敏惠醫護管理專科學校

「資訊安全管理系統」
資通安全情資管理程序書

機密等級：一般

編　　號：IS-MHCHCM-02-016

版本編號：1.0

制訂日期：112.10.30

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說　　明	核准者
1.0	112.10.30	資訊安全執行小組	初版發行	執行秘書

本程序書由資訊安全執行小組負責維護。

目錄：

1　目的

為確保敏惠醫護管理專科學校（以下簡稱本校）對威脅情資之識別，以利採取適當因應措施，降低威脅對本機關造成之傷害或減少同類型威脅的影響，特訂定本程序。本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、可接受之風險，決定最適當之因應方式與預防策略，並從中學習，以達到預防再次發生的目標。

2　適用範圍

本校資訊暨圖書中心資訊組。

3　權責

3.1 資訊安全小組

3.1.1　接受資通安全情資後，應指定資訊安全小組進行情資分析

3.1.2　分析情資來源的事件類型、影響範圍及影響標的

3.2 本校各業務管理單位

3.2.1　依據情資內容進行辦理。。

4　資通安全威脅情資定義

資通安全情資係具有相關性、特殊性、明確發生來源、以及可處理性。依照特性可分為四個層面：策略威脅情資、戰術威脅情資、運作威脅情資以及其他資通安全相關之訊息情資。

4.1 策略威脅情資

策略威脅情資為特定攻擊類型或攻擊者類型。包含：資安事件(Incidents)、策略分析(Strategic Analysis)等。

4.2 戰術威脅情資

戰術威脅情資為攻擊方法、工具或技術等相關資訊。包含：漏洞公告(Vulnerabilities)、最佳實務(Best Practices)等。

4.3 運作威脅情資

運作威脅情資為特定攻擊之細節，包含發生原因與背景等等跡證。包含：威脅預警(Threats)、涉態勢感知(Situational Awareness)等。

4.4 其他資通安全相關之訊息情資

其他潛在或疑似危害資訊安全之情資，包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等。

5 作業程序

5.1 資通安全情資之評估

5.1.1 依據國家資安資訊分享與分析中心 N-ISAC 情資格式說明，說明如下：

5.1.1.1 資安事件(Incidents)

【特定對象情資】與特定對象所屬設備相關之資安事件。

5.1.1.2 漏洞公告(Vulnerabilities)

【通用型情資】針對系統、軟體及服務存在明確或可能造成重大影響之漏洞資訊，如：重大資安漏洞情資。

5.1.1.3 威脅預警(Threats)

【通用型情資】協助組織偵測或阻止資安事件發生之預警防護資訊，如：資安威脅指標情資。

5.1.1.4 涉態勢感知(Situational Awareness)

【通用型情資】提供各式網路攻擊行動與攻擊手法研析等相關資訊，如：網路攻擊活動情資、惡意程式分析報告。

5.1.1.5 最佳實務(Best Practices)

【通用型情資】提供國內外各式之資安實務建議，供各組織學習其經驗之資訊，如：資安防護指引。

5.1.1.6 策略分析(Strategic Analysis)

【通用型情資】提供各式趨勢分析報告，作為組織制訂資安防護相關決策之參考，如：資安威脅防護分析報告、 趨勢分析報告、各國資安策略政策。

5.1.2 本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之評估，包含事件類型、影響範圍、影響標的。如須進行情資處理，則開立資安情資分享處理單列管追蹤，必要時得調整本機關資訊安全管理系統之相關控制措施。

5.1.3 資通安全情資分類評估準用資通安全責任等級分級辦法附表九，識別對本單位之衝擊性，並紀錄於資安情資分享處理單。

5.2 資通安全情資之因應措施

本校對於資通安全情資因應措施，依照資通安全情資之定義進行分項因應。

5.2.1 策略威脅情資：

由資安專責人員判斷有無立即發生可能性，並進行風險評估。如有發生可能，應識別影響範圍，啟動營運持續演練計畫，並通知各單位進行預防處理措施。

5.2.2 戰術威脅情資：

由資安專責人員進行風險評估，並識別影響範圍，通知相關單位進行預防處理措施。

5.2.3 運作威脅情資

由資安專責人員進行風險評估，依照攻擊發生原因與跡證，提出預防處理措施。必要時，通知相關單位進行預防處理措施。

5.2.4 資通安全情資處理

5.2.4.1 資訊組或業務管理單位權責人員依資安情資分享處理單進行各項處理作業。

5.2.4.2 處理完成後回覆資安管理小組

5.2.4.3 資安管理小組進行確認是否已處理完成。

6 相關文件

6.1 資通安全事件通報及應變辦法

6.2 資安情資分享處理單