變流程。
2.【區縣市網人員】須於收到**(通報應變)審核工單**後 4 小時登入通報平台完成審核。若未能於收到**(通報應變)審核工單**後 4 小時內完成審核，則為逾時處理。
3.逾時處理流程:

- 平台將於發送審核工單超過 4 小時後寄發第一次【審核已逾時】**Email** 給【區縣市網人員】。
- 之後每 12 小時寄發【審核已逾時】**Email** 給【區縣市網人員】。

▶**審核作業說明事項:通報與應變流程皆需審核**

1.通報流程審核：【區縣市網人員】需特別注意事件等級與是否需支援。
(1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。
2.應變流程審核：【區縣市網人員】需特別注意解決辦法是否合適。
若是通過(解決辦法合適)則按通過，若是不通過(也就是說, 解決辦法不合適)則按不通過，並填寫(1)原因。【區縣市網人員】需主動告知(視難易度，採 Email 或電話告知方式)【第一線人員】合適之建議措施並請【第一線人員】進行後續處理。
3.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▶【區縣市網人員】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**
(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已通報審核作業。
(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=3、4 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】登入平台進行審核作業

▶注意事項

1.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。

▶審核作業說明事項:通報與應變流程皆需審核

1.(3、4 級)資安事件，【教育機構資安通報應變小組】需審核通報流程和應變流程。
2.通報流程審核：【教育機構資安通報應變小組】需特別注意事件等級與是否需支援。
(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。

(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。

3.應變流程審核：【教育機構資安通報應變小組】需特別注意解決辦法是否合適。

3、4 級資安事件【教育機構資安通報應變小組】需主動聯絡【區縣市網人員】,就【第一線人員】之解決辦法是否合適進行瞭解。若是通過(解決辦法合適)則按通過，若是不通過(也就是說, 解決辦法不合適)則按不通過，並填寫(1)原因。【教育機構資安通報應變小組】需主動告知(視難易度，採 Email 或電話告知方式) 【區縣市網人員】與【第一線人員】合適之建議措施並請【第一線人員】進行後續處理，請【區縣市網人員】協助【第一線人員】處理。

4.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個通報流程正式完成。

▶【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 產生一**歷史工單**到【所有人員】歷史通報目錄，顯示通報已正式完成。

✉ 平台寄發相同格式的【通報應變已審核】Email 分別通知

(1)【第一線人員】: 目的在告知該工單已正式結案。
(2)【區縣市網人員】目的在告知該工單已正式結案。
(3)【教育機構資安通報應變小組】: 目的在告知該工單已正式結案與備查。
(4)【教育部人員】: 目的在告知該工單已正式結案與備查。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

四、 【告知通報】(3、4)級通報處理流程(通報應變分開進行)

本情境所規範之處理流程圖如下：

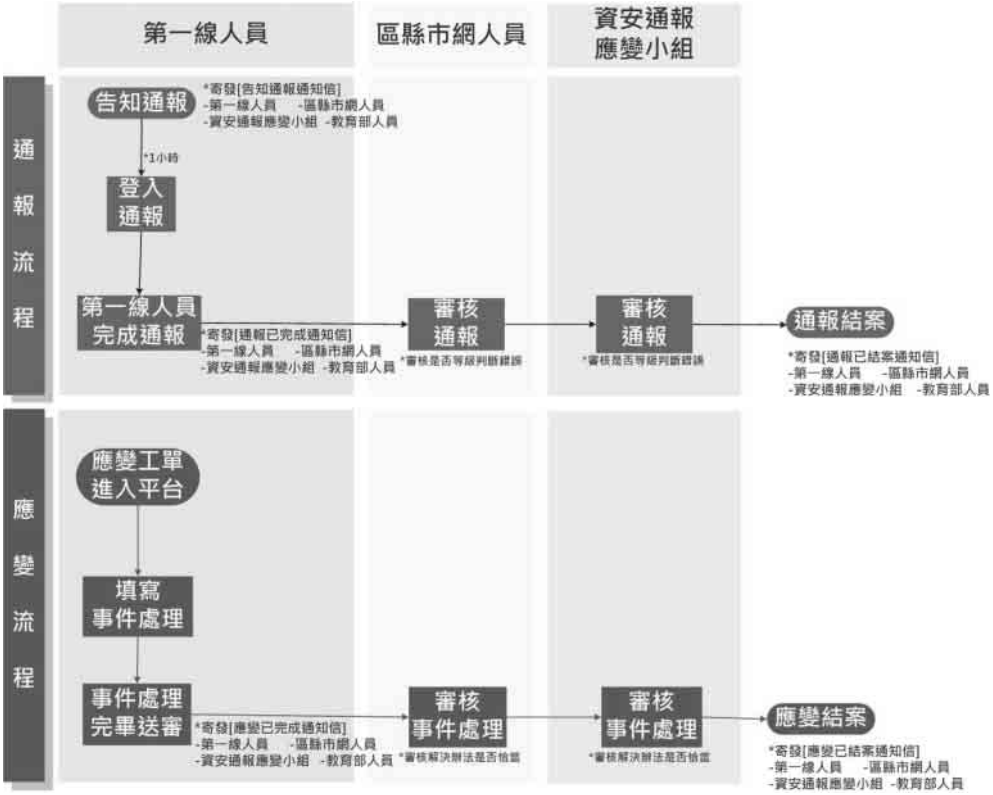
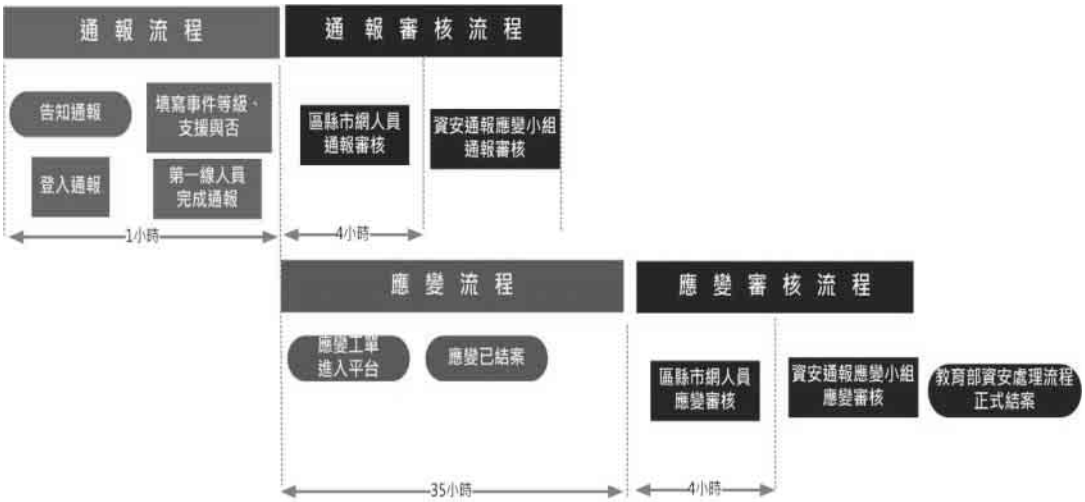


圖 3、4 級告知通報(通報應變分開進行)處理流程

本情境所規範之處理時限如下:



請參考上述規範與底下之說明與敘述。

I.通報流程說明：

I.1【第一線人員】登入通報平台進行(通報)作業

【第一線人員】於收到【告知通報】之 Email 或 SMS 簡訊，須於 1 小時內登入通報平台完成通報此資安事件。

▶說明事項

1.資安事件說明包含受害之系統 IP 等基本資料,請特別仔細填寫

(1)事件等級: 因係 3-4 級通報須電話告知【區縣市網人員】及【教育機構資安通報應變小組】。

(2)是否需支援:若需支援，則主動電話聯繫區縣市網人員請求協助。

⇨完整的工單填寫內容請參考『附件 1：資安工單填寫說明』。

2.【第一線人員】完成通報時，按送出結案，便已完成【第一線人員】之通報，此時間即為通報完成時間。

⇨【第一線人員】完成通報應變流程之時間即為回報給行政院之通報完成時間

3.完整之通報仍待【區縣市網人員】與【教育機構資安通報應變小組】審核結果。

▸【第一線人員】完成處理後，平台接續處理事項:

➡平台會自動產生◎**完成時間**：(**工單編號於發送工單時就已經產生**)
【第一線人員】可於後續**工單處理狀態**檢視得知◎**工單編號**與◎**完成時間**

➡平台會自動產生下列**工單**(已知:事件等級=3、4級)
(1)送一**應變待處理工單**到【第一線人員】應變待處理目錄。
(2)一**通報待審核工單**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。
(3)產生一處理狀態**工單**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列Email:（已知:事件等級=3、4級）

平台寄發相同格式的【通報已完成】Email 分別通知
(1)【第一線人員】: 目的在確認確實有發通告。。
(2)【區縣市網人員】: 目的在提醒有**通報待審核工單，**區縣市網需進行審核。
(3)【教育機構資安通報應變小組】: 目的在告知與備查。
(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發SMS簡訊通知(已知:事件等級=3、4級)
平台寄發【**待審核**】簡訊通知【區縣市網人員】，目的在提醒有**通報待審核工單，**區縣市網需進行審核。

I.2【區縣市網人員】登入平台進行(通報)審核作業

▸注意事項

1.【區縣市網人員】收到**通報待審核工單**後，須於4小時內登入通報平台完成審核，若未能於收到**通報待審核工單**後4小時內完成審核，則為逾時處理。
2.逾時處理流程:
- 平台將於發送審核工單超過4小時後寄第一次【審核已逾時】**Email**給【區縣市網人員】
- 之後每12小時寄發【審核已逾時】**Email**給【區縣市網人員】。

3.(3、4級)資安事件，【區縣市網人員】需審核通報流程和應變流程。

▸(通報)審核作業說明事項:

1.【區縣市網人員】需特別注意事件等級與是否需支援。
(1)若見到需支援的請求,請主動電話聯繫【第一線人員】協助處理。
(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。
2.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▶【區縣市網人員】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**
(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已完成通報審核作業。
(2)一**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=3、4 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

I.3【教育機構資安通報應變小組】登入平台進行通報審核作業

▶注意事項

1.【教育機構資安通報應變小組】須於收到**通報待審核工單**後登入通報平台完成審核。
2.(3、4 級)資安事件,【教育機構資安通報應變小組】需審核通報流程和應變流程。

▶審核作業說明事項:通報與應變流程皆需審核

1.【教育機構資安通報應變小組】需特別注意事件等級與是否需支援。
(1)若見到需支援的請求,請主動電話聯繫【區縣市網人員】要求其協助【第一線人員】處理並了解處理細節。
(2)審核事件等級若是通過則按通過，若是不通過(也就是說,事件等級填寫錯誤)則按不通過，並填寫(1)建議等級，與(2)原因。
2.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個通報流程正式完成。

▶【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**(已知:事件等級=3、4級)

(1) 平台會自動更新【所有人員】的工單處理狀態目錄，顯示【教育機構資安通報應變小組】已完成通報審核作業。

✉平台會提供 Email 通知(已知:事件等級=3、4級)。

平台寄發相同格式的【通報已審核】Email 分別通知

(1)【第一線人員】: 目的在告知。

(2)【區縣市網人員】: 目的在告知。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4級)。

II.應變流程說明：

應變流程開始於應變待處理工單進入到平台【第一線人員】應變待處理目錄，平台會依等級進行不同處理流程。

II.0 平台會自動檢查是否逾時

▶說明事項

1.1、2級資安事件【第一線人員】需於 71 小時內處理完成應變並送出審查。

2.3、4級資安事件【第一線人員】需於 35 小時內處理完成應變並送出審查。

▶平台處理事項:

1.平台會每 1 小時自動檢查是否逾時。若過程(通報流程+應變流程)中處理已逾時，平台會進行應變逾時處理流程。

2. 3、4級應變逾時處理流程

✉平台將會自動寄發下列 Email: (已知:事件等級=3、4級)

(1)逾時前 1 小時寄發【應變將逾時】Email 通知【第一線人員】。

(2)逾時後每 12 小時寄發【應變已逾時】Email 通知【第一線人員】。

➡平台在此並沒有提供 SMS 簡訊通知。(已知:事件等級=3、4級)

II.1【第一線人員】登入平台並進行應變處理

▸注意事項

1.當【第一線人員】於一小時內完成通報後，須在於35小時內登入平台完成應變處理。

▸說明事項

1.當第一線人員處理完畢後，需進入通報平台填寫事件處理情況。
2.第一線人員於填寫緊急應變措施、解決辦法與解決時間後，按發佈應變通報送出結案。
3.教育部規範之完整通報仍待區縣市網與教育機構資安通報應變小組審核結果。

▸【第一線人員】完成處理後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單:**

(1)送一**應變待審核工單(相同工單編號)**到【區縣市網人員】待審核工單目錄，提交區縣市網審核。

(2)產生一處理狀態**工單(相同工單編號)**到【所有人員】工單處理狀態目錄，顯示與追蹤工單之最新處理狀態。

✉平台會自動寄發下列Email:（已知:事件等級=3、4級）

平台寄發相同格式的【應變已完成】Email分別通知

(1)【第一線人員】: 目的在告知與備查。

(2)【區縣市網人員】: 目的在提醒【區縣市網人員】須登入平台處理，【應變待審核】。

(3)【教育機構資安通報應變小組】: 目的在告知與備查。

(4)【教育部人員】: 目的在告知與備查。

➡平台會自動寄發SMS簡訊通知（已知:事件等級=3、4級）

平台寄發【待審核】簡訊通知【區縣市網人員】，提醒【區縣市網人員】須登入平台處理。

II.2【區縣市網人員】登入平台進行應變審核作業

▸注意事項

1.【區縣市網人員】收到**應變審核工單**後須於4小時內登入通報平台完成審核。若未能於收到**應變審核工單**後4小時內完成審核，則為逾時處理。
2.逾時處理流程:

- 平台將於發送審核工單超過 4 小時後寄發第一次【應變審核逾時通知】Email

給【區縣市網人員】

- 之後每 12 小時會再寄發【應變審核逾時通知】**Email** 給【區縣市網人員】。

▸(應變)審核作業說明事項:

1.【區縣市網人員】需特別注意解決辦法是否合適。
2.若是通過(解決辦法合適)則按通過，若是不通過(也就是說, 解決辦法不合適)則按不通過，並填寫(1)原因。【區縣市網人員】需主動告知(視難易度，採 Email 或電話告知方式)【第一線人員】合適之建議措施並請【第一線人員】進行後續處理。
3.當【區縣市網人員】按確定時，代表【區縣市網人員】審核流程已完成。

▸【區縣市網人員】完成(應變)審核作業後，平台接續處理事項:

➡平台會自動產生(更新)下列**工單**

(1) 更新【所有人員】工單處理狀態目錄之處理狀態**工單**，顯示【區縣市網人員】已完成(應變)審核作業。

(2)一應變**待審核工單**到【教育機構資安通報應變小組】待審核工單目錄，提交【教育機構資安通報應變小組】審核。

✉平台在此並沒有提供 Email 通知(已知:事件等級=3、4 級)。

➡平台在此並沒有提供 SMS 簡訊通知(已知:事件等級=3、4 級)。

⇨完整之通報仍需教育機構資安通報應變小組審核結果。

II.3【教育機構資安通報應變小組】登入平台進行應變審核作業

▸注意事項

1.【教育機構資安通報應變小組】須於收到應變**待審核工單**後，需登入通報平台完成審核。

▸(應變)審核作業說明事項:

1.【教育機構資安通報應變小組】需特別注意解決辦法是否合適。
2.3、4 級資安事件【教育機構資安通報應變小組】需主動聯絡【區縣市網人員】，就【第一線人員】之解決辦法是否合適進行瞭解。
3.若是通過(解決辦法合適)則按通過，若是不通過(也就是說, 解決辦法不合適)則按不

通過，並填寫(1)原因。

4.【教育機構資安通報應變小組】需主動告知(視難易度，採 Email 或電話告知方式)【區縣市網人員】與【第一線人員】合適之建議措施並請【第一線人員】進行後續處理，請【區縣市網人員】協助【第一線人員】處理。

5.當【教育機構資安通報應變小組】按確定時，代表【教育機構資安通報應變小組】審核流程已完成，同時整個通報流程正式完成。

▶【教育機構資安通報應變小組】完成處理後，平台接續處理事項:

➡平台將會平台會自動更新【所有人員】歷史通報目錄夾

【所有人員】可於歷史通報目錄夾看到最新完成與更新後之所有紀錄。

✉平台會自動寄發下列 Email:（已知:事件等級=3、4 級）

平台寄發相同格式的【應變已審核】Email 分別通知

(1)【第一線人員】: 目的在告知與備查

(2)【區縣市網人員】: 目的在告知與備查

(3)【教育機構資安通報應變小組】:目的在告知與備查

(4)【教育部人員】:目的在告知與備查

➡平台在此並沒有提供 SMS 簡訊通知。(已知:事件等級=3、4 級)

教育部規範之完整資安處理流程正式結案。

伍、 結論

一、 獎勵制度

為配合教育機構資安通報應變平台之運作，此平台已規劃並完成榮譽排行榜以鼓勵優秀資安人員並提醒尚需加強的單位。

為鼓勵第一線人員與區縣市網人員主動任事的作為，教育部將特別設立獎勵制度以嘉勉表現優良之單位，其獎勵制度將分自行通報與告知通報之處理績效。各級單位每處理完十筆事件即可獲一徽章。教育部第一階段將先收集 3~6 個月的營運資料，並經內部分析與討論後，再就各項方案進行評比與最後決策。

詳細的獎勵制度將以實際營運成果及各級單位之回饋由教育部另行訂定並公告。

二、 新版制定

本手冊將隨不同情況下進行更新與修正。其更新之需求來自於:

(1)行政院(G-ISAC)更新/新增其通報應變格式

由於教育部需回傳相關資安處理情況至行政院(G-ISAC)，因此教育部規劃的通報應變格式需與行政院版一致。因此當行政院(G-ISAC)有增新或修改其分享格式時，教育部(A-ISAC)也必須同步加以適度修正。

(2)教育部營運經驗所提之更新與修正

附件1： 資安工單填寫說明

一、本文件目的:

說明通報應變流程所需填寫之資安工單內容。

二、本文件適用性:通報應變流程所需填寫之資安工單

通報應變流程依照不同資安情報來源可畫分為:(1)自行通報(2)告知通報。

自行通報係由各單位(可以是【第一線人員】、【區縣市網人員】或是【教育機構資安通報應變小組】)自行發現問題時，需主動向上級報告。

告知通報係由其他單位所告知教育部所屬單位所發生之資安事件。告知單位來源包括: (1)ICST(行政院/技服中心) (2)A-SOC(教育部)(3)Mini-SOC(99 年度計畫新增) (4)其他(99 年度計畫新增)

本文件旨在說明上述兩大類型所需填寫之資安工單

三、資安工單的填寫:

教育部規範之通報應變作業分為通報流程與應變流程，教育部鼓勵各單位盡可能通報與應變流程同時進行，以落實緊急應變處理之效。惟處理時間考量下，亦可以通報與應變流程分開進行，先完成通報流程使上級可先掌握資安狀況，第一線人員則可同步進行應變流程。

資安工單的填寫也對應到上述的通報與應變流程。
(I).通報流程: 有二大項目。第一大項: 一、發生資通安全之機關(機構)聯絡資料(使用者無須填寫,系統會自動顯示)及第二大項: 二、各機關因受外在因素所產生資通安全事件時通報事項(七大項,使用者須填寫部分內容)

(II).應變流程: 也有二個項目：(1)緊急應變措施 與(2)解決辦法

底下分別說明這些內容。

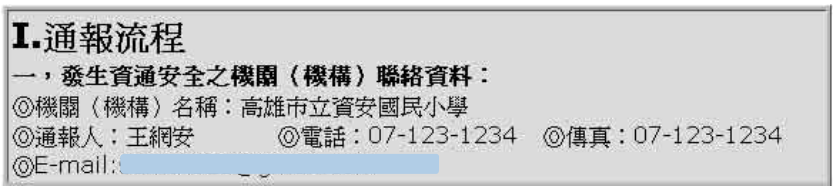
I.通報流程

第一大項: 發生資通安全之機關(機構)聯絡資料

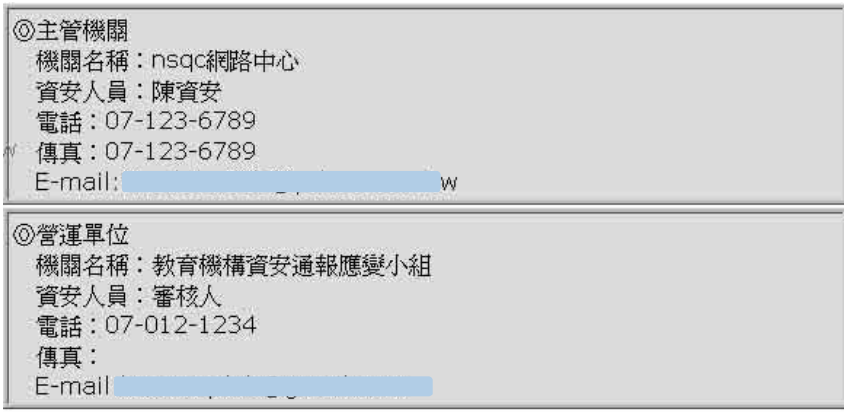
(1)本大項目使用者無須填寫,系統會自動顯示。

(2)當使用者登入後， 系統會自動產生填報時間(此時間即為通報時間)

(3)使用者登入後，系統自動載入通報人資訊



(4)系統也會自動顯示主管機關與教育機構資安通報應變小組聯絡資訊

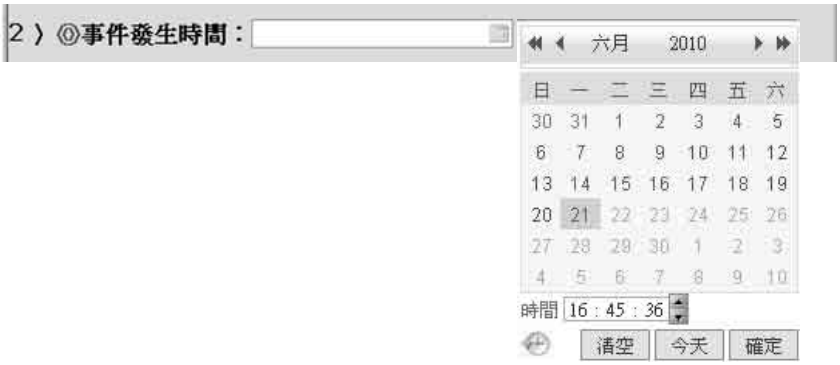


第二大項:各機關因受外在因素所產生資通安全事件時通報事項

1〉通報型態

◆ 使用者無須填寫通報型態,系統會自動顯示：主動通報或告知通報

2 〉事件發生時間:請點選事件所發生時間，通常是點選今天的按鈕即可。



3 〉填寫設備資料: 請盡可能填寫詳盡，以方便上級支援與審核。

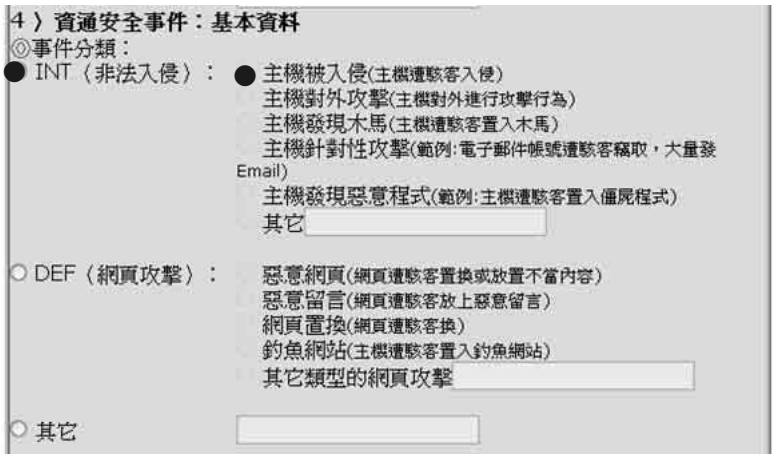
4 〉資通安全事件：

◎事件分類：

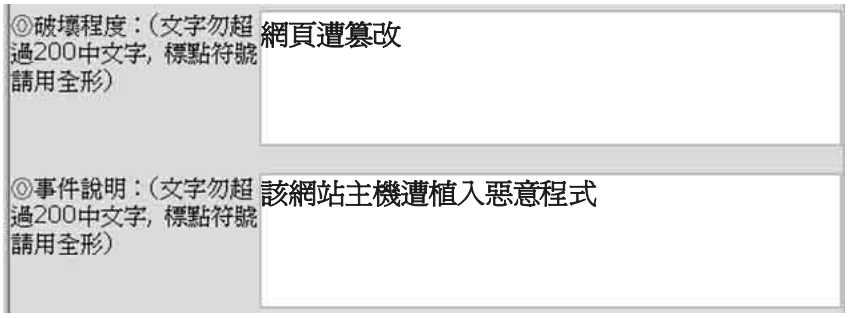
(1)INT(非法入侵)包括：系統被入侵、系統對外攻擊、系統發現木馬、系統針對性攻擊

(2) DEF(網頁攻擊)包括：惡意網頁、惡意留言、網頁置換、釣魚網站

以上事件分類僅能選擇一種，若不屬於上述分類，請選擇其他並填入受攻擊之資安事件。



填寫完事件分類後，請填寫破壞程度與事件說明



5 〉資通安全事件：

在資通安全事件欄位裡，需填寫資安事件判斷與可能影響範圍

資安事件判斷分為(1)機密性衝擊、(2)完整性衝擊、(3)可用性衝擊，就此三大分類在依序判斷事件等級，各分類之詳細事件等級如下所示：

(1)機密性衝擊：

- 無（0級）
- 1級-非核心業務資料遭洩漏
- 2級-非屬密集或敏感之核心業務資料遭洩漏
- 3級-密集或敏感公務遭洩漏
- 4級-國家機密資料遭洩漏

(2)完整性衝擊：

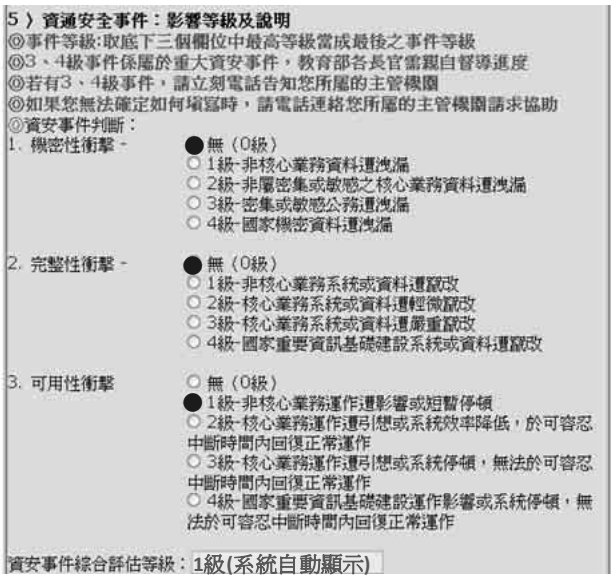
- 無（0級）
- 1級-非核心業務系統或資料遭竄改
- 2級-核心業務系統或資料遭輕微竄改
- 3級-核心業務系統或資料遭嚴重竄改
- 4級-國家重要資訊基礎建設系統或資料遭竄改

(3)可用性衝擊：

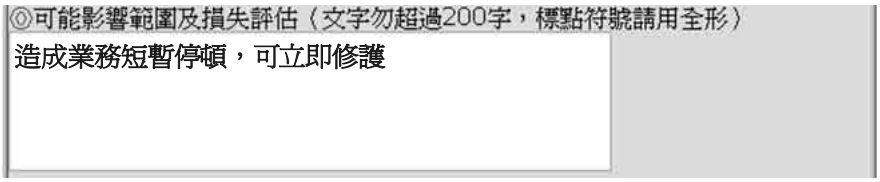
- 無（0級）
- 1級-非核心業務運作遭影響或短暫停頓
- 2級-核心業務運作遭引想或系統效率降低，於可容忍中斷時間內回復正常運作
- 3級-核心業務運作遭引想或系統停頓，無法於可容忍中斷時間內回復正常運作

- 4級-國家重要資訊基礎建設運作影響或系統停頓，無法於可容忍中斷時間內回復正常運作

當使用者判斷完成後，系統會自動顯示資安事件綜合評估等級



填寫完資安事件判斷後，需繼續填寫可能影響範圍

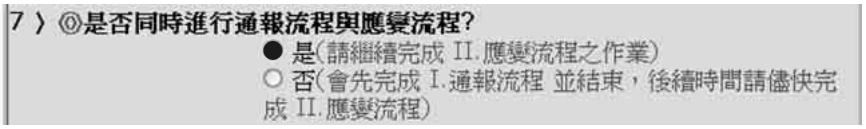


6 〉是否需要支援：

- ◆ 若需支援可與系統顯示之主管機關聯絡人連繫
- ◆ 若無需支援，則直接按否。

7 〉是否同時進行通報流程與應變流程?

- ◆ 若否，此工單會顯示於第一線人員應變待處理欄位等待處理，第一線人員按”發佈通報”後，確定送出該工單，即完成通報流程。
- ◆ 若是，則繼續填寫第二大部分：應變流程



★請注意★

1.2 級資安事件請於 72 小時內完成應變流程

3.4 級資安事件請於 24 小時內完成應變流程

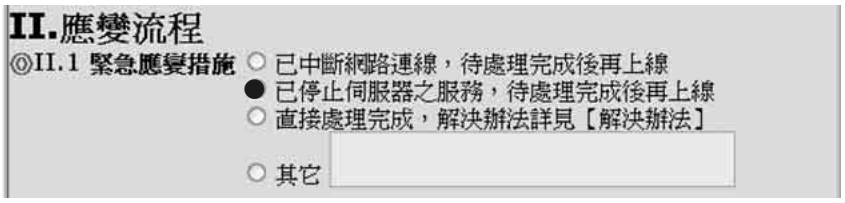
II.應變流程

(1)當第一線人員通報流程與應變流程同時進行時，請直接繼續上述工單之填寫。

(2)當第一線人員通報流程與應變流程分開處理時，需再次登入首頁之應變待處理欄位完成該工單之應變流程(如下圖)

II.1 緊急應變措施

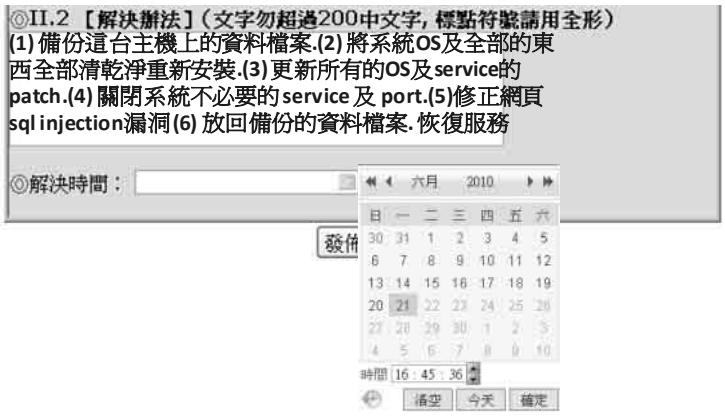
◆ 填寫緊急應變措施



II.2 〉解決辦法

◆ 填寫解決辦法與解決時間

◆ 按”發佈通報”後，確定送出該工單，即完成應變流程。



附件2： Email 格式與範例說明

本文旨在說明資安處理於各種狀態時所寄發的 E-Mail 格式，並依照四種角色提供分類與範例說明（第一線人員(代碼:I)、區縣市網人員(代碼:II)、教育機構資安通報應變小組(代碼:III)、教育部(代碼:IV)）。共分為五種格式:**A.新增告知通報 B.結案通知 C.審核結案 D.逾時通知**

本案所使用之 Email，其收信內容與 Email 格式說明如下：

I. 實際收信內容：

信件主旨:(工單編號:AISAC-23)(事件等級)(完成狀態)通知信

資安聯絡人您好:

此為教育機構資安通報平台所寄發之通知信，旨在確認[高雄市立資安國民小學]已完成事件流程。

通報時間: 2010-03-02 13:50:46
工單編號: AISAC-23
通報機關名稱: [高雄市立資安國民小學]
影響等級: 1 級
事件分類:對外攻擊
事件說明:本單位註冊 IP 210.240.212.239 於 2010/03/01 01:00 ~ 01:04 左右對外進行攻擊行為。

主管機關: nsqc 網路中心
資安聯絡人: 陳資安
聯絡電話: 07-123-4567

事件等級 3.4 級，請於 72 小時內登入教育機構資安通報平台進行應變流程。
事件等級 1.2 級，請於 36 小時內登入教育機構資安通報平台進行應變流程。
若您有任何問題，請與主管機關聯絡,謝謝!

教育機構資安通報應變小組連絡資訊
網址：www.cert.tanet.edu.tw
電話：07-5250211

傳真 07-5250212
E-Mail：boyi@cert.org.tw

II. 內容格式：

上述實際收信內容將以底下內容格式加以敘述，目的在於方便討論與設計。為使資安人員可以快速掌握信件的意義，本附件也提供範例說明來加強資安人員的理解。

信件主旨	（工單編號:AISAC-23)(事件等級)（完成狀態）通知信
收信人	資安聯絡人您好
目的與主旨	此為教育機構資安通報平台所寄發之通知信，旨在確認[高雄市立資安國民小學]已完成事件流程。
事件細節	通報時間: 2010-03-02 13:50:46 工單編號: AISAC-23 通報機關名稱: [高雄市立資安國民小學] 影響等級: 1 級 事件分類:對外攻擊 事件說明:本單位註冊 IP 210.240.212.239 於 2010/03/01 01:00 ~ 01:04 左右對外進行攻擊行為。
主管機關	主管機關: nsqc 網路中心 資安聯絡人: 陳資安 聯絡電話: 07-123-4567
注意事項	事件等級 3.4 級,請於 72 小時內登入教育機構資安通報平台進行應變流程。 事件等級 1.2 級,請於 36 小時內登入教育機構資安通報平台進行應變流程。 若您有任何問題，請與主管機關聯絡,謝謝!
連絡資訊	教育機構資安通報應變小組連絡資訊 網址：www.cert.tanet.edu.tw 電話：07-5250211 傳真 07-5250212 E-Mail：boyi@cert.org.tw

上述表格化之教育機構資安通報應變小組連絡資訊欄位為教育部委外教育機構資安通報應變小組之資訊，對所有的寄發對象都是一樣的，因此後續的討論將不說明此欄位。

A. 新增告知通報 E-Mail 樣式

- **格式：（通報格式)(工單編號)（事件類型）警報**
  - **通報格式：僅適用於告知通報，無自行通報**

- **寄發對象:**(1)【第一線人員】(2)【區縣市網人員】(3)【教育機構資安通報應變小組】 (4)【教育部人員】
- **情資來源：(1)ICST(技服)，與(2)A-SOC**

範例 A1:（第一線人員)收到(告知通報)（工單編號:AISAC-23)(入侵事件)警報

信件主旨：(工單編號:AISAC-23)(通報格式)(入侵事件) 警報

工單編號: AISAC-23

原發布編號	ICST-INT-2010-0122	原發布時間	2010-06-2322:11:53
事件類型	對外攻擊	原發現時間	2010-06-23
事件主旨	高雄市立資安國小資訊設備對外攻擊警訊通知		
事件描述	技術服務中心發現 貴單位註冊 IP 163.16.10.4 於 2010/06/23 左右對外進行攻擊行為。 為避免不必要之資安風險，請針對該系統進行詳細檢查並加強相關防範措施。		
手法研判	該電腦透過 TCP Port 22(SSH 服務)嘗試猜測系統帳號密碼。		
建議措施	回復措施： 由於所得資訊有限，無法明確提供回復措施，請依該系統平台參考相關檢查暨回復措施。 相關建議： 1.檢查防火牆記錄，查看內部是否有對外大量不同目的 IP 之異常連線，特別注意但不限於 TCP Port 22。 2.檢查個別系統上是否有異常連線、異常執行中程序、異常服務及異常開機自動執行程式等，特別注意但不限於正對外開啟 TCP Port 22 連線之程式。 3.注意個別系統之安全修補，若僅移除惡意程式而不修補，再次受相同或類似攻擊的機率極高。修補程式須持續更新，Windows 自動安裝更新程式機制可參考微軟保護電腦三步驟。 4.系統上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除。 5.安裝防毒軟體並更新至最新病毒碼。 6.檢驗防火牆規則，確 認個別系統僅開放所需對外提供服務之通訊埠。 7.若無防火牆可考慮安裝防火牆或於 Windows 平台使用 Windows XP/2003 內建之 Internet Firewall/Windows Firewall 或 Windows 2000 之 TCP/IP 篩選。Linux 平台可考慮使用 iptables 等內建防火牆。		
參考資料	微軟保護電腦三步驟 http://www.microsoft.com/taiwan/security/protect/ 微軟內建防火牆: http://www.microsoft.com/taiwan/security/protect/firewall.asp http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx http://www.microsoft.com/windowsxp/using/networking/learnmore/icf.mspx 微軟相關弱點 http://www.microsoft.com/technet/security/current.aspx		
此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

B.結案通知 E-Mail 樣式

- **格式：(工單編號)(等級)(完成狀態)通知信**
- **等級：區分為(1 級、2 級、3 級、4 級)**
- **完成狀態：有（通報已完成）、(應變已完成)、(通報應變已完成)共三種**
- **此僅限於第一線人完成一筆[自行通報]所寄發的結案通知信件**

範例 B1:（第一線人員)收到（通報已完成)通知信

信件主旨	（工單編號:AISAC-23)(2 級)（通報已完成）通知信
收信人	資安聯絡人您好
目的與主旨	此為教育機構資安通報平台所寄發之通知信，旨在確認[通報機關名稱]已完成事件流程。
事件細節	通報時間: 2010-03-02 13:50:46 工單編號: AISAC-23 通報機關名稱: [高雄市資安國民小學] 影響等級: 2 級 事件分類: 主機針對性攻擊 事件說明:本單位註冊 IP 210.240.212.239 於 2010/03/01 01:00 ~ 01:04 左右對外進行攻擊行為。
主管機關	主管機關: 高屏澎區網中心 資安聯絡人: 王資安 聯絡電話: 07-1234567
注意事項	事件等級 3.4 級,請於 72 小時內登入教育機構資安通報平台進行應變流程。 事件等級 1.2 級,請於 36 小時內登入教育機構資安通報平台進行應變流程。 若您有任何問題，請與主管機關聯絡,謝謝!

C.審核結案 E-Mail 樣式

- **格式：(工單編號)（等級)（審核結案)通知信(審核狀態)**
- **等級：區分為(1 級、2 級、3 級、4 級)**
- **審核狀態：有（通報已審核）、(應變已審核)、(通報應變已審核)共三種**

範例 C1:

信件主旨	(工單編號:AISAC-18)(2 級)(審核結案)通知信(應變已審核)

收信人	資安聯絡人您好
目的與主旨	此為教育機構資安通報平台所寄發之通知信，旨在告知貴單位［工單編號18]已審核結案。 [通報機關名稱]在資安通報平台[工單編號：18]已審核結案。
事件細節	通報時間: 2010-06-28 04:38:03 工單編號: AISAC-18 通報機關名稱:［高雄市資安國民小學］ 影響等級: 2 級 事件分類:對外攻擊 事件說明:本單位註冊 IP 210.240.212.239 於 2010/03/01 01:00 ~ 01:04 左右對外進行攻擊行為。
主管機關	主管機關: 高屏澎區網中心 資安聯絡人: 王資安 聯絡電話: 07-1234567

D.逾時通知 E-Mail 樣式

逾時通知有兩種，分別為(1)(逾時前)(1 小時)通知信、(2)(每 12 小時)(已逾時)通知信、(3)(審核已逾時)通知信，其中(1)與(2)適用人員為【第一線人員】而(3)適用人員為【區縣市網人員】，底下分別加以說明。

(1)(逾時前)(1 小時)通知信

- **格式：(逾時前)(1 小時)通知信**

範例 D1:

信件主旨	(工單編號 AISAC-6)(逾時前)(1 小時)通知信
收信人	[通報機關名稱]資安聯絡人您好
目的與主旨	此為教育機構資安通報平台所寄發之通知信，旨在提醒有一則通報即將逾時。 [通報機關名稱] 在資安通報平台[工單編號：AISAC-6]即將逾時。
事件細節	通報時間: 2010-06-25 15:33:19 工單編號: AISAC-6

	通報機關名稱:[高雄市立資安國民小學] 影響等級: 1 級 事件分類:對外攻擊 事件說明:本單位註冊 IP 210.240.212.239 於 2010/03/01 01:00 ~ 01:04 左右對外進行攻擊行為。

(2)(審核已逾時)通知信

- **格式：(工單編號)(逾時類型)通知信**
- **逾時類型：有(應變審核已逾時)與(通報審核已逾時)兩種**

範例 D2:

信件主旨	(工單編號 AISAC-6)(**通報審核已逾時)通知信**
收信人	[收信單位]資安聯絡人您好
目的與主旨	此為教育機構資安通報平台所寄發之通知信，旨在提醒有一則通報已逾時。
事件細節	通報時間: 2010-3-2 13:50:46 工單編號: AISAC-6 影響等級: 1 級 事件分類:對外攻擊 事件說明:本單位註冊 IP 210.240.212.239 於 2010/03/01 01:00 ~ 01:04 左右對外進行攻擊行為。

附件3： SMS 簡訊格式與範例說明

本文旨在說明資安處理於各種狀態時所寄發的 SMS 簡訊格式，並依照四種角色提供分類與範例說明（第一線人員、區縣市網人員、教育機構資安通報應變小組、教育部）。

➢SMS 簡訊發送原則:

SMS 簡訊發送之原則以有效經費達到最關鍵之流程提醒為主，避免浪費。

➢SMS 簡訊類型:

SMS 簡訊可分為兩大類:

I.新進工單之通知簡訊:包括自行通報與告知通報。

II.作業提醒之簡訊：主要在提醒各單位需進行審核。

底下分別加以說明之。

I.新進工單之通知簡訊:包括自行通報與應變通報

（1） 自行通報：

- 含（資安等級）
- 寄發對象:區縣市網，教育機構資安通報應變小組，教育部人員
- 格式:

新增[資安等級]級通報[影響等級]:[通報單位], [通報人],[連絡電話],[工單編號],需要支援:[是|否]

- 範例 1: [1]級自行通報

新增[1]級通報[輕微資安事件]:[高雄市資安區資安國小],[林資安],[(07)12345678#62321],[11],需要支援:[否]

- 範例 2: [2]級自行通報

新增[2]級通報[一般資安事件]:[高雄市資安區資安國小],[林資安],[(07)12345678#62321],[12],需要支援:[否]

- 範例 3: [3]級自行通報

新增[3]級通報[嚴重資安事件]:[高雄市資安區資安國小],[林資安],[(07)12345678#62321],[12], 需要支援:[否]

- 範例 4: [4]級自行通報

新增[4]級通報[重大資安事件]:[高雄市資安區資安國小],[林資安],[(07)12345678#62321],[12], 需要支援:[是]

(2) 告知通報：

- 不含（資安等級）
- 寄發對象: 所有單位(第一線、區網、營運、教育部)
- 格式:

(告知通報)[受駭單位][事件類型]警訊[工單編號] ,請盡速至平台完成事件處理。

  - 情資來源:現階段以 ICST(技服)與 ASOC 為主

- 範例 1: 來自 ICST(技服)之【INT(非法入侵)】告知通報

(告知通報) [高雄市資安區資安國小][入侵事件]警訊[24], 請盡速至平台完成事件處理。

- 範例 2: 來自 ICST(技服)之【DEF(網頁攻擊)】告知通報

(告知通報) [高雄市資安區資安國小][網頁攻擊]警訊[25], 請盡速至平台完成事件處理。

II.作業提醒之通知簡訊:

➢用途:主要是待審核簡訊，用來提醒相關單位之流程作業

➢發送時機: 第一線人員於 3.4 級[應變流程]完成後，提醒區縣市網人員進行審核作業

➢告知通報與自行通報皆會寄發

➢格式:

(待審核通知) [受駭單位],於[時間(Time)]事件通報完成請在 1 小時內登入平台完成事件審核。

➢範例 1: 提醒區縣市網人員進行審核作業

(待審核通知) [高雄市資安區資安國小]於 2010-04-08 23:05:55 事件通報完成請在 1 小時內登入平台完成事件審核。