106年
推動4G應用服務系統推廣委外服務案
4G應用服務系統營運資安參考指引
(V1.0)

執行單位：中華民國資訊軟體協會
中華民國106年08月

修訂歷史紀錄表

項次	計畫資訊			發行紀錄		說明
	年度	版次	修訂日期	版次	日期	
1	106	V1.0	106/08/30			新編
2						
3						

報告摘要

報告名稱	4G 應用服務系統營運資安參考指引
資訊等級	☐機密　☐密　☐內部使用　☒普通
相關撰稿人	張德維、方怡婷、陳鴻棋、李民偉
閱讀對象	☒一般主管　☒資安人員　☒資訊人員　☒一般使用者

內容摘要：

本指引係依循經濟部工業局之「4G 應用服務系統資安推動計畫」，並參考國際相關標準(如 ISO/IEC 27001、CNS29100 等)，編訂「4G 應用服務系統營運資安參考指引」，以資通安全角度，提升系統資安品質及安全防護能力。

本指引共分為前言、4G 應用服務系統基本介紹、4G 應用服務系統營運構面資訊安全要求、結論及參考文獻共 5 部分。第 1 章說明本指引之依據、目的、適用對象、章節架構說明、引用標準及用語與定義；第 2 章介紹 4G 應用服務系統，包括 4G 應用服務系統營運模式與 4G 應用服務系統面臨之安全風險；第 3 章介紹本指引針對系統營運構面資訊安全要求，分別為「事前準備機制」、「事中應變機制」及「事後處理機制」；第 4 章說明本指引之結論；第 5 章參考文獻則詳列本指引所參考的文件或資料。

關鍵詞	4G 應用服務系統、資通安全、系統資安品質

目　次

圖　目　次

表　目　次

壹、前言

一、依據

隨著智慧型手機及平板電腦等行動裝置與應用的普及，行動寬頻網路已經成為民眾生活不可或缺的要素。為提昇資訊國力及民眾生活品質，政府於 2013 年釋出行動寬頻業務(4G)執照，促使行動通訊產業與數位生活邁入新的紀元。值此進入 4G 行動通訊時代，需要積極建構行動寬頻友善的環境，以帶動豐富 4G 內容服務與創新應用服務發展、保障消費者權益。

行政院科技會報辦公室特別會同相關部會規劃「加速行動寬頻服務及產業發展方案」，期使所有民眾早日享受優質且價格合理的高速行動寬頻服務、保障消費者權利及引領 4G 行動寬頻網路的創新應用，推動下世代行動寬頻前瞻技術開發與系統設備佈局。

經濟部工業局之「4G 應用服務系統資安推動計畫」為協助行政院「加速行動寬頻服務及產業發展方案」服務普及類計畫之「4G 應用服務系統」提升資訊安全防護能力，參考國際或產業相關標準及依循工業局 App 基本資安檢測基準，進行系統資安風險評估、檢測及訪查，並提出改善建議，以提升系統資安品質。

「4G 應用服務系統營運資安參考指引(以下簡稱「本指引」)」係依循經濟部工業局之「4G 應用服務系統資安推動計畫」研擬應用服務系統之營運資安參考指引。

二、目的

本指引提供「4G 應用服務系統」營運管理單位就資訊安全各面向進行管理參考，包括 Web 應用服務系統、行動應用 App 軟體（以下簡稱 App）及其後端平臺（以下簡稱 App 後台），供營運管理單位之 4G 應用服務系統營運管理人員、系統開發人員、系統管理人員與資安技術

人員等作為參考，協助其提升資訊安全防護能力及品質。

三、適用對象

本指引之適用對象為 4G 應用服務系統之營運管理單位，希透過本指引讓營運管理單位 4G 應用服務系統之系統開發人員、系統維運人員、資料庫管理人員、系統管理人員、網路管理人員、機房管理人員與資安技術人員等對象瞭解資訊安全防護之重點方向。

四、章節架構說明

於**錯誤! 找不到參照來源。**說明各章節摘要說明，以利 4G 應用服務系統相關人員瞭解本指引使用重點。

表1　章節摘要說明

章節	名稱	摘要說明
壹	前言	介紹本指引之依據、目的、適用對象、引用國際標準及用語定義等說明。
一	依據	說明本參考指引訂定之依據。
二	目的	說明本參考指引訂定之目的。
三	適用對象	說明本參考指引之適用對象。
四	章節架構及說明	即為本章節。
五	引用標準	說明本參考指引之引用標準。
六	用語與定義	說明本參考指引之專有名詞用語與定義。
貳	4G 應用服務系統基本介紹	介紹 4G 應用服務系統之基本架構、

章節	名稱	摘要說明
		營運模式及面臨之安全威脅等資訊。
一	4G 應用服務系統營運模式	介紹 4G 應用服務系統營運模式，包含終端設備、4G 應用程式等面向。
二	4G 應用服務系統面臨之安全威脅	說明 4G 應用服務系統面臨之資訊安全威脅。
參	4G 應用服務系統營運資訊安全要求	從事前準備機制、事中應變機制、事後處理機制等面向說明 4G 應用服務系統之安全要求。
一	事前準備機制	從組織管理面、資料管理面、系統管理面、網路管理面、環境管理面及安全檢測等面向說明 4G 應用服務系統之相關要求。
二	事中應變機制	從資安事件應變與數位元鑑識等流程說明注意與遵循事項。
三	事後處理機制	從資安事件學習以及從資安事件中回復角度說明。
肆	結論	本參考指引之結語。
伍	參考文獻	說明參考文獻。
陸	附件	

資料來源：本計畫整理

五、引用標準

本指引參考國內外資安規範或準則如下：

(一)ISO/IEC 27001：2013

Information technology-Security techniques-Information security management systems-Requirements Information technology

(二)ISO/IEC 27002：2013

Information technology-Security techniques-Information security management systems-Requirements Information technology

(三)ISO/IEC 27017：2015

Information technology-Security techniques -Code of practice for information security controls based on ISO/IEC 27002 for cloud services

(四)ISO/IEC 27018：2011

Information technology-Security techniques-Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

(五)ISO/IEC 29100:2011

Information technology -- Security techniques -- Privacy framework

(六)ISO/IEC 20000-1:2011

Information technology-Service management-Part 1: Service management system requirements

(七)ISO/IE CTR 20000-9:2015

Information technology-Service management- Part 9: Guidance on the

application of ISO/IEC 20000-1 to cloud services

(八)ISO/IEC 27037:2012

Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence

(九)ISO/IEC 27038:2014

Information technology - Security techniques - Specification for digital redaction

(十)ISO/IEC 27034-1:2011 Preview

Information technology - Security techniques - Application security - Part 1: Overview and concepts

(十一)ISO/IEC/IEEE 29119-1:2013 Preview

Software and systems engineering - Software testing - Part 1: Concepts and definitions

(十二)NIST SP 800-144

Guidelines on Security and Privacy in Public Cloud Computing

六、用語與定義

(一)分散式阻斷服務攻擊(DDoS)

利用網路上因為惡意程式而被控制的電腦作為跳板，集中向某一特定的目標電腦發動密集的「拒絕服務」要求，藉以把目標電腦的網路資源及系統資源耗盡。

(二)行動應用 App（Mobile Application）

指一種設計給智慧型手機、平板電腦和其他行動裝置使用之應用程

式。

(三)機敏性資料（Sensitive Data）

指依使用者行為或行動應用程式之運作，於行動裝置及其附屬儲存媒介建立、儲存或傳輸之資訊，而該資訊之洩漏有對使用者造成損害之虞，包括個人資料、通行碼、金鑰、即時通訊訊息、筆記、備忘錄、通訊錄、地理位置、行事曆、通話紀錄及簡訊。

(四)個人資料（Personal Data）

指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動。

(五)復原時間目標(Recovery Time Objective , RTO)

復原時間目標(RTO)係指當系統受到衝擊時造成停機，透過選擇的復原程式或方法進行復原所需的最少時間。

(六)復原點目標(Recovery Point Objective , RPO)

指單位可容許最大的資料損失時間、資料量，來評估多久進行一次備份。

(七)白名單(White-list)

意通過識別系統中的進程或檔是否具有經批准的屬性、常見進程名稱、檔案名稱、發行商名稱、數字簽名，白名單技術能夠讓企業批准哪些進程被允許在特定系統運行。

(八)黑名單(Blacklist)

在網路搜尋引擎最佳化（Search Engine Optimization，SEO）優化當中，搜尋引擎或者義務用戶收集的搜尋引擎拉圾製造者列表，可以用於從搜尋引擎封殺或抵制這些垃圾製造者。

(九)灰名單(Greylist)

灰名單介於黑名單和白名單兩者之間,用解釋型的幕後程式和 SMTP 狀態標記來動態創建黑名單和白名單。

貳、**4G 應用服務系統基本介紹**

近年來在行動網路方面，全球的行動數據流量呈現爆炸性的成長；在智慧終端方面，在無線通訊技術的推波助瀾之下，智慧型終端迅速普及，各類新興服務也如雨後春筍般蓬勃發展中；在雲端應用方面，則可以見到各行各業積極利用巨量資料，結合雲端、社群服務，或發展電子商務，或調整產品製程、優化行銷手法、探索新興商業營運模式。

政府於 2013 年釋出行動寬頻業務(4G)執照,我國行動通訊產業與數位生活將邁入新的紀元。值此進入 4G 行動通訊時代，需要積極建構行動寬頻友善的環境，以帶動豐富 4G 內容服務與創新應用服務發展、保障消費者權益。

4G 應用服務系統營運模式為使用者透過行動終端設備(如：智慧型手機、平板電腦或穿戴式裝置等)，利用「行動應用 App」、「Web 應用系統」或「應用程式介面 API」以 4G 行動通訊與後端服務進行連結，使用娛樂內容、教育內容、文創內容等創新應用服務模式之應用系統。

一、4G 應用服務系統營運模式

4G 應用服務系統營運模式區分為「4G 應用服務系統營運端」與「4G 應用服務系統使用終端」，如下圖所示。

資料來源：本計畫整理

圖1　4G 應用服務系統營運模型

(一)「4G 應用服務系統營運端」

為提供功能並從該領域使用的終端中收集資料所需的服務、平臺、協定及其他技術。通常從終端收集資料，並將其存儲至伺服器環境中。將資料的生動描述在多個使用者介面呈現，使用者就可以瞭解該資料。資料經常採用指標、參數或命令的形式，也可以通過服務基礎設施中生成的 API 交給授權協力廠商。

(二)「4G 應用服務系統使用終端」

包括低複雜性設備、設備和閘道，它們通過多種有線和無線網路將真實世界連接數位世界。終端設備包括智慧型手機、平板電腦與運動感測器等。終端從其周圍的真實環境中收集指標，並以多種形式通過 4G 網路將資料傳輸至「4G 應用服務系統營運端」，通常會接收到回應的指示或行動。

4G 應用服務系統營運管理角色，如下圖所示。

資料來源：本計畫整理

圖2　4G 應用服務系統營運管理角色

二、4G 應用服務系統面臨之安全威脅

由於網路攻擊技術的發展日新月異，跨境服務的需求也日漸提升，對消費者之隱私及資訊安全維護均形成挑戰。當行動寬頻服務深入民眾日常生活時，如何妥適維護消費者權益，保障消費者使用網路服務的品質，安心、安全的進行網路活動，避免受到網路犯罪的侵害，已成為 4G 應用服務系統發展的重要議題。

4G 應用服務系統在終端設備、應用程式與後端服務管理等面向，面臨了外部駭客攻擊、電腦病毒(含勒索病毒)、分散式阻斷服務(DDoS)、社交工程、內部人員操作疏失、資料竊取與電腦設備當機失效等資訊安全威脅，建議 4G 應用服務系統營運管理單位依參考本指引進行管理。

4G 應用服務系統營運的安全議題包含「存取控制」、「身分驗證」、「不可否認性」、「資料機密性」、「資料完整性」、「通訊安全」、「可用性」、「隱私保護」等維度，4G 應用服務系統包括了多種無線網路元素，主要為移動設備端、無線網路之接入網路、無線網路之核心網路與 IP 骨

幹網路或網際網路等四者，故其相關安全風險也多與此四者相關，且現行既有存在於無線網路和網際網路的風險，也將作為一種繼承式的固有風險，由 4G 所概括繼承。

(一)「4G 應用服務系統營運端」對應之資安威脅

1.網路基礎設施攻擊

從網路的角度看，因實體通信網路存在弱點，而通過實體通信網路服務接入點提供的公開服務也存在漏洞。如果在網路中處於高許可權地位，則在通信通道中也會同樣處於高許可權地位。

最常見的攻擊方式是中間人攻擊(Man-in-the-middle attack，MITM)，是指攻擊者與通訊的兩端分別建立獨立的聯繫，並交換其所收到的資料，使通訊的兩端認為正在通過一個私密的連線與對方直接對話，但事實上整個對談都被攻擊者完全控制。在中間人攻擊中，攻擊者可以攔截通訊雙方的通話並插入新的內容。

其他攻擊包括針對正向加密和加密通信分析的攻擊以及旁道攻擊等，必須使用合適的加密協定、演算法和標準降低這些攻擊風險。此類攻擊很難應對，其需要存取網路基礎設施，試圖操縱終端的網路基礎設施，例如 Wi-Fi、乙太網或蜂窩網路，以獲取服務特殊權限管理者地位。

不管是何種類型的攻擊，只要利用相互驗證、正向加密、適當的加密協定和演算法，就可降低該模型的攻擊風險。這樣可使攻擊者無法濫用此基礎設施，或增加此類型攻擊的成本，使普通攻擊者難以實施攻擊。

2.雲服務或伺服器基礎設施攻擊

這些攻擊假定在雲服務或伺服器基礎設施環境中具有一個特殊權限管理者地位。例如，如果攻擊者能夠攻破雲服務網路，就可能

進入正在運行訪客虛擬機器 (Virtual Machine , VM) 系統的主機，這樣可讓攻擊者檢查並修改正運行的 VM 系統。

另一種雲服務或伺服器基礎設施攻擊假定攻擊者可控制與目標 VM 相同的物理伺服器上的 VM，攻擊者可能會使用多種方法攻破伺服器上的其他 VM：

(1)利用 VM 基礎設施的漏洞擺脫訪客身份限制進入主機系統

(2)利用旁道攻擊推斷另一訪客 VM 的金鑰

(3)利用伺服器上的大量資源，強制目標 VM 遷移至攻擊者具有更多控制的伺服器上

雲服務供應商必須充分發揮作用，以降低攻擊者破壞雲服務或伺服器基礎設施的可能性。降低此風險的一種方式就是實施基於容器的架構和獨特的加密身份，該架構能夠將每個容器限定給特定用戶。雖然這是一種資源高度密集型的活動，並且可能產生額外費用，但其能夠削弱攻擊者濫用 VM 基礎設施同時訪問多個使用者或多項服務的能力。

雖然雲服務或伺服器環境中的高許可權地位對訪客 VM 中應用程式的執行構成嚴重威脅，但訪問該位置需具備強大的技能，投入大量的時間和資源。一旦獲得存取權限，攻擊者必須對其長期維護以識別哪些系統包含與其利益相關的 VM。此外，必須能夠在不被雲服務供應商的事件子系統檢測到的情況下監測或更改該 VM。

3.應用程式服務攻擊

應用程式服務層級若遭受攻擊面臨的風險將最大，攻擊者會從對網路基礎設施的攻擊一路到對應用程式自身進行攻擊，應用程式代表著任何產品或服務中最複雜的層級，並且始終存在攻擊者通

過多個技術層提升其許可權的可能。

若要降低攻擊的可能性，請查閱大量記錄應用程式安全的指引（如： OWASP TOP 10 開放網路軟體安全計畫十大弱點），以便盡可能安全地實施應用程式執行架構。

4.隱私與個人資料保護

4G 應用服務系統若會與合作夥伴系統交換使用資料/指標或其他以使用者為中心的元件為整個系統提供增值功能，對於合作夥伴所執行的安全級別應進行要求遵循安全規定，必須對應遞交的資料類型、回應類型以及應如何保護資訊等方面進行風險評估。

亦可通過契約和保險條款減弱法律責任，但由於協力廠商的失職仍可能造成客戶流失。組織不應冒損失業務的風險，而是需評估協力廠商工程團隊，以確定其基礎設施、應用程式和 API 應用的安全級別。若安全級別不足，建議尋找替代合作夥伴。

5.惡意對象

單位必須評估經特定管道傳遞的不同類型的技，決定哪些內容可以傳遞，哪些內容不能向其客戶傳遞。由於惡意軟體形式多樣，從多形態的檔案類型到 Adobe Flash、Java 以及多媒體漏洞，應有防護方法來確保終端使用者的安全。如：監測系統和沙箱管理，以確保系統上呈現的任何軟體沒有被濫用之情形。

6.驗證和授權

合作夥伴通常提供僅特定於某些使用者的服務，可能包括使用者可選擇訂閱的有償服務，單位必須確保技術不會無意間使用憑證以濫用未明確授權給協力廠商服務的許可權。例如，某些平臺 API 允許將許可權限定在用戶接受或拒絕的類別中。這樣可使使用者根據其特定的隱私需求調整使用體驗。若平臺不能提供細化的安

全許可權，應列出其確實要訪問的技術。

團隊必須要求其合作夥伴提供可行的細化許可權，以確保服務的取消不會無意間使得在訂閱取消後仍繼續提供使用者資料訪問。

7.誤報和漏報

檢測和日誌服務是管理安全基礎設施的重要方法，但必須對其慎重評估以防誤報和漏報。監控過程自動發生且存在錯誤，許多使用者可能會由於客戶應用程式或基礎設施異常所引起的誤報而無法使用其合法服務。若不能完全信任所獲取的資料，而應用程式又無法正確評估最安全的行動措施，誤報和漏報可能會造成嚴重後果。單位必須有充足的時間、完備的技術和專業知識進行預防。

(二)「通信網路」對應之資安威脅

(1)實體層之安全議題常包括無線網路連線的議題，主要是探討經由人工進行中間幹擾，並因高態訊號與噪音之比值而停止工作。

(2)通訊網路連線安全議題。

(3)阻斷服務攻擊（Denial-of-Service Attack , DoS Attack）安全議題。

(4)4G 下之 Wi-Fi 無線網路安全議題。

(5)其他潛在議題包括 VoIP 的欺騙誤導通訊、資料竄改、IP 竄改、隱私或通話攔截等。

(三)「4G 應用服務系統使用終端」對應之資安威脅

(1)4G 移動設備端於平臺層面對應之資安風險

A.移動設備端於硬體層面，常見於平臺的架構中，對於完整性及驗證機制的考量，使其中的模組易因惡意攻擊而受竄改。

B.硬體於各種通訊埠較缺乏完整性與機密性之考量，使其資料

易受竊聽或竄改。

C.既有的移動設備端平臺較缺乏存取控制機制，常使移動設備端的遺失所釀成的損失驚人。

(2)移動設備端使用不同類型的作業系統，這使得最後的 4G 架構需承擔各種作業系統遺傳而來的各類型漏洞。

(3)當受硬體支持的應用不斷增加時，其各式應用本身之安全潛在風險或漏洞，都將進一步遺傳至所使用之 4G 系統；此外，更多的應用也代表了更多受惡意程式攻擊的管道，使系統本身所身處的環境暴露在更高的風險中。

(4)使用者對於移動設備端的組態設定自由度隨著時代潮流而趨向開放，但設定者的資訊安全認知與能力不一，而不恰當的組態設定可能致使安全性下降。

(5)因時代變遷而進步的技術，移動設備端開始擁有比擬甚至超過十至二十年前的個人電腦之運算能力，也使得各種移動設備端變成新興的攻擊工具，並被惡意人士利用執行非法或惡意行為。

(6)移動設備端在功能性提升的同時，便捷性也逐步提高，包括體積的縮小，但也因此使得遺失或被竊的機率大幅增高，但與之相對的身分鑑別或相關安全機制卻未必完善。

(7)防毒軟體並未跟上使用者從個人電腦轉移至移動設備的潮流，而跟著一併在各式移動設備端廣為佈署。

(8)使用者可在不同的系統間切換，但其架構之安全性常有思考欠周現象。

(9)4G 網路常需連接不同架構的非 IP 網路和 IP 網路，但 QoS 的考量則常被犧牲。

(10)在不同的無線網路架構間，通常有不同的安全機制、安全協議和安全系統。

(11)不同無線網路架構間的介接。

(四)4G 應用服務系統安全威脅與控管領域

4G 應用服務系統於「4G 應用服務系統營運端」、「通信網路」與「4G 應用服務系統使用終端」等面向面臨之安全威脅，如：網路基礎設施攻擊、雲服務或伺服器基礎設施攻擊或應用程式服務攻擊等，應以資訊安全強化機制進行控管，建議以下表各項對應控管領域進行強化措施之設計與實施。

表2　4G 應用服務系統安全威脅與控管領域

營運模式	安全威脅	控管領域對應章節說明
4G 應用服務系統營運端	網路基礎設施攻擊	3.1.4.1. 網路安全架構
	雲服務或伺服器基礎設施攻擊	3.1.3.5. 雲端環境安全管理
	應用程式服務攻擊	3.1.3.1. 系統安全開發管理
	隱私與個人資料保護	3.1.2.1. 資料產生與取得
	惡意對象	3.1.6.2. 應用系統滲透測試 3.1.6.3. 應用系統弱點掃描
	驗證和授權	3.1.3.2. 作業系統管理 3.1.3.3. 資料庫管理系統管理
	誤報和漏報	3.2.1. 資訊安全事件管

		理
4G 應用服務系統使用終端	使用終端安全威脅	3.1.6.1. 行動應用 App 安全檢測

資料來源：本計畫整理

三、4G 應用服務系統營運資訊服務管理

為持續提升 4G 應用服務系統之服務品質，滿足使用者需要，除提供符合需求的服務外，更須提供使用者不中斷的服務，因此穩定可靠的資訊系統為 4G 應用服務系統營運管理單位核心競爭能力的重要來源，但徒有資訊系統尚無法達到前項要求，惟有良好的資訊系統生命週期之整體維運管理機制，方可達到穩定可靠的要求。

4G 應用服務系統營運管理單位宜逐步以服務為導向，規劃與建置資訊服務品質監控與持續改善整體流程之管理體系。

(一)資訊服務管理介紹

資訊服務管理為資訊服務提供與支援之整體管理體系架構，係以結構化且有效率的資訊科技服務提供與管控流程設計，建構可提昇資訊系統服務可靠度及整體資訊服務品質之整合性管理體系。

具體流程包括兩大類：

1.資訊服務支援（Service Support）管理流程：

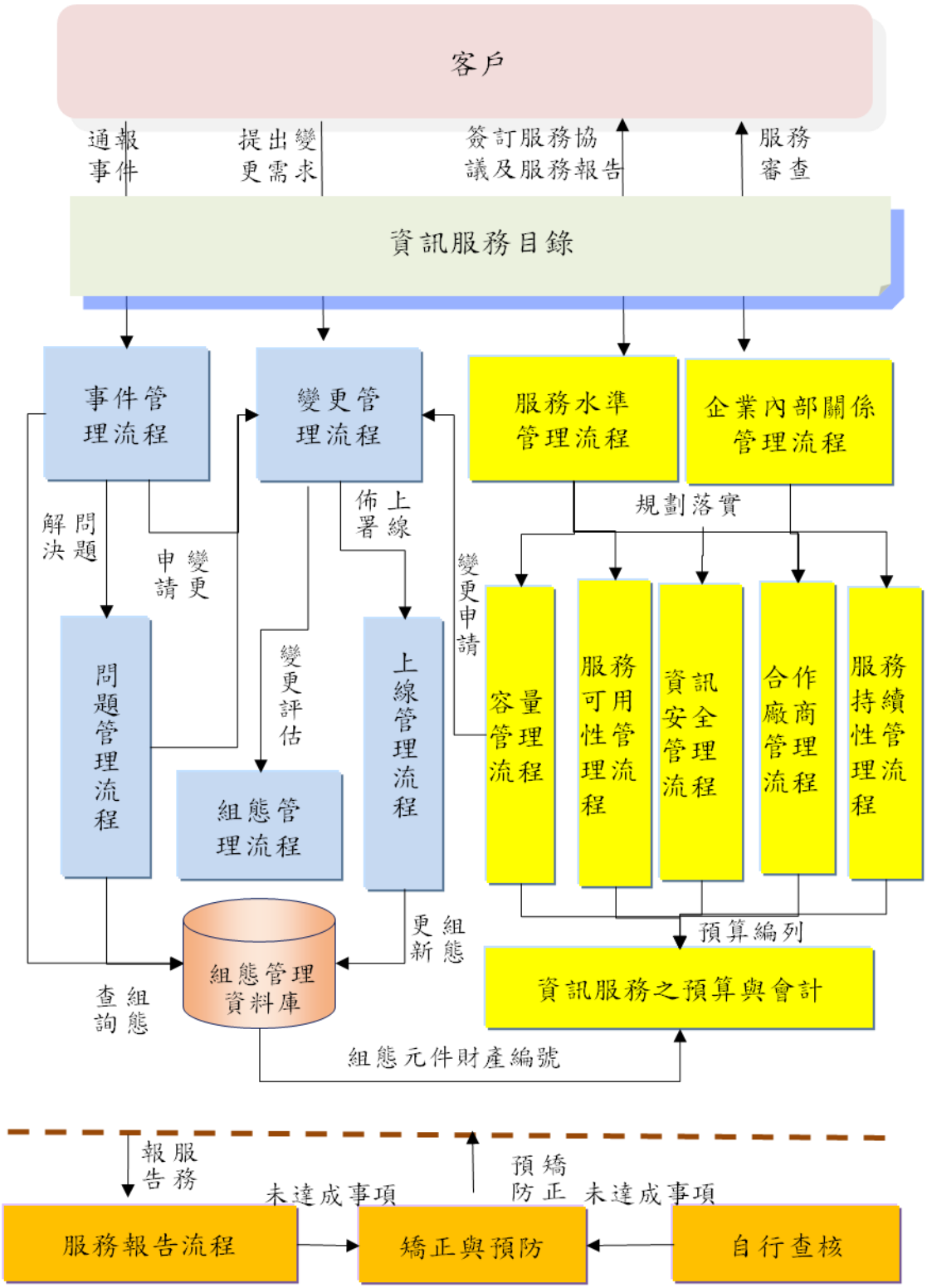
著重於提供反應式之資訊系統服務運行之作業流程，偏重操作面，代表回應使用者之需求，包括事件管理、問題管理、變更管理、上線管理及組態管理等流程，並以組態管理資料庫（Configuration Management DataBase：以下簡稱 CMDB）作為各流程間以資訊服務為導向之組態資訊彙整平台，各流程則分別依流程特性訂定各類可量化之關鍵績效指標，作為具體評估資訊服

務管理流程成效之依據，同時以服務窗口作為使用者與資訊服務平台間之主要聯繫管道。

2.資訊服務交付（Service delivery）管理流程：

著重於提供主動式之監控與規劃作業流程，偏重於策略面， 代表主動提供給使用者適切之服務，用以達到資訊服務水準協議（Service Level Agreement：以下簡稱 SLA）所需執行之作業流程，包括服務水準管理、可用性管理、服務持續營運管理、容量管理及財務管理等流程，經由資訊 4G 應用服務系統營運管理單位與使用者代表研議訂定之 SLA 作為使用者所要求之業務整體服務品質具體指標，本類各項流程則為達到各 SLA 指標所需投入資源之規劃與管理程序。

資訊服務管理流程如下圖所示。



資料來源：本計畫整理

圖3　資訊服務管理流程示意圖

(二)資訊服務管理建議

1.資訊服務之新增、終止及重大異動

(1)針對資訊服務之新增及重大異動，宜事先進行可行性評估及先期規劃之前置作業，用以判斷資訊服務需求之可行性，進而訂定執行目標與方法；針對資訊服務之終止，則宜先進行可行性評估。

(2)針對新服務或服務異動(含服務之終止)，宜透過正式之變更管理規劃並經核可。

(3)新服務或服務變更宜於正式環境實施前依規定核可。

(4)宜事先擬定變更管理規劃，並須包含：

A.實施、操作及維護之角色與責任。

B.對於資訊安全、資訊服務管理制度及資訊服務之影響。

C.與利害相關團體之溝通結果。

D.相關之時程、流程、監控方式、管理方法及工具。

E.合約或服務水準協議修改之必要。

F.針對新服務運作情形或預期效益，宜設定量化管理績效指標。

G.對於新服務或服務異動完成後之驗用方法。

H.對於新服務或服務異動之預算、人力需求。

I.對於新服務或服務異動之技能及訓練需求。

2.服務水準管理

(1)透過資訊服務目錄說明提供之資訊服務與內容，並訂服務水準協議，取得對於資訊服務管理目標之共識。

(2)依據資訊服務水準協議，管理資訊服務流程，並確保資訊服務達成需求。

(3)服務水準協議之異動宜有正式之變更管理管控。

(4)服務水準協議宜定期進行審查，以確保服務水準協議維持在最新及有效狀態。

(5)服務水準宜進行監控並與目標進行比較，以顯示現況及趨勢資訊。

3.資訊服務預算與會計管理

(1)4G 應用服務系統營運管理單位對於下列事項宜有明確之程序：

A.與資訊服務相關資源(例：人力、軟硬體等)之預算與會計。

B.分攤專屬成本及分配共用成本至資訊服務。

C.有效之財務控制及授權。

(2)4G 應用服務系統營運管理單位宜彙整資訊服務預算，以做為有效之財務控制與決策。

(3)宜檢視資訊服務的財務預測與成本支出，用以分配資訊服務的預算與成本之編列；資訊服務的預算宜適度考量服務水準要求。

4.容量管理

(1)宜分析現行資訊服務之容量狀況，並規劃未來使用資訊設備及資源需求，確保資訊服務符合需求之變動。

(2)資訊服務之容量規劃宜考量其服務水準要求。

(3)宜透過容量管理評估下列項目：

– 企業需求。

A.目前與預測之容量與效能要求。

B.鑑別升級時所需時程、臨界值與成本。

C.就預期之服務升級、變更請求、新科技及容量相關技術評估其影響。

D.預測外部變更之衝擊，如：法令。

E.可用於能夠執行預測性分析之資料與流程。

(4)宜監控服務容量並調整服務效能，確保有適當容量提供服務之運作。

5.服務持續性與可用性管理

(1)確保協議之服務水準，滿足企業服務持續運作及其可用性。

(2)宜考量其資訊服務水準要求。

(3)宜發展可用性與服務持續計畫，確保內容已考量從一般異常到服務中斷之不同狀況，並應執行年度審查。

(4)可用性和服務持續計畫宜於業務環境發生重大變化時重新測試。

(5)宜確保當辦公場所無法使用時，服務持續計畫、聯絡清單與組態管理資料庫仍可被取得。

6.資訊安全管理

(1)宜依資訊安全管理制度，管理各項資訊服務所涵蓋之資訊安全議題。

(2)應執行資訊安全控制措施，管理與資訊服務相關之風險。

(3)宜依據事件管理流程通報並記錄資訊安全事件;且有適當程序以

確保所有資訊安全事件被調查，並採取相關行動。

(4)宜有適當機制以量化並監控資訊安全事件與故障之類型、數量及衝擊。

7.企業內部關係管理

(1)4G 應用服務系統營運管理單位宜鑑別及建立服務之利害關係人與客戶清單。

(2)4G 應用服務系統營運管理單位宜透過服務審查會議，討論服務績效、達成情況、問題與行動計畫；並於年度終了前討論服務範圍、服務水準協議、合約及企業需求之變更。

(3)4G 應用服務系統營運管理單位宜注意企業需求之重大異動，並做好回應之準備。

(4)藉由了解使用者需求及其業務特性，與其建立並維持良好之互動關係。

(5)4G 應用服務系統營運管理單位宜建立適當之服務抱怨程序，並執行抱怨記錄、調查及結案程序；當無法透過正常管道解決時，4G 應用服務系統營運管理單位宜提升處理層級。

(6)4G 應用服務系統營運管理單位宜指派專人負責管理客戶滿意度及企業內部關係流程，確保可從定期客戶滿意度中獲得回饋；並將任何已鑑別之措施紀錄，做為服務改善計畫之輸入。

8.合作廠商管理

(1)宜有書面化之管理流程，以維持高品質之資訊服務。

(2)宜有效協調使其合約協議與服務水準協議一致。

(3)宜將其與分包廠商之角色及關係書面化；其對分包廠商履約之

部分，應負完全責任。

(4)針對資訊服務合作廠商之契約，宜定期進行一次審查，確保契約與本行需求間之適用性。

(5)宜採用適當程序處理其服務之正常結束及提前結束。

(6)宜依據其服務等級目標進行監測並審查績效。

9.事件管理

(1)宜記錄所有事件，並透過有效之管理程序，儘速將資訊服務回復至正常運作狀態。

(2)宜確認程序已定義事件記錄、優先順序、企業衝擊、分類、更新、升級、事件解決及事件結束之流程活動。

(3)宜回覆客戶已通報事件或請求之進度；若可能無法達到服務水準時，應通知客戶並採取適當行動。

(4)宜確保所有涉及事件管理之同仁可存取相關資訊，包括：已知錯誤、問題解決方案及組態元件資料庫。

(5)重大事件宜根據已制定之流程進行分類與管理。

10.問題管理

(1)宜記錄所有問題，並以根因分析及管理機制，降低服務中斷之情形及異常事件之發生。

(2)宜確認程序已定義問題記錄、分類、更新、升級、解決與結束之流程活動。

(3)宜採取預防措施以減少潛在問題，如進行趨勢分析。

(4)透過變更管理流程採取矯正潛在根因或解決該問題所需之變

更。

(5)宜監測、審查及報告問題解決之有效性。

(6)問題管理宜負責確保事件管理可使用已知錯誤及已矯正問題等最新資訊。

11.組態管理

(1)宜定義與控制支援資訊服務之重要組態元件，並維持其正確性。

(2)組態元件宜定義財務資產會計流程之介面。

(3)資訊服務與基礎架構中之組態元件宜能被鑑別、控制及追蹤；控制程度應滿足企業需求、失效之風險、關鍵性服務。

(4)宜提供變更管理流程對資訊服務與基礎架構之變更衝擊資訊。在適當情況下，宜可追蹤及查核組態元件之變更。

(5)宜在資訊服務重大異動前執行組態元件之基準點(Baseline)。

(6)宜將組態元件之實體置於管制環境中。

(7)宜確保每一組態元件為唯一可識別，並記錄於受管制之組態管理資料庫中，且該組態管理資料庫已被確保其可靠性與正確性，並提供下列資訊：

A.組態元件之狀態及關聯性。

B.組態元件之版本。

C.組態元件之位置。

D.相關變更與問題。

E.相關之文件。

12.變更管理

(1)對於服務與系統架構之變更，宜具有明確書面化定義之範圍。

(2)宜記錄所有變更請求並加以分類，並應對變更請求評估其風險、衝擊與企業利益。

(3)流程中宜包含變更失敗時之還原或補救方式。

(4)變更宜被核准並以可控制之方法實施。

(5)宜制定程序以控制緊急變更之授權與實施。

(6)所有已核可之變更及其提議實施之時程宜予以維護，並向所有相關團體溝通。

(7)變更紀錄宜被定期分析以偵測變更之增加、經常重複發生之類型、浮現之趨勢及其他相關資訊；並將變更分析之結果及結論予以記錄。

13.上線管理

(1)將變更管理所變更之組態元件，發佈至正式環境運作。

(2)宜擬定上線管理書面程序。

(3)4G 應用服務系統營運管理單位宜規劃服務、系統及軟硬體之發佈；並與相關團體協議上線計畫。

(4)上線計畫宜包含如何取銷及補救上線方法、上線日期暨可交付之事項。

(5)上線計畫宜提及相關之變更需求、已知錯誤問題；上線管理流程應提供適當資訊至事件管理流程。

(6)宜建立受控管之可接受測試環境(Acceptance Test Environment)。

(7)宜制定程序以控制緊急上線之授權及實施。

(8)上線與發佈活動宜被設計及實施，以確保在安裝、處理、封裝、交付時，能保持軟硬體之完整性。

(9)宜量測上線之成功與失敗，包括：在上線之後與上線有關之事件、評估對企業、資訊營運與支援人力資源之衝擊；並將結果輸入改善服務之計畫。

14.服務報告管理

(1)宜定期產出資訊服務報告，用以促進管理階層制定決策與進行有效之溝通。

(2)服務報告中之發現事項宜與相關團體進行溝通。

(3)服務報告宜包括：

A.績效與服務水準目標之對照。

B.不符合與問題。

C.工作量特性。

D.重大服務事件後之績效報告。

E.趨勢資訊。

F.滿意度分析。

4G 應用服務系統營運單位宜持續推動資訊服務管理工作，以提升資訊服務管理制度之執行成效及效率，進而提供使用者更快速、更即時、更穩定且符合使用需求的資訊服務，以應業務發展所需。

參、4G 應用服務系統營運資訊安全要求

一、事前準備機制

本指引針對「事前準備機制」資訊安全要求，分別從「組織管理面」、「資料管理面」、「系統管理面」、「網路管理面」、「環境管理面」及「安全檢測」等面向說明 4G 應用服務系統之相關要求。

(一)組織管理面

1.資訊安全政策

4G 應用服務系統之營運管理單位應訂定資訊安全政策，研訂資訊作業之安全水準，並以書面、電子或其他方式通知員工及與其連線作業之有關單位與廠商。

(1)資訊安全係指為達到資訊作業之正確性、機密性、完整性及可使用性所進行之各項防護措施及危機處理等相關事宜。

(2)資訊的存取與資產的使用，須獲取正式授權，除職務所需外，嚴禁擅自存取使用。對於客戶資料採行正式的存取管制與認證程式，以維護其機密性。

(3)宜建立資訊服務系統使用狀況之監控程式，隨時發掘系統潛在風險。

(4)應建立資訊傳輸及儲存之安控機制，必要時輔以密碼學技術，以加強資訊之機密性及完整性。

(5)宜事先規劃與測試演練，降低系統故障或安全事故所導致的風險，提昇系統可用性。

(6)對於有發生安全事故、安全弱點及違反安全政策與程式之虞

者，應隨時保持警戒。

(7)應建立通報系統，安全事故發生時依規通報。

(8)嚴禁安裝、使用、下載非法或未取得授權之軟體。

(9)應建立防範病毒、惡意軟體等相關程式。

(10)訂定業務永續經營計畫，並測試演練，維持其適用性。

(11)對未經授權擅自使用資訊系統或違反安全政策者，經查屬實將衡酌情節依規議處。

(12)應經常辦理資訊安全教育訓練及宣導，以提昇員工資訊安全之認知及管理能力。

2.資訊安全管理權責

(1)4G 應用服務系統之營運管理單位應訂定保護個人資訊資產及執行特定資訊安全作業，有關人員應負之責任。

(2)應訂定有關人員在資訊安全作業應扮演之角色，責任分配之一般性指導原則，以作為各單位之權責分工依據。

(3)每一 4G 應用服務系統應指定系統擁有者，並課予必要的安全責任。

3.人員安全管理

(1)營運管理單位各項資訊作業活動之工作分配應依員工個人之專業技能做適當權責分工，並預防未經授權存取之行為，以杜絕舞弊。

職位風險指派反映人事管理單位的政策和指導。風險指派可以指導和通知人員存取機關資訊和資訊系統時收到的授權類型。職位篩選標準包括明確資訊安全角色任命需求(如訓練或安全

許可等)。

人員篩選和複篩活動反映適用的法規命令與行政規則(含規範與指引等文件)和建立指定職位風險指派的具體標準。基於系統處理、儲存或傳輸資訊的種類，營運管理單位可以為人員存取資訊系統定義不同的複篩條件和頻率。

(2)若因人力不足而有兼任之情形時，須採取適當之補償性控制措施，如留存操作稽核軌跡或人員陪同作業等。

(3)重要職務人員應設置代理人制度，以確保營運作業不中斷。

(4)人員離(調)職應辦理移交事項及帳號權限之移除作業。

資訊系統相關的財產包括：硬體鑑別符記、系統管理技術手冊、鑰匙、識別證和建物通行證等。離職面談應確保離職人員瞭解離職所產生的安全限制和資訊系統相關財產適當的可歸責性。離職人員的安全議題，包括提醒保密協議和在未來的就業潛在的限制。

某些離職人員可能無法進行離職面談，例如：放棄工作、疾病及不適任等相關因素。離職面談對人員的安全許可非常重要。由於個人因素而及時執行終止行動是必要的。在某些情況下，營運管理單位應考慮通知人員離職前先行終止該員資訊系統的帳號。

(5)營運管理單位所有員工對於與工作上資訊安全相關之法令要求，應有所瞭解並依據相關規定辦理。

營運管理單位元制裁程式應反映適用的法規命令與行政規則(含規範與指引等檔)。制裁程式在存取協議中描述，可做為營運管理單位元人事政策和程式的一部分。

(6)協力廠商人員安全

協力廠商供應商包括：服務中心、承包商、和提供資訊系統的開發、資訊技術服務、外包應用和網路及安全管理的其他單位等。營運管理單位宜將人員的安全要求明確納入採購相關檔。協力廠商供應商可能有人員在機關設施工作，擁有機關發布的憑證、徽章，或資訊系統權限。協力廠商人事變動通知可以確保及時的終止權限和憑證。營運管理單位定義人員調動或離職須報告的安全相關特性包括：職能、角色和與人員調動或離職相關憑證或權限的性質。

4.資訊安全教育訓練

營運管理單位基於特定需求和已獲授權存取資訊系統的人員，來決定安全認知訓練和安全認知技術適當的內容，其內容包括對資訊安全基本認知和使用者維護安全所應採取的行動，如何回應可疑的安全事件，以及作業安全認知等。而提昇安全認知的作法包括：資安警語、海報、電子郵件公告/通報、顯示於登錄螢幕、桌面及螢幕保護程式上的資訊，以及進行資訊安全認知事件演練等。

(1)為資訊作業需要或提升同仁之工作能力，資訊安全教育訓練計畫宜考量以人員角色及職能為基礎，針對不同層級的員工，進行相關的資訊安全教育訓練。

(2)資訊安全教育訓練內容宜含資訊作業相關之議題，如資訊安全管理制度實施規範、資訊安全法令規定、資訊作業程式、資通安全事件或案例、資訊安全技術與其他相關知識。

(3)資訊安全教育訓練宜考量設計學習評量機制，如隨堂測驗或討論等方式，以作為評估訓練效果之依據。

(4)資訊安全教育訓練計畫、學習評量結果及簽到紀錄等相關紀錄

宜予以保存，以便追蹤管理。

(5)資訊安全技術人員宜定期接受資訊安全管理知識、資訊安全技術能力或模擬駭客攻擊能力等資訊安全領域教育訓練。

(6)營運管理單位訓練宜包括安全認知訓練實際演練，以模擬真實的網路攻擊。

實際演練宜包括不通知的社交工程來嘗試收集資訊、獲得未授權的存取、模擬打開惡意電子郵件附件或外部連結的不利影響、透過魚叉式釣魚攻擊和惡意網站連結等。

(7)基於角色的安全訓練

營運管理單位宜基於人員指派的角色和權責、特定的安全需求，以及已獲授權存取資訊系統的人員，來決定安全訓練之內容。此外，營運管理單位宜提供營運管理單位、系統開發人員、系統維運人員、資料庫管理人員、系統管理人員、網路管理人員、機房管理人員與資安技術人員等，專門用於所指派任務之適當的安全相關的技術訓練。

基於角色的全方位訓練闡述管理、維運和技術角色和權責，涵蓋實體、人員和技術防護措施和對策。這種訓練可以包括：機關之安全角色所定義的政策、程式、工具和工件。營運管理單位還提供人員資訊安全計畫內維運和供應鏈安全相關之履行職責的必要訓練。

A.安全訓練/環境控制

B.營運管理單位宜定期提供人員或角色有關職場環境控制的基本訓練。

C.環境控制包括偵測滅火設備/系統、自動噴水滅火系統、手持

滅火器、固定消防水帶、煙霧探測器、溫度/濕度系統、空調系統和電力設施等。營運管理單位與環境控制相關特定的角色和權責人員(如：機房管理人員)，需施以必要的專業訓練。

5.營運持續管理

(1)營運持續計畫/與相關計畫協調

為降低 4G 應用服務系統遭遇突發緊急危難或異常事件所可能造成資訊作業之衝擊，並規劃相關應變策略與處理計畫，以確保關鍵性資訊作業持續運作。

A.營運管理單位宜與負責相關計畫的部門協調營運持續計畫的制定。

4G 應用服務系統與營運持續計畫相關的計畫宜包括維運連續性計畫、災害復原計畫、連續性的運作計畫、危機處理計畫、關鍵基礎設施計畫、網路事故回應計畫、內部威脅實作計畫和操作人員應急計畫等。

B.訂定演練模式及週期

營運管理單位宜依資訊資產業務重要性，擬定資訊系統備援演練時程表，決定該年度之測試範圍及標的，由營運管理單位依時程表就資訊作業持續營運管理計畫執行演練測試。資訊作業營運持續管理計畫之演練可擇以下一種或數種測試模式：

a.書面模擬演練(Desktop Exercise)(無法進行實況演練者)

b.資料回復演練(Data Recovery)

c.情境模擬演練(Scenario Simulation)

d.實況演練(Simulation)

e.預警/無預警演練

C.營運管理單位依據演練計畫，於執行測試演練前擬訂書面演練計畫及時程表。

演練計畫宜包含以下項目：演練目的與範圍、演練情境說明、演練時程規畫、演練順序及步驟、演練所需資源清單、參與單位及負責人員清單、協力廠商聯絡清單與模擬通報機制等。

(2)營運持續計畫/容量管理計畫

營運管理單位進行營運衝擊分析時，應判斷各項資訊資產與業務服務流程中斷時，產生對於各項業務服務流程所造成之影響及衝擊程度，據以判斷最大可容忍中斷時間(MTPD)、系統復原時間目標(RTO)以及資料復原點目標(RPO)等，並分別給予重要分級。

A.營運管理單位元應進行容量管理計畫，以便提供在營運持續行動期間存在的資訊處理、通信和環境支援的必要能力。

由於不同類型的威脅(如自然災害、針對性的網路攻擊等)可能導致可用的程式、通信和預劃支援機關任務/維運功能的服務減少，因此營運管理單位需在營運持續行動和容量計畫降低前，先行預估降級操作之可能性。

B.需求蒐集

營運管理單位亦宜考量下述相關之內外部需求與協議，做為擬定、維護容量管理計畫書之參考：

a.業務單位或使用單位對於服務效能之需求或期望

b.服務水準協議

c.支援服務水準協議之內部作業水準協議或外部合作廠商之契約資訊

d.預計實施之年度大型專案或重大服務變更

e.外部法令法規或企業內部相關之管理規範與要求

C.容量規劃與評估

a.容量現況與未來之容量需求預測(宜考量可用性與持續性需求對應之容量需求)

b.容量管理範圍與對應之容量監控項目、監控頻率與臨界值

c.評估預期下可能發生之服務升級、變更請求、新科技資訊，以及與容量相關之技術對容量管理規劃之影響

d.用以進行容量預測與分析之資料數據及執行方法說明，包含因容量因素導致之資訊服務事件、問題案件資訊

D.容量監控與分析

a.營運管理單位元宜定期提供容量管理之資源使用資訊，做為擬定、維護容量管理計畫書之參考。

b.營運管理單位宜依據所訂定之監控項目、臨界值，監督資源及服務之使用情形、記錄監控結果，並依據監控結果適

時將異常或潛在問題反應通報予營運管理單位。

E.容量調校與改善

a.依據容量監控、分析與預測結果，而須採取調校或購置作業時，營運管理單位宜依據已制定之相關要點進行。

b.依據容量管理計畫書之需求蒐集、規劃與評估、監控與分析結果，針對未能符合相關服務水準協議或容量管理目標之項目，提出並執行相關改善措施。

F.營運持續計畫/恢復基本任務/維運功能

營運管理單位宜辨識關鍵資訊作業流程，就營運衝擊分析之結果，並考量成本效益因素，進行因應方案之可行性分析，並研擬資訊作業營運持續計畫。

a.營運管理單位宜規劃在一定期間內啟動營運持續計畫，以恢復基本任務/維運功能。

營運管理單位可以選擇在此強化控制措施實行營運持續計畫活動，做為維運連續性計畫的一部分，例如依據營運衝擊分析的結果。恢復基本任務/維運功能的時間，將視資訊系統及其配套基礎設施中斷的嚴重程度和範圍而定。

G.營運持續計畫/維持基本任務/維運功能

營運管理單位宜規劃利用少許或未受損的系統，使基本任務和維運功能得以繼續運行，直到資訊系統的主要處理或儲存場所恢復正常運作為止。

營運管理單位可以選擇此項強化控制措施實行營運持續計畫活動，做為機關維運連續性計畫的一部分，例如依據維運衝擊分析的結果。營運持續計畫的所定義之主要處理或儲存場

所可能會改變，應取決於與營運持續相關的情況(如備用場所可能會成為主要場所)。

H.營運持續計畫/備份處理/儲存場所

備用儲存場所應與主儲存場所在不同的地理位置。除非主儲存場所失效，備用儲存場所宜維持資訊和資料的複製拷貝。備用儲存場所涵蓋的協議項目應包括：備用場所的環境條件、存取規則、實體與環境保護要求、交付和擷取備用媒體的程式等。備用儲存場所要能對應到營運持續計畫中的連續性要求，以確保一旦機關資訊系統中斷、被破壞或失效時，機關仍能維持執行基本任務和維運功能。

I.營運持續計畫/協調外部服務供應商

營運管理單位宜協調其營運持續計畫與外部服務供應商的營運持續計畫，以確保營運持續需求可以得到滿足。

當營運管理單位依賴外部的服務供應商維持其核心任務/維運功能的能力時，發展及時和全面的營運持續計畫將更具挑戰性。在這種情況下，營運管理單位應加強與外部機關協調其營運持續計畫相關活動，以確保個別的計畫對應機關的整體營運持續之需求

J.營運持續計畫/確認關鍵資產

營運管理單位應確認資訊系統關鍵資產以支援基本任務和維運功能。

機關可以選擇在這項強化控制措施實行營運持續計畫活動，做為營運管理單位維運連續性計畫的一部分，例如依據維運

衝擊分析的結果。營運管理單位應確認資訊系統的關鍵資產，並採行額外的防護措施及對策 (除定期實施的防護措施和對策之外)，以協助營運管理單位的任務/維運功能可以在應變期間持續進行。

此外，關鍵資訊資產的識別有利於機關資源的優先順序。關鍵資訊系統資產包括技術和運作兩方面。技術方面的問題，如資訊技術服務、資訊系統元件、資訊科技產品和機制等。運作方面包括程式(手動執行操作)和人事(人員操作技術防護措施和執行手動程式)等。機關程式保護計畫可以提供並協助識別關鍵資產。

K.營運持續計畫測試

測試營運持續計畫，以確定計畫的有效性，並識別計畫中潛在弱點的方法包括實地考察和沙盤推演、查檢表、模擬(平行、完全中斷)和綜合演練等。營運管理單位基於營運持續計畫連續性的需求進行測試，包括確定對機關運作、資產及人員因營運持續行動所產生的影響。營運管理單位執行本項控制措施應具，靈活性，並在廣度、深度和矯正行動的時效性上可自由裁量。

L.資訊系統備份

系統層級資訊，包括系統狀態資訊、作業系統、應用軟體及使用授權等。使用者層級資訊包括系統層級資訊之外的任何資訊。營運管理單位用來保護資訊系統備份完整性的機制包括數位簽章與密碼學的雜湊函數等。至於傳輸過程中的系統備份資訊之保護在，已超出了本項控制措施的範圍。資訊系統備份將反映出機關營運持續計畫中的需求，以及其他備份資訊要求。

M.資訊系統復原與重建

復原是指執行資訊系統營運持續計畫的活動，以恢復機關之任務/維運功能。重建是繼復原之後發生，包括返回充分運作狀態的活動。復原和重建行動反映任務和維運的優先順序、復原點/時間和重建目標，並建立了與營運持續計畫要求一致的機關準則。

重建包括停用任何可能在復原操作過程中需要的臨時資訊系統功能。重建還包括充分恢復的資訊系統功能、連續監視活動、潛在的資訊系統重新授權和預先防範未來系統中斷、被破壞或失效活動的評鑑。營運管理單位所採用的復原/重建功能包括自動化機制和手動程式。

N.備用通信協定

營運持續計畫和相關的訓練及測試，將備用通信協定能力做為增加機關資訊系統彈性的一部分。

O.安全模式

資訊系統支援的重要任務或營運功能，營運管理單位可以選擇在某些條件下，將這些系統回復到預先定義的安全模式下操作。

安全模式的操作，可以自動或手動啟動，當遇到這些條件時，可以執行限制活動的類型或資訊系統的操作。而所謂的限制包括：只允許某些功能，可以在有限的電力或減少通信頻寬下進行。

P.備用安全機制

此控制措施支援資訊系統營運持續計畫和維運連續性的彈

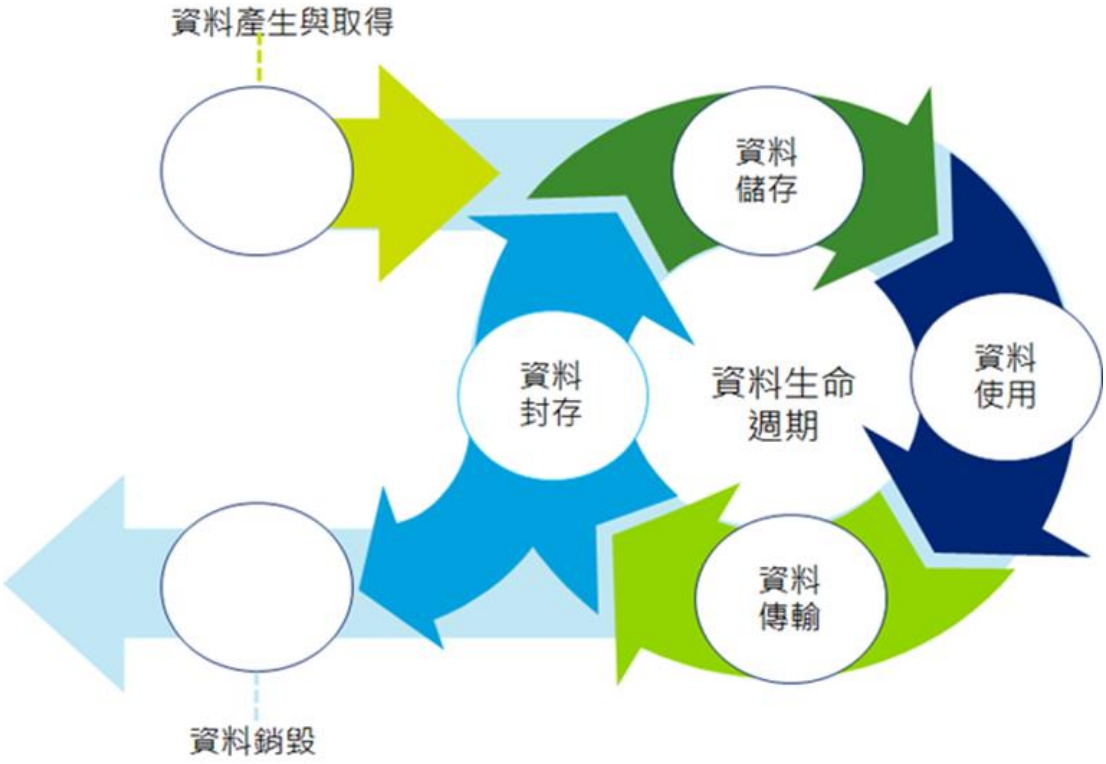
性。為確保任務/維運連續性，機關可以實作替代或補充的安全機制。這些機制可能不如主要機制有效(例如不容易使用、不可伸縮的、或不安全等)。

然而，有能力馬上使用這些替代/補充機制，可提升整體的任務/維運連續性，以免主要實作的方法恢復功能前，機關運作被削減，而造成衝擊。

考慮到成本和提供這種替代的能力所需的資源，此控制措施通常將只應用於由資訊系統、系統元件或資訊系統服務提供重要的安全功能。

(二)資料管理面

資料管理面將會從資料生命週期管理（Information Lifecycle Management）的角度，來探討 4G 應用服務系統從資料的產生與取得、資料儲存、資料使用、資料傳輸、資料封存到資料銷毀這整個過程中的資訊安全管理機制，資料生命週期如下圖所示。



資料來源：本計畫整理

圖4　資料生命週期(Information Lifecycle)

1.資料產生與取得

營運管理單位應依據個人資料保護法等相關規定，審慎蒐集、處理及利用個人資料，並建立個人資料安全控制及管理機制。

應用服務系統於蒐集個人資料前，應取得使用者同意，並進行個資告知聲明。

依據個資法第八條之要求，向當事人蒐集其個資時，應明確進行個資告知聲明，其告知內容應包含：

(1)蒐集個資之機關名稱

(2)蒐集目的

(3)蒐集之個資類別

(4)個資利用期間、地區、範圍

(5)當事人可行使之權利

(6)當事人保有自由選擇提供個人資料之權利，如不提供，將對其權益之影響

另外，若符合以下狀況者，得免告知，可直接向當事人進行個人資料之蒐集：

(1)依法律規定得免告知。

(2)個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

(3)告知將妨害公務機關執行法定職務。

(4)告知將妨害公共利益。

(5)當事人明知應告知之內容。

(6)個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

2.資料儲存

(1)對於存放個人資料或機敏性檔案的系統，應建立資料外洩防護與網站管理機制。

對於個人資料或機敏性檔案，於資料儲存前應執行一定強度之加密機制後，如：MD5、SHA-1 或其他安全等級更高之雜湊演算法，方可儲存。

(2)對於存放個人資料或機敏性檔案的系統應定期進行資料稽核，使用紀錄、軌跡資料及證據之保存都必須被完整保留。

宜定期檢視存放個人資料或機敏行檔案的系統日誌，避免有不必要或是異常的操作行為。除此之外，系統應該完整留存所有稽核日誌紀錄，以便日後營運管理單位發生個資侵害事件或其他與個人資料或機敏性檔案相關的事件時，能夠及時勾稽並進行後續追蹤，甚至能夠直接做為數位鑑識的佐證依據。

3.資料使用

(1)對個人資料或機敏性資料應在使用過程中以加密方法保護，並

決定採取適當等級的安全保護措施。

個人資料或機敏性資料在使用過程中應以 MD5、SHA-1 或其他安全等級更高之雜湊演算法進行保護，以確保資料使用過程中資料之正確性，並確保資料不會遭到有心人士惡意竄改。

(2)營運管理單位應遵守資料保密規範，對於測試用之個人資料或機敏性資料，應先進行資料遮蔽處理或管制保護。

營運管理單位應小心選擇、保護及管制測試資料，若非得用真實資料進行測試，於測試前必須依照個人資料及機敏性檔案管理相關規範，進行資料遮蔽或去識別化，以確保個人資料及機敏性檔案受到適當的保護。

(3)在使用真實的個人資料或機敏性資料進行測試時，應採行下列保護措施：

A.適用在實際作業系統的存取控制措施，亦應適用在測試用的系統。

B.真實資料被複製到測試系統時，應依複製作業的性質及內容，在取得授權後始能進行。

C.測試完畢後，真實資料應立即從測試系統中刪除。

D.真實資料的複製情形應予以記錄，以備日後稽核之用。

4.資料傳輸

(1)單位間進行資料或軟體交換，應訂定正式的協定，將機敏性資料的安全保護事項及有關人員的責任列入。

各單位間進行資料交換或傳輸時，除應訂定正式協議明確定義雙方應遵守之事項外，雙方尚須簽屬保密協議，保護資料傳輸雙方之權利與義務。

(2)透過 FTP 線上傳輸方式應使用加密機制或專線等機制。

(3)透過電子郵件傳輸個資或機敏性資料，應對檔案本身施予加密或編碼等保護機制，如：開啟壓縮軟體密碼保護之功能。

5.資料封存

(1)應準備適當及足夠的備援設施，定期執行必要的資料及軟體備份和備援測試演練作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

(2)資料備份作業原則如下：

A.正確及完整的備份資料

應用服務系統於進行資料備份時，應將儲存於備份媒體中之資料予以適當保護，如：加密，以避免個人資料外洩的狀況發生。另外，對於存放備份資料之儲存媒體，除存放在主要的作業場所外，應實施異地備援機制，將備份資料存放在其他場所分散風險，以防止主要作業場所發生災害時造成的傷害，同時確保備份資料之正確性與完整性。

B.備份資料應有適當的實體及環境保護，其安全標準應盡可能與主要作業場所的安全標準相同。

保存備份資料的場所其實體環境控管措施皆應比照主要作業場所規格，如：門禁控管方式、CCTV 監控系統、環控系統溫溼度告警值、消防設備規格等等。

C.應定期測試備份資料，以確保備份資料之可用性。

營運管理單位應擬定應用服務系統之備份政策，並依照備份政策所訂定之備份排程定期進行系統備份，事後定期測試備份資料之內容，以確保其可用性，避免應用系統實際發生不

可預期之意外時，無法回復當前資料的狀況。

6.資料銷毀

(1)完成銷毀與刪除作業後，個資或機敏性資料檔案應不復存在。

(2)不可再復原及留存備份個資或機敏性資料檔案。

(3)進行個資或機敏性資料銷毀與刪除作業時，應確保該資料檔案上之資訊無法再利用。

進行記載有個人資料或機敏性檔案之紙本資料或數位媒體銷毀或刪除作業時，應採用物理性實體破壞方式，如以碎紙機絞碎或撕毀，或送至焚化爐焚化，或送至紙廠回收溶解，或擊碎、消磁或低階格式化等無法回復之安全方式處理，避免銷毀或刪除後遭有心人士復原資料檔案。

(4)以委外方式辦理個資或機敏性資料檔案銷毀與刪除作業時，應謹慎選擇有適切控制措施及經驗之協力廠商委外廠商。

在選擇協力廠商委外廠商時，應依照營運管理單位現有之供應商評選流程進行選商，並以檔化方式告知協力廠商委外廠商其所應履行之資訊安全保護責任，其內容應包含：涉及存取、處理、儲存、通信或提供資訊處理基礎設施與元件的協議，並要求執行個資或機敏性資料檔案銷毀與刪除作業之協力廠商委外廠商簽署保密協議，確保其在執行檔案銷毀或刪除的過程中所觸及到的資料檔案室絕對保密的。

(5)以委外方式辦理個資或機敏性資料檔案銷毀或刪除作業時，應要求協力廠商委外廠商提供個資或機敏性資料檔案已實際被銷毀或刪除之證明。

以委外方式辦理個人資料或機敏性檔案銷毀或刪除作業時，應

要求協力廠商委外廠商執行銷毀或身除作業後，檢附個資或機敏性資料檔案已實際被銷毀或刪除之證明文件或檔案，如：執行前的資料或檔案照片，以及執行銷毀中的資料檔案照片，或者資料銷毀或刪除執行的影片，除留存紀錄證明資料已按照標準流程進行銷毀或刪除以供備查外，同時也能監督協力廠商委外廠商是否有依照合約內容履行其所應交付的服務。

(三)系統管理面

1.系統安全開發管理

(1)規劃安全系統發展生命週期

A.定義完善的系統發展生命週期提供系統成功開發、實施和運作的基礎。在系統發展生命週期內應用所需的安全控制措施，需對資訊安全、威脅、弱點、不利衝擊和關鍵任務/維運功能之風險有基本的瞭解。如負責設計、編碼和測試資訊系統和系統元件(包括資訊科技產品)之人員不瞭解資訊安全，則安全工程原則將無法被正確應用。

B.應在系統發展生命週期活動時納入合格人員，以確保營運管理單位的資訊系統包含安全需求。同樣重要的是系統開發人員，應具備必要的安全專業知識和技能，以確保所需的安全功能有效地被整合到資訊系統當中。

C.安全認知和訓練計畫可以協助確保具關鍵安全角色和責任的人員，具備適當的經驗、技能和專業知識以進行指派的系統發展生命週期活動。

(2)需求分析階段

A.4G 應用服務系統(新發展的資訊系統，或是現有系統功能之強化)應在資訊系統規劃之需求分析階段，即明定資訊安全需

求，並將安全需求納入系統功能。

B.系統之新增及修改，應視部門之技術人力、開發時程、預算與需求，評估以自行開發或選購外部廠商所開發之系統。

C.自行開發之應用程式，其系統開發及修改應確保資訊安全已被設計並落實至系統開發生命週期內。

D.在分析與描述安全的軟體需求時，系統開發人員應掌握SMART+原則具體描述：

a.Specific：明確的，不模糊的。需求必須提供詳細的說明，同時包含一致的專業用語。

b.Measurable：可量化、可量測的。需求必須可以被分析與測試。

c.Appropriate：適當、符合所需的。需求必須被驗證以確保符合真正需要。

d.Reasonable：有依據、具合理性。需求執行前最好參照類似專案。

e.Traceable ：可追蹤 ：可追蹤 、有建檔 及有紀錄可循。需求必須融入開發生命週期以容易追蹤或驗証。

(3)應用程式開發階段

A.Web 應用系統管理機制宜參考行政院國家資通安全會報技術服務中心之「Web 應用程式安全參考指引與實作手冊」、「安全軟體設計參考指引」、「安全軟體測試參考指引」與「安全軟體發展流程指引」等規範進行管理。

B.行動應用 App 管理機制宜參考經濟部工業局之「行動應用 App 安全開發指引」、「行動應用 App 基本資安規範」與「行動應

用 App 基本資安檢測基準」等規範進行管理。

(4)安全測試及評估

A.系統測試與開發環境，應與正式應用系統實體區隔。

B.安全測試及評估/靜態代碼分析

組織應要求資訊系統、系統元件或資訊系統服務的系統開發人員，採用靜態代碼分析工具來識別常見的漏洞並檔化分析結果。

靜態代碼分析提供了安全審查之技術和方法。這種分析可用於識別安全弱點及執行安全編碼工作。在發展過程早期時使用靜態代碼分析，每個代碼的變更可以自動掃描潛在的弱點是最有效的。靜態分析可以隨著漏洞提供明確的修復指引，使系統開發人員能夠修復這些漏洞。

正確實作靜態分析的證據可以包括對關鍵漏洞類型聚合漏洞密度，由系統開發人員或安全專業人員檢視漏洞的證據並證明漏洞已修復。忽略過高密度的結果(通常稱為忽略或誤報)顯示分析過程或工具潛在的問題，在此情況下，機關應權衡來自其他來源的證據之有效性。

C.安全測試及評估/威脅和弱點分析

組織應要求資訊系統、系統元件或資訊系統服務的系統開發人員，執行威脅和弱點分析及後續已建系統、元件或服務之測試/評估。

應用程式可能會與系統發展生命週期的需求及設計階段產生之功能及設計規格大幅偏離。因此，交付前的資訊系統、系統元件和資訊系統服務之威脅和弱點分析對這些系統、元件

和服務的有效運作至為關鍵。威脅和弱點分析在生命週期的這個階段可協助確保設計或實作的變更已被納入考量，任何因為這些變化而產生新的弱點都已進行審查並減緩。

D.安全測試及評估/人工代碼審查

組織應要求資訊系統、系統元件或資訊系統服務的系統開發人員，依據定義之流程、程式、技術及特定代碼來執行人工代碼審查。

人工代碼審查通常是保留給資訊系統的關鍵軟體和韌體元件。這種代碼審查需要瞭解應用程式的需求或背景知識，對識別弱點是唯一有效，更自動化的分析工具和技術，如靜態或動態的分析通常不可用。受益於人工審查的元件，例如驗證存取控制矩陣對應用控制和審查詳細的加密實作和控制方面。

E.開發人員安全測試及評估/滲透測試/分析

組織應要求資訊系統、系統元件或資訊系統服務的系統開發人員，在定義之廣度/深度及限制因素下執行滲透測試。

滲透測試是一種評估方法，評估人員使用所有可用的資訊科技產品或資訊系統檔(如：產品/系統設計規格、原始碼和管理員/操作員手冊等)並在特定限制下工作，試圖規避資訊科技產品和資訊系統實作之安全功能。

滲透測試可包括由技術熟練的資安技術人員模擬敵人的行動執行之白、灰、黑箱測試及分析等。滲透測試的目的是發現在資訊科技產品及資訊系統的潛在弱點，造成執行錯誤、組態故障或其他運作部署的弱點或漏洞。滲透測試可以和自動及手動代碼審查結合，以提供可能會比平常更高等級的分析。

F.安全測試及評估/攻擊面審查

營運管理單位應要求資訊系統、系統元件或資訊系統服務的系統開發人員來執行攻擊面審查。

資訊系統的攻擊面是易受攻擊的區域，使這些系統更容易受到網路攻擊，例如在資訊系統(包括硬體、軟體和韌體元件)中任何可存取區域的弱點或漏洞，均提供敵人利用弱點的機會。

G.安全測試及評估/驗證測試/評估範圍

營運管理單位應要求資訊系統、系統元件或資訊系統服務的系統開發人員，依機關定義之深度的測試/評估，提供完全涵蓋所需之安全控制措施來驗證安全測試/評估的範圍。

提供完全涵蓋所需之安全控制措施來驗證安全測試/評估的範圍可以透過從非正式到正式的各種分析技術來完成。每種技術均提供日益增加的程度來保證對應正式分析的程度。嚴格證明安全控制措施涵蓋在保證的最高級別可以使用正式的模式和分析技術，包括控制措施實作和對應之測試案例間的關聯性。

H.系統開發人員安全測試及評估/動態代碼分析

營運管理單位應要求資訊系統、系統元件或資訊系統服務的系統開發人員，採用動態代碼分析工具來識別常見的漏洞及檔化分析之結果。

動態代碼分析提供軟體程式運行時的驗證，使用能夠監控程式之記憶體損壞、使用者特權議題，和其他潛在安全問題之工具。動態代碼分析採用運行時之工具，以協助確保在其設計的方式執行安全功能。一種特殊類型的動態分析，稱為模

糊測試，透過故意導入畸形的或隨機的資料至軟體程式導致程式失效。

模糊測試策略源於應用程式之預期使用和功能及應用程式之設計規格。要瞭解動態代碼分析之範圍，進而提供保證，機關應考慮進行代碼涵蓋分析(使用度量標準檢查已測試之代碼的程度，如已測試副程式之百分比或執行測試套件時程式敘述被呼叫之百分比)或一致性分析(檢查不適合之軟體代碼，如非英文單詞或貶詞)。

I.伺服端安全檢測

行動應用程式所搭配之行動應用平臺伺服端，由於其提供之存取介面為行動應用程式，而非使用者直接存取之介面，系統開發人員易忽略伺服端安全的防護措施。行動應用平臺伺服端本質為網站及 Web Service 伺服器，若無適當的安全設計與開發，同樣會存在傳統網頁應用程式所具有的弱點。因此，在伺服端的安全檢測，系統開發人員可斟酌採用滲透測試方式進行檢測。目前於國際間具公信力及參考價值的滲透測試文件有:

a.OWASP (Open Web Application Security Project)的 OWASP 測試指引(OWASP Testing Guide)

b.ISECOM (the Institute for Security and Open Methodologies)的開放源始碼安全測試方法手冊(Open Source Security Testing Methodology Manual, 55 OSSTMM)

c.SANS (System Administration, Networking, and Security Institute)的滲透測試相關文件

由於安全威脅種類繁多，故應優先針對風險性較高的進行檢

測才能提高效率，且許多關於網路安全的研究報告(包括 Gartner、Forrester 及 IDC)指出 Web 應用程式已成為主流網路攻擊目標，主要威脅之增加歸咎於 Web 應 用程式的弱點，因此針對網頁應用程式的弱點檢測特別重要，下面列出三個網站或組織對於網頁應用程式弱點的最新消息發布及更新，可作為檢測項目的參考：

a.OWASP Top 10

此 OWASP 組織所執行的一項計畫，每年會發布該年對於網頁應用程式最具威脅性或最常見的十大弱點，OWASP Top 10: 2017 年所提出的清單詳見下表。

表3　OWASP Top 10: 2017

編號	威脅項目	說明
1	**注入**	注入攻擊漏洞，例如：SQL、OS 以及 LDAP 注入。這些攻擊發生在當不可信的數據作為命令或者查詢語句的一部分，被髮送給解釋器的時候。攻擊者發送的惡意數據可以欺騙解釋器，以執行計劃外的命令或者在未被恰當授權時訪問數據。
2	**失效的身份認證和會話管理**	與身份認證和會話管理相關的應用程式功能往往得不到正確的實現，這就導致了攻擊者破壞密碼、密匙、會話權杖或攻擊其他的漏洞去冒充其他用戶的身份（臨時性的或永久性的）。
3	**跨站腳本（XSS）**	當應用程式收到含有不可信的數據，在沒有進行適當的驗證和轉義的情況下，就將它發送給一個網頁瀏覽器，這就會產生跨站腳本攻擊（簡稱 XSS）。XSS 允許攻擊者在受害者的瀏覽器上執行腳本，從而劫持用戶會話、危害網

編號	威脅項目	說明
		站、或者將用戶轉向至惡意網站。
4	**失效的訪問控制**	對已通過身份驗證用戶的運行限制，沒有得到恰當的強制執行。攻擊者可以利用這些缺陷訪問未經授權的功能和/或數據, 例如：訪問其他用戶的帳戶、查看敏感文件、修改其他用戶的數據、更改訪問權限等。
5	**安全配置錯誤**	好的安全需要對應用程式、框架、應用程式服務器、web服務器、數據庫服務器和平臺定義和執行安全配置。由於許多設置的默認值並不是安全的，因此，必須定義、實施和維護這些設置。這包含了對所有的軟件保持及時地更新，包括所有應用程式的庫檔。
6	**敏感資訊洩漏**	許多 Web 應用程式沒有正確保護敏感數據，如信用卡，稅務 ID 和身份驗證憑據。攻擊者可能會竊取或篡改這些弱保護的數據以進行信用卡詐騙、身份竊取，或其他犯罪。敏感數據值需額外的保護，比如在存放或在傳輸過程中的加密，以及在與瀏覽器交換時進行特殊的預防措施。
7	**攻擊檢測與防護不足**	大多數應用程式和 API 都缺乏檢測、防止和響應手動和自動攻擊的基本能力。攻擊防護遠遠超出了基本的輸入驗證，並涉及到自動檢測、記錄、響應，甚至阻止漏洞的利用企圖。應用程式所有者還需能夠快速部署修補程式以防止攻擊。
8	**跨站請求偽造（CSRF）**	一個跨站請求偽造攻擊迫使用戶已登錄的瀏覽器將偽造的 HTTP 請求(包括該用戶的會話 cookie 和其他認證資訊）發送到一個存在漏洞的 web 應用程式。這就允許了攻擊者迫使用戶瀏覽器向存在漏洞的應用程式發送請求，而這些請求會被應用程式認為是用戶的合法請求。

編號	威脅項目	說明
9	**使用含有已知漏洞的組件**	組件，比如：庫檔、框架和其它軟件模塊，幾乎總是以全部的權限運行。如果一個帶有漏洞的組件被利用，這種攻擊可以造成更為嚴重的數據丟失或服務器接管。應用程式使用帶有已知漏洞的組件會破壞應用程式防禦系統，並使一系列可能的攻擊和影響成為可能。
10	**未受到充分保護的 API**	現代應用程式通常涉及富客戶端的應用程式和 API，如：在瀏覽器和移動應用程式中的 JavaScript，它們連接到某種 API（如：SOAP/XML、REST/JSON、RPC、GWT 等）。這些 API 通常是沒有保護的，並且包含大量漏洞。

資料來源：本計畫整理

b.WASC 威脅分類

WASC (Web Application Security Consortium)是由許多資訊安全專家及組織所組成的非營利聯盟，該聯盟持續發布與 Web 應用程式的安全性相關之技術資訊、安全指引，以及其他有用的檔以供企業、教育機構、政府部門及應用程式開發人員等使用。其提出 WASC Threat Classification v2.0，將網站的安全威脅進行分類(以字典順序排序)，詳見下表。

表4 WASC Threat Classification v2.0: Attack list

編號	攻擊
1	功能濫用(Abuse of Functionality)
2	窮舉法攻擊(Brute Force)
3	緩衝區溢位(Buffer Overflow)

編號	攻擊
4	內容偽冒(Content Spoofing)
5	認證與會話辨識碼的預測(Credential/Session Prediction)
6	跨站腳本攻擊(Cross-Site Scripting, XSS)
7	跨站冒名請求(Cross-Site Request Forgery, CSRF)
8	阻絕服務(Denial of Service)
9	指紋探索與辨識(Fingerprinting)
10	格式化字串攻擊(Format String)
11	HTTP 回應偷渡(HTTP Response Smuggling)
12	HTTP 回應分割攻擊(HTTP Response Splitting)
13	HTTP 請求偷渡(HTTP Request Smuggling)
14	HTTP 請求分割攻擊(HTTP Request Splitting)
15	整數溢位(Integer Overflows)
16	LDAP 注入(LDAP Injection)
17	郵件命令注入(Mail Command Injection)
18	空字元注入(Null Byte Injection)
19	未經授權執行作業系統命令(OS Commanding)
20	路徑尋訪(Path Traversal)
21	可預測的資源位置(Predictable Resource Location)

編號	攻擊
22	遠端檔案含入(Remote File Inclusion, RFI)
23	路由迂迴攻擊(Routing Detour)
24	會話固定攻擊(Session Fixation)
25	SOAP 陣列濫用(SOAP Array Abuse)
26	SSI 注入(Server-Side Include Injection)
27	SQL 注入(SQL Injection)
28	URL 重定導向濫用(URL Redirector Abuse)
29	XPath 注入(XPath Injection)
30	XML 屬性爆毀(XML Attribute Blowup)
31	XML 外部實體(XML External Entities)
32	XML 實體擴張(XML Entity Expansion)
33	XML 注入 (XMLInjection)
34	XQuery 注入(XQuery Injection)

資料來源：本計畫整理

c.WASC Threat Classification v2.0

亦將常見的弱點進行以下分類(以字典順 序)，詳見下表。

表5　WASC Threat Classification v2.0: Weaknesses list

編號	攻擊
1	應用程式設定不正確(Application Misconfiguration)
2	目錄索引(Directory Indexing)
3	不當的檔案系統使用權限(Improper Filesystem Permissions)
4	不當的輸入處理(Improper Output Handling)
5	資訊外洩(Information Leakage)
6	不安全的索引(Insecure Indexing)
7	應用程式不足以因應自動化攻擊(Insufficient Anti-automation)
8	驗證機制安全性不足(Insufficient Authentication)
9	授權機制安全性不足(Insufficient Authorization)
10	密碼還原機制安全性不足(Insufficient Password Recovery)
11	應用程式流程驗證與控制不足(Insufficient Process Validation)
12	Session 過期機制安全性不足(Insufficient Session Expiration)
13	傳輸層保護機制安全性不足(Insufficient Transport Layer Protection)
14	伺服器設定不當(Server Misconfiguration)

資料來源：本計畫整理

d.CWE / SANS Top 25

CWE (Common Weakness Enumeration)是由 US-CERT 所

資助的 MITRE 組織所發布有關網頁應用程式安全弱點的類別。SANS (SysAdmin, Audit, Networking, and Security)則是個專門進行資訊安全培訓、認證與研究的機構，該機構對於資安領域有著深入地研究及分析，網站上提供最新資訊安

全相關研究。CWE / SANS Top 25 就是由 MITRE 和 SANS 合作，共同發布網頁應用程式前 25 大的威脅，詳見下表。

表6　CWE / SANS Top 25

等級	威脅
1	SQL 注入(SQL Injection)
2	作業系統命令注入(OS Command Injection)
3	緩衝區溢位(Buffer Overflow)
4	跨站腳本攻擊(Cross-site Scripting, XSS)
5	重要功能缺乏驗證(Missing Authentication for Critical Function)
6	缺乏授權機制(Missing Authorization)
7	將驗證的機密性資料直接寫入(Use of Hard-coded Credentials)
8	敏感性資料缺乏加密機制(Missing Encryption of Sensitive Data)
9	沒有限制危險類型的檔案上傳(Unrestricted Upload of File with Dangerous Type)

等級	威脅
10	安全決策依靠不可信任的輸入(Reliance on Untrusted Inputs in a Security Decision)
11	非必要的執行權限(Execution with Unnecessary Privileges)
12	跨站冒名請求(Cross-Site Request Forgery, CSRF)
13	路徑尋訪(Path Traversal)
14	下載源碼時未做完整性檢查(Download of Code Without Integrity Check)
15	不正確的授權(Incorrect Authorization)
16	包含了非信任及非控制範圍的功能(Inclusion of Functionality from Untrusted Control Sphere)
17	對重要資源不正確的權限指派(Incorrect Permission Assignment for Critical Resource)
18	使用有潛在危險性的函式(Use of Potentially Dangerous Function)
19	使用具瑕疵或具風險的加密演算法(Use of a Broken or Risky Cryptographic Algorithm)
20	緩衝區大小計算不正確(Incorrect Calculation of Buffer Size)
21	沒有適當的限制不斷的驗證企圖(Improper Restriction of Excessive Authentication Attempts)
22	URL 重新導向至非信賴的網站(URL Redirection to Untrusted Site ('Open Redirect'))

等級	威脅
23	未控制的字串格式(Uncontrolled Format String)
24	整數溢位或越界繞回(Integer Overflow or Wraparound)
25	雜湊加密時未加上 salt 搗亂(Use of a One-Way Hash without a Salt)

資料來源：本計畫整理

(5)部屬與維運

當 Web 應用程式上線進行運作時，仍應注意其安全性，以下將就源碼安全、定期稽核及即時監控，進行說明。

A.在稽核方面，一方面應善用 Syslog 等記錄機制與 Tripwire 等系統面的異動比較，另一方面，對於 Web 應用程式應定期以自動化檢測工具或專家服務來評估比較現況與前次檢測是否存在具體差異，主要注意項目包括：

a.程式異動，例如：源碼行數異動、函式增減及過濾條件變化等。

b.檔案異動，例如：檔案列表不一致、最後更新日期變更及檔案大小異動等。

c.安全修補，例如：新的弱點、再發生的弱點及已修補的弱點等。

d.入侵事件，例如：頁面異動、網站掛馬及不合法的請求(request)等。

以確保上線之系統無論在驗收之初或日後更版均至少維持規格檔之資訊案全要求。

B.即時監控

預防勝於治療，擁有監控性質的安全控制措施，能確保營運管理單位即時因應資安事件，將影響層面及早控制住。目前常見的解決方案可分為端點式監控(從單位內部監控單位的網站)，例如：安裝網頁防竄改系統與遠端監控(從單位外部監控單位的網站)，例如：購買網頁掛馬監控服務。前者可能需要建置硬體或安裝軟體，後者則需要訂閱遠端服務。

C.源碼安全

在系統開發階段除了考量程式撰寫的安全性，同時也要兼顧程式碼本身存取的安全性與完整性，例如：透過版本控制與權限控管等。此外，要避免程式碼被外部使用者或非系統開發人員取得。

2.作業系統管理

(1)系統管理人員宜參考「政府組態基準(GCB)」，規範資通訊終端設備(如：個人電腦) 與伺服器的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道。

(2)「政府組態基準(GCB)」針對帳號與密碼原則管理、螢幕保護程式、稽核軌跡留存等控管措施應有效落實於 4G 應用服務系統。

3.資料庫管理系統管理

(1)資料庫帳號及存取權限管理

A.資料庫管理人員宜定期辦理資料庫帳號清查，相關確認檔宜留存備查。

B.資料庫管理人員擁有資料庫系統之最高權限，並依據工作職掌設定具有資料庫系統存取權限之使用者。

C.除資料庫管理人員外，其他的使用者帳號（ID）不可分配到資料庫管理人員群組。

D.為符合職能分工之要求，資料庫管理人員、營運管理單位、系統管理人員與系統開發人員之權限應適當區隔。

E.資料庫系統帳號及群組之新增或刪除，應循組織定義之正式程式提出申請，並經權責主管授權核准後方可新增或刪除，異動時亦同。

F.若有資料庫存取權限異動需求,應由應用系統開發人員於表單管理系統敘明欲變更之權限暨其相關緣由後提出申請。

(2)資料庫實體檔案目錄管理

確保資料庫實體檔案目錄下所有程式權限適當設定為僅有資料

庫管理人員群組擁有。

(3)資料管理

資料管理包含資料庫(DB)、資料表(Table)、預存程式(Stored Procedure)、檢視表(View)及資料庫檔案之資料(Data)等。

資料擁有者對資料庫有異動及查詢需求時，應循組織定義之正式程式提出申請且經權責主管核准後，由資料庫管理人員進行變更作業。

4.委外廠商管理

A.訂定組織委外服務資安策略

營運管理單位應依據以下要點規畫委外服務資安策略：

a.考量資訊廠商專業領域之差異，組織應視委外個案性質決定，將資訊安全需求所需費用列入成本分析計價項目。例如：Web 應用程式開發案，鑑於網路攻擊無所不在，問題層出不窮，為避免日後因系統漏洞產生資安攻擊事件或個資外洩等問題，建議將資安檢測另列預算，並將資訊安全服務成本納入考量。

b.營運管理單位應於遴選廠商過程中，將資訊安全需求納入評選計分，藉以提高廠商的重視，除一般功能的滿足外，遴選出能提供最佳資安解決方案之廠商，以保障組織之資訊安全。

c.營運管理單位應將安全規範對廠商要求納入契約書，以便日後「履約管理」階段，要求承商遵循契約書訂定之標準或規範執行，並提供可行建議方案，以確保委外作業安全。

B.為降低委外廠商存取或處理組織資訊的風險，應與委外廠商

協議並檔化資訊安全控管的要求。

C.提供委外廠商資訊時，除公開資訊外應由委外廠商管理人員提出申請，經權責主管審核同意，機敏資訊需採用加密或其它確認資料安全之保護機制後始得提供。

D.委外廠商需存取組織資訊資產時，組織應考量以下各項因素：

a.存取目的及用途

應符合法令規定或主管機關之規定。

該資訊資產之存取應視其必要性，例如：軟、硬體廠商維護之需求或合約之要求。

b.存取方式

實體存取，如外部人員須進入安全區域、取得實體檔或媒體等需要。

邏輯存取，如透過網路或資訊系統之方式存取。

資訊或媒體之交換，應考慮以下因素：

網路傳輸使用之通訊協定、介面、格式。

資料、檔傳遞之安全，如加密方式、依檔等級採取適當之傳遞方式。

遺失或損毀之風險。

協調制定交換程式或作業手冊。

資訊所有權及保護責任之劃分。

E.應定期監視、審查與稽核委外廠商交付的服務。

F.委外廠商所提供服務的變更，包括維持與改進現有的資訊安全

政策、程式及控制措施均應加以管理，並考量所涉及之營運資訊、系統與過程的重要性以及風險的重新評鑑。

G.委外廠商如為長期服務提供性質者，如軟硬體維護合約、系統委外管理等，外部單位應依合約或工作說明書要求，定期提交服務水準報告，交由委外廠商管理人員審核備查。

H.委外廠商管理人員認為有進行監控或查核之必要時，得會同稽核單位對外部單位進行查核。

5.雲端環境安全管理

(1)根據美國國家標準技術研究所 NIST 的定義，雲端運算是一個支援方便性與即時性的網路存取模式，使用者可自行調控所需的運算資源；另一方面，4G 應用服務系統營運管理單位能有效地管理整個可共用與可調整的運算資源，以達到降低管理成本、彈性提升計算處理能力及易於量測服務等目的，以下說明雲端服務的基本特徵、服務及部署模式，詳見下圖所示。

資料來源：本計畫整理

圖5　雲端服務的基本特徵、服務及部署模式

(2)雲端服務的 5 個基本特徵

A.隨需隨用(On-demand self-service)：使用者可以單方面的使用其計算能力，並能自動的得到所需要的資料，不需要隨時與服務供應商互動。

B.廣泛的網路連接(Broad network access)：使用者可以使用各種平臺來連接網路，如智慧型手機、筆記型電腦、桌上型電腦、穿戴式裝置及平板電腦或物聯網智慧裝置等。

C.資源共用(Resource pooling)：所提供的運算資源可依使用者的需求自動動態分配，使用者無須也無法控制服務資源來源。

D.快速彈性(Rapid elasticity)：所提供的服務是快速且有彈性的，對於使用者而言，可配置的功能似乎是無限的。

E.測量服務(Measured Service)：雲端運算提供服務時，會計量、監控資源的使用，以達到雲端系統自動控制與優化的目的。

(3)雲端運算的 3 個服務模式

A.軟體即服務(Cloud Software as a Service, SaaS)

透過網際網路提供軟體的一種服務模式，廠商將應用軟體統一部署在雲端伺服器上，客戶可透過瀏覽器使用廠商提供的應用軟體服務，使用者不用再購買軟體，且無須對軟體進行更新維護，服務提供商會全權管理和維護軟體，如 Google DOCS、Microsoft Office Live、Facebook 及 Saleforce 等。

B.平臺即服務(Platform as a Service, PaaS)

廠商透過網際網路將雲端服務平臺，例如：儲存設備、資料庫等開放給使用者，使用者可以自行部署應用程式，自行使用編程語言使用服務平臺，但無須管理或控制雲端設備，包

含網路設備、伺服器，如 Google App Engine、Windows Azure 及 AMAZON AWS：S3(Simple Storage Service)等。

C.基礎設施即服務(Infrastructure as a Service, IaaS)

廠商透過網際網路，以虛擬主機方式提供完整的作業系統、資料庫存取，如 Flexiscale、AWS(Amazon Web Services)等。

(4)雲端服務使用者應事先評估雲端服務提供者之服務水準(含資訊安全防護)等，若有不符合需求之處，應考量其他補償性措施，前述服務水準(含資訊安全防護)要求基準，可參考下表。

表7　雲端服務提供者要求基準

	IaaS	SaaS	PaaS
可用性管理	以服務水準協定方式，要求廠商確保虛擬主機平臺，包含以下之伺服器、儲存及網路等軟硬體設施之可用性，並檢視廠商營運持續、資料復原計畫及執行情形。其中營運持續之異地備援距離本地至少 35 公里(含)以上，且當一台實體伺服器故障可於 10 分鐘內將其上 VM(VirtualMachine)移轉至其它實體主機中重新開啟。	1.達成 IaaS 可用性管理。 2.確保雲端應用系統平臺，如資料庫、儲存空間等可用性。	1.達成 PaaS 可用性管理。 2.確保雲端軟體服務之可用性。
存取控制	依資安規範要求廠商建立虛擬主機平臺暨所屬軟硬體設施存取控制機制，包括帳號安全認證、權限管理、網路安全傳輸及遠端存取控管，並能驗證其有效性。	除將帳號安全認證管理提升至雲端應用系統平臺層次外，並達成 IaaS 其餘存取控制措施。	除將帳號安全認證管理提升至雲端軟體服務層次外，並達成 PaaS 其餘存取控制措施。

	IaaS	SaaS	PaaS
弱點管理	要求廠商確保虛擬主機平臺暨相關軟硬體弱點皆能有效管理與更新。	1.達成 IaaS 弱點管理。 2.確保雲端應用系統平臺弱點皆能有效管理更新。	1.達成 PaaS 弱點管理。 2.確保雲端軟體服務弱點有效管理更新。
變更管理	要求廠商對於虛擬主機平臺暨相關軟硬體皆有變更標準、規範與程式。	1.達成 IaaS 變更管理。 2.確保雲端應用系統平臺落實變更管理。	1.達成 IaaS 變更管理。 2.確保雲端服務平臺落實變更管理。
設定管理	依資安規範要求廠商對於虛擬主機平臺暨所屬軟硬體進行適當配置與設定，以強化其安全性，並檢視廠商定期測試評估情形。	1.達成 IaaS 設定安全管理。 2.確保雲端應用系統平臺設定安全管理。	1.達成 PaaS 設定安全管理。 2.確保雲端軟體服務設定安全管理。
意外應變	對於虛擬主機平臺暨所屬軟硬體應有事件應變處理機制，包括管理政策、規範、程式及 處理窗口，並檢視廠商定期演練情形，確認有效性。	同 IaaS，並包括雲端應用系統平臺部分。	同 PaaS，並包括雲端軟體服務部分。
監測	廠商對於虛擬主機平臺之設定、使用情形、控制措施及重大改變事件，應提供可	同 IaaS，並包括雲端應用	同 PaaS，並包括雲端軟體服

	IaaS	SaaS	PaaS
系統使用與存取	靠、持續性的監控機制。	系統平臺部分。	務部分。
資料安全	廠商對於虛擬主機平臺內之虛擬主機映射檔，應強化其儲存與使用安全，避免遭竊或有不當侵害情形發生。	1.達成 IaaS 資料安全管理。 2.雲端應用系統平臺內如存有機密或個人資料應依相關法令強化資料安全防護措施。	1.達成 PaaS 資料安全管理。 2.雲端軟體服務內如有機密或個人資料應依相關法令強化資料安全防護措施。
電子蒐證	廠商對於虛擬主機平臺應能建立電子蒐證機制，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、虛擬主機異動、資料存取及重要安全性事件等，並應確保其完整與正確性。	1.達成 IaaS 電子蒐證標準並擴展至雲端應用系統平臺層次。 2.雲端應用系統平臺內如存有機密或個人資料應依相關法令	1.達成 PaaS 電子蒐證標準並擴展至雲端軟體服務層次。 2.雲端軟體服務內如存有機密或個人資料應依相關法令落實電子蒐證機制。

	IaaS	SaaS	PaaS
		落實電子蒐證制。	
實體環境	設備所在建築物須符合 921 地震後內政部公佈之建築法規標準，5 級抗震設計。(提供土木結構技師出具之「建築物結構證明書」佐證資料)；門禁系統採 24 小時、365 天實體管制：所有溫度、溼度和門禁監控元件之狀態一律由中央環控系統進行控管；監控錄影應 24 小時無死角，且錄影保存期限宜至少 30 天。	達成 IaaS 實體環境管理。	達成IaaS實體環境管理。

資料來源：本計畫整理

(5)雲端服務使用者應考量雲端服務提供者是否有將雲端資訊系統或儲存資料移至本國以外地區之虞，並對其風險(包含違規風險)進行評估。

(6)雲端服務使用者就雲端服務委外作業，應落實定期對雲端服務提供者之查核，若雲端服務提供者已取得雲端安全國際認證(CSA-Star)銅牌以上、ISO 27017 或 ISO 27018 者，則可視實際情況要求提供驗證報告或進行實地查核。

(7)隱私安全需求-符合個人資料保護法及相關法規

對於雲端資訊系統中之個人資料數據，廠商必須依據法令辦理相關保護與管理事項，除個人資料檔案之備分保存外，亦應包括個資在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體所衍生之軌跡資料，如資料存取人之代號、存取時間、使用設備代號、網路位址(IP)、經過之網路路徑等，以比對、查證資

料存取之適當性。

(四)網路管理面

1.網路安全架構

(1)網路規劃與建置

A.在網路規劃時，網路管理人員應協同資訊安全人員，評估網路架構的規劃是否滿足營運需求及資訊安全管理體系之規範。

B.網路管理人員在規劃與建置內部網路與外部網路連線時，應將不同營運目的之網段加以切割：

a.Internet：連接網際網路之網段。

b.DMZ：對外開放網路服務的主機所放置之網段。

c.Intranet：含 Server Farm，為內部伺服器或部門間內部相互存取之網段。

d.Extranet：因配合業務需求，提供特定外部單位連線之網段。

e.VPN 連線：因配合業務需求，提供遠端網路之連線。

C.網路管理人員在規劃與建置網路時，重要設備如連結網路骨幹之中心交換器(Core Switch)、防火牆、路由器等，應考量組織歷史及資源分配等因素，適度配置備援(Redundant)機制，以滿足高可用性要求。

D.網段管理：為有效管理網路，將網路分成各網段，因業務或營運需要新增之設備，必須遵照各網路網段使用之用途設計，不可交叉混用及任意串接。

E.路徑控制：對於使用者端與被存取的電腦服務(Server Service)

間應予控制，以使用者採用其他路徑存取與業務活動無關之路徑。對於路徑使用者應被限制僅能與業務所需系統連線，以防止使用者連線至非本身業務所需之網段。可採用的控制措施如下：

a.透過內部使用者群組設置不同的邏輯網段(如 VLAN、區域、單位、業務等性質)來限制跨網段之使用網路服務。

b.網路管理人員於網路設備中設定通訊協定存取控制列表，以過濾並控制各單位之間封包流向、通訊協定或流量。

c.可於聯繫各網段間的路由器或交換器設定動/靜態路由機制及存取控制列表，使內外部使用者連線至所屬網路之節點。

d.網路管理人員宜定期檢核與營運直接相關之網路設備其存取控制規則。

F.外部網路連線管理：外部網路連線管理之目的在於確保網路上所有節點(包含個人電腦、主機、伺服器，或重要儲存設備)之資源與資料於各節點間之互通與受到應有的保護，並依其必要性而設置存取控制列表(ACL)，應考量控制措施如下：

a.需與外部網路連線時，應評估其風險，並考慮傳輸時所需之安全機制，及彼此權利義務之關係。

b.未經授權，不得私自於內部架設與外部網路連線之設備，如 ADSL、數據機、無線網路設備等。

c.外部網路與內部網路介接之網段，應配置適當之防火牆或路由設備，並依據存取控制列表設定安全控管規則，其他非必要服務一律阻絕，以達到網路服務安全。

d.外部網路連線服務通訊協定服務，採正面表列方式管理，

任何新增服務及通訊協定均應經過適當之授權。

e.所有非屬組織設備、主機及個人電腦，如有需要接組織網路，須透過適當之申請，並依其用途限制可連接之網路區段。

f.網路管理人員應定期檢視公共區域內之網路設備有無連線之需要，如無需要使用網路連線，應移除其網路連線。

g.外部電腦設備需連接回組織進行維護與控制時，需使用適當之安控機制，如回撥機制或 VPN。

G.網路位址(IP Address)管理

a.由網路管理人員統一協調，並規劃網路位址範圍，其中主機與網路設備應使用固定網路位址。

b.網路管理人員應管理並保持一份最新之網路位址列表，並依資產機密等級妥善保存。

c.網路位址異動時，應由網路管理人員統一指定，視需要更新相關 NAT 及 DNS 之內容。

H.網功能變數名稱稱系統(Domain Name System)管理

a.營運管理單位網功能變數名稱稱為重要資產，未經適當授權，不可任意以單位或個人名義向外界申請其他具有代表營運管理單位之網功能變數名稱稱。

b.網路管理人員應建立網路設備命名標準，作為命名之依據。

c.網路設備進行名稱異動時，應由網路管理人員統一指定名稱，其名稱不可與現存名稱重複。

d.網路管理人員應定期檢視內部與外部網路之 DNS 內容，以

維護其適當性與正確性。

e.在網路上使用 DNS 時，應採用下列控制措施：

應建立有良好保護之備援或次要名稱伺服器(Secondary Name Servers)，以輔助主要名稱伺服器。

DNS 應劃分內部網路與外部網路使用，且內部網路之名稱資訊應妥善保存，以防止外部網路或外界取得內部網路之名稱資訊與網址之對應關係。

啟用具封包過濾功能之路由器(Filtering router)或入侵防禦系統(IPS)，保護外部 DNS 免於遭受癱瘓服務(Denial of Service)攻擊。

DNS 應禁止未經授權 IP Domain Zone Transfer 之功能。

I.網路管理人員應編製網路拓撲圖及相關輔助說明(如用途、名稱、IP 及 Subnet ID 等)，以作為網路配置組態管理，並依其機密等級予以妥善保存。

(2)網路設備管理

A.設備應放置於機房統一管控，並使用專屬線路，以保護設備及資訊的安全，並提供適切的存錄與監控機制，以記錄相關執行活動。

B.網路設備連線保護措施

a.網路管理人員應變更網路設備預設之登入密碼，並避免共用帳號密碼，網路設備管理人員應定期變更網路設備之登入密碼，如網路設備可支援複雜性密碼，應考量採用複雜性密碼或其他雙因數認證方式登入密碼。

b.中心網路設備之維護與組態的變更，包含使用終端機模擬

程式、操控埠(Console Port)或網路設備管理軟體，應使用帳號密碼或其他認證機制，驗證身分後才可進行網路設備組態管理與變更。

c.使用終端機模擬程式連結網路設備進行管理維護作業時，應使用加密方式進行連結後，再登入網路設備進行相關作業。

d.網路設備的管理，除應限定由網路管理人員進行設定、維護外，亦需要：

限制終端機模擬程式連線之來源網路位址或網段。

如設備的功能允許，應啟動帳號密碼之驗證機制。

廠商使用之遠端連接埠平時應關閉，如需使用時則應由網路管理人員開啓使用，於使用完畢後予以關閉。

(3)防火牆管理

A.設置原則

a.如有兩道以上防火牆系統應儘可能採用不同公司廠牌，並於每一道防火牆採取兩台以上負載平衡架構或可互為備援自動切換架構，以提昇防火牆之可用性。

b.網際網路進出閘道口及重要主機進出閘道口須架設防火牆，確保重要主機及內部區域網路各級電腦的安全。

c.應透過防火牆機制，區隔內部網路(Intranet)、非軍事武裝區(DMZ)與外部網路(包含網際網路(Internet)、企業網路(Extranet))；並應將提供公開服務之主機(網站主機、郵件主機等)，建置於非軍事武裝區；除特殊因素外，來自於外部網路之連線將僅允許其連接組織網站主機、郵件主機或其

他提供對外服務之主機。

d.任何來自於外部網路欲進入內部網路之連線須經由防火牆及其他身分驗證機制驗證確認無誤後，始得通行；防火牆與服務主機應開啟適當稽核功能，記錄連線狀況。

e.使用網路專線與合作之各公私機構網域，須架設防火牆，確保內部網域的安全。

f.防火牆之取存政策為「Implicit Deny all」(正面表列)。

g.重要主機需經由防火牆控管，只開放內部使用者及內部非軍事武裝區伺服器進入，並只開放業務所需之必要服務通道，禁止由外部網路直接進入擷取資訊。

h.因業務需求，須指定來自外部網路連線之網路位置(IP)，方可連線至位於非軍事武裝區提供檔案傳輸(FTP)服務之主機。

i.對外開放之各業務網站、電子郵件，防火牆應開放其所需之服務通道，例如 HTTP、HTTPS，其餘非相關之服務通道一律禁止通行，並拒絕非軍事武裝區主機主動連線至網際網路。

j.除網際網路區使用外部公共(開)IP 外，由防火牆系統隔開之其他內部區域均設定為虛擬私有 IP，以阻絕公眾由外部網路直接進入內部各區域存取資源；對外開放公眾由網際網路進入之伺服器(如：網站伺服器)，應由防火牆系統轉址為外部公共(開)IP。

k.因公務需要開放或阻絕之特殊服務通道應另行申請，並經權責主管核准後始得開放。

l.應建置防火牆熱備援機制，以降低其對外服務中斷之時間。

B.系統管理

a.防火牆系統實體設備存放於控管之機房內，除網路管理人員外，其餘人員不得靠近使用。

b.網路管理人員對於新建置之防火牆系統，應檢查、修改或移除不適用之預設規則或參數設定。

c.網路管理人員應定期審查與檢視防火牆系統，如：防火牆過濾規則，並考慮效能以及邏輯重複問題。

d.網路管理人員應於防火牆系統上重要的檔案設定及規則變更時，將變更後的網路設備組態值加以備份，並集中保管於有權限控管之處。

e.網路管理人員應檢核進出各道防火牆系統之網路流量及系統效能，遇有大量佔用網路頻寬以致影響防火牆系統正常運作或其他使用者效能時，得立即中斷其服務，以維護其他使用者之權益，並依規定進行通報。

f.防火牆系統若遭遇大量網路攻擊時,網路管理人員應立即將該 IP 與 Service Port 進行緊急阻斷處置,必要時得關閉防火牆設定，以防止內部各電腦或網路設備遭受攻擊或破壞。

g.網路管理人員應適當保留防火牆系統所產生之稽核紀錄，並定期予以檢視，針對異常狀況進行通報，追蹤不明來源之惡意攻擊者，必要時得進行緊急之 IP 阻斷處置。

h.防火牆系統稽核紀錄應定期匯出存放及備份，並限定只能由網路管理人員、權責主管與資訊安全人員得以檢視及調閱，任何人均無權限可刪除紀錄，相關檢視應留存紀錄。

i.測試區域與正式區域連接最多以三個月為限,如需延長時間測試，應重新申請。但若特殊需求，經單位主管核定者，不在此限。

C.規則異動

a.營運管理單位因業務需求，需經 VPN(Virtual Private Network)或數據專線連接至資訊網路，以便進行各項業務工作，例如存取應用伺服器、網際網路、收發電子郵件等，或是存取網際網路(Internet)之其他網路服務時,若其網路服務非現行已開放之網路服務時(如 HTTP、HTTPS 等)，須向網路管理人員申請開放防火牆服務。

b.營運管理單位因業務需求架設伺服器以提供網路服務時，其提供服務之伺服器及通訊埠須由需求單位向網路管理人員申請開放防火牆服務。

c.各業務系統負責人、內部使用者或網路管理人員因系統實際運作要求須變更防火牆系統規則或參數之需求時，應由需求單位向網路管理人員申請開放防火牆服務。

d.當申請之目的消失，各業務系統負責人、內部使用者或網路管理人員應立即由需求單位向網路管理人員申請撤銷防火牆服務，並註明撤銷原因，提出撤銷申請後，由網路管理人員執行規則之移除。

e.為避免防火牆系統規則及參數設定因時間或業務變更等相關因素導致產生不符合現狀之處，網路管理人員應定期重新檢討規則及參數設定之適當性，並由單位權責主管覆核後，據以修正防火牆規則。

f.當有防火牆系統修正程式發布且內容包含嚴重安全性漏洞

或系統缺陷導致可能影響業務運作或穩定性時，網路管理人員應立即取得，經測試無誤後，在不影響業務正常營運之前提下，必要時共同協同委外廠商進行防火牆系統更新作業。

g.維護作業

h.防火牆應定期進行乙次維護，並視需要更新版本及修補程式。

i.委外廠商進行定期維護時,若須變更防火牆系統規則或參數之需求時，應向網路管理人員提出申請。

j.委外廠商應將該次維護進行變更之項目詳細記錄,由網路管理人員進行各項作業之確認並應保留該表單副本。

k.維護完畢且經網路管理人員測試無誤並簽名後，相關維護紀錄單由網路管理人員進行歸檔備查。

(4)入侵偵測防禦系統(Intrusion Prevention System , IPS)

A.設置原則

a.爲維護網路及資訊系統使用品質與安全，入侵偵測防禦系統管理人員應將風險較高之網際網路進出閘道口、DMZ 與 Intranet 區域納入入侵偵測防禦系統防護範圍，以偵測異常攻擊與違反資安政策之違規事件,確保 Internet、Intranet 與 DMZ 區域中個人電腦、伺服器及網路設備的安全與正常運作。

b.入侵偵測防護系統軟硬體設施之新增與維護、網路通訊埠設定之申請與變更使用，以及系統安全規則與參數訂定等，應由入侵偵測防禦系統管理人員負責統籌管理。

B.系統管理

a.入侵偵測防禦系統實體設備存放於控管之機房內，除入侵偵測防禦系統管理人員及被授權之維護人員外，其餘人員不得靠近使用。

b.入侵偵測防禦系統包含軟硬體設備及相關管理平臺，除被授權之人員可連接登錄操作外，其餘人員不得登入使用。

c.入侵偵測防禦系統管理人員應定期變更系統管理密碼，並設定適當密碼強度。

d.入侵偵測防禦系統管理人員應檢查、修改或移除不適用之預設規則或參數設定。

e.入侵偵測防禦系統管理人員應定期對入侵偵測防禦系統組態設定值備份後集中存放，並至少存放最近兩版的組態設定值。

f.入侵偵測防禦系統應定期進行維護,並視需要更新版本及修補程式。

g.入侵偵測防禦系統管理人員應每日定期監控入侵偵測防禦系統，並記錄留存備查。

h.入侵偵測防禦系統管理人員應對入侵偵測防禦系統定期製作分析報告，陳單位權責主管核可後留存備查。

i.入侵偵測防禦系統之韌體、組態、特徵碼及硬體有異動需求時，入侵偵測防禦系統管理人員應填單申請經核可後執行，並將異動前後設定值之差異紀錄留存備查。

j.入侵偵測防禦系統如具有備援設計,入侵偵測防禦系統管理人員宜定期進行演練並記錄演練結果，陳單位權責主管核

可後留存備查。

C.規則異動

a.各業務系統負責人、內部使用者或入侵偵測防禦系統管理人員，因系統實際運作要求、業務營運或因公務需要開放或阻絕特殊服務通道，有變更入侵偵測防禦系統之安全規則或參數之需求時，應填單申請經核准後始得進行異動作業。異動後，申請單應留存備查。

b.當申請之原因消失，各業務系統負責人、內部使用者或入侵偵測防禦系統管理人員應註明異動原因，提出異動申請。

c.入侵偵測防禦系統管理人員於入侵偵測防禦系統原廠發布更新資訊，如系統(OS 或 Firmware)更新、特徵碼(Signature)更新等，應於測試環境進行最新版本部署與測試作業，其中特徵碼(Signature)更新應每月定期執行。上述作業經測試無誤並取得單位權責主管核可，在不影響業務正常營運之前提下進行正式環境系統更新作業，必要時得要求廠商協助進行。

d.為避免入侵偵測防禦系統之安全規則及參數設定因時間或業務變更致與現狀不符，入侵偵測防禦系統管理人員之權責主管應定期重新覆核系統之安全規則及參數設定之適當性，必要時入侵偵測防禦系統管理人員應配合修正、調整。

e.遇有大量佔用網路頻寬、大量網路攻擊或其他緊急異常事件，以致影響網路正常存取運作、入侵偵測防禦系統正常運作或其他使用者之網路存取效能時，經網路管理人員評估為係受入侵偵測防禦系統影響時，應通知入侵偵測防禦系統管理人員進行問題處理，必要時應取得單位權責主管

核可後，立即進行緊急處置作業，包含變更系統安全規則及參數設定，以維護其他使用者之權益。

(5)路由器及交換器

A.網路管理人員應定期檢視核心路由設備流量與系統負載程度，適時提升容量，並考量路由器及交換器可用性等級，設計備援機制。

B.如為電信公司放置於營運管理單位之網路或通訊設備，應指定人員負保管、監看及故障通知之責。

C.若路由器以遠端連線進行管理，應於主要路由器中作適當之安全設定，例如：

a.限制來源 IP

b.使用密碼認證

c.路由器系統設定檔須定期與變更前進行備份。

d.路由器系統設定檔僅開放存取權限予路由器系統管理人員。

D.外部單位路由器傳輸管理：

a.與外部單位路由器間傳輸需採取專屬線路或是加密連線方式進行。

b.加密連線須設置自動定時交換金鑰的連線機制。

c.加密金鑰產生：以一組固定長度字元之初始加密值經由演算方式，產生符合加密要求 168 位元（含）以上之金鑰值執行加密傳輸。

d.初始加密值由安全管制部門保管及產生。

e.初始加密值須由營運管理單位、系統管理人員配合資安技術人員定期變更。

(6)無線設備

A.設置原則：

a.架設無線 AP 之機制，應採用中央控管方式，以利無線網路管理人員之定期檢視與查核

b.設定無線 AP 射頻(RF)信號之涵蓋率，減少不必要的無線電波暴露以避免有心人士截收通訊封包再進行內容破解，使用天線時必須針對使用環境作調整，限制溢出控制範圍之外的無線電波在合理範圍內。(目前對合理範圍的偵測是：以筆記型電腦內建之無線網路卡，使用微軟無線訊號搜尋軟體，所偵測到的電波強度為平均不高於 40%，且無法連續 30 秒內不中斷。)

c.變更無線 AP 之通訊頻道(channel)，以避免基地台之相互幹擾。

d.不定期使用工具(如 NetStumbler 等)，搜集非法架設之無線 AP。

B.系統管理：

a.變更無線 AP 之預設管理密碼，同時必須定期變更管理密碼。

b.關閉無線 AP 之還原出廠設定值功能。

c.限制無線 AP 之遠端管理 IP 及變更預設的管理埠號(port number)。

d.設定無線 AP 之 Service Set Identifier(SSID)及變更預設頻道

(channel)，SSID 之設定值應避免使用銀行名稱，並注意長度及複雜度，可考慮混合使用英文大小寫字母、數字等。

e.關閉 SSID 廣播模式(封閉系統認證，Closed-system Authentication)，以保護無線 AP 之名稱讓惡意使用者難以偵知。

f.設定啟用無線 AP 之 WEP(Wired Equivalent Protocol)加密，其金鑰長度不得低於 128 位元，並視使用頻率變更 WEP 金鑰：或 WPA 加密驗證機制，或是使用其他更為嚴謹之加密驗證機制。。

g.採用至少使用英數、文字混合等足夠複雜的使用者帳號密碼登入驗證方式，或是以更為安全有效的機制限制連線的存取權限。

h.設定無線設備之 IP 分配範圍。

i.不使用無線 AP 之 SNMP 社群碼(SNMP Community String)或使用時須變更無線 AP 之 SNMP 社群碼並搭配有效的控管機制，或至少需使用 MAC 位址存取列表（ACL）限定可存取 SNMP 資訊的 IP 位址等管理參數之設定。

j.建置虛擬私有網路(VPN)通道，利用加密技術(如 Tri-DES 等)配合認證機制，以保護使用者與無線 AP 之間傳輸資料。

k.關閉無線 AP 之簡易模式(Ad-Hoc mode)，使用基礎架構模式(Infrastructure Mode)，以避免惡意使用者利用無線使用者間的點對點(peer-to-peer)直接通訊，將合法無線使用者作為攻擊跳板。

l.無線 AP 之設定，應另行彙總製作無線 AP 設定彙總表(SW-0066-F005)，其電子檔案及檔應妥為保管及備份。

m.無線 AP 之設定需異動時，則由無線網管人員填寫無線 AP 設定變更申請單，經網管單位主管同意後始可開始異動作業，同時其異動應盡可能留下異動前後紀錄存查。

n.應定期進行無線 AP 之韌體版本檢視、系統弱點是否修補等作業。

C.例行管理與維護

a.僅網路管理人員可存取、設定、變更與維護營運管理單位之網路通訊設備。

b.網路管理人員使用之網路設備，如有使用備援設計，宜定期演練並記錄演練結果，以確保網路設備之可用性。

D.網路實體安全：

a.網路服務設備的實體應置於管制區域內，如有特別情形無法置於機房或封閉空間內之設備(含交換器、路由器、Gateway、網路主機等)，資訊資產保管者應列冊記錄，並定期檢查設備之實體連接與設定是否有異常現象。

b.網路服務設備僅有經授權之人員始可存取，外部維修人員或廠商因維修需要使用設備時，必須由該資訊資產擁有者指派之人員陪同進行。

c.電源纜線與通信電纜承載資料或提供資訊服務，應避免被截斷或受損，應考慮以下控制措施：

d.為避免網路傳輸線路(包含網路線及電話線)遭致蓄意或非蓄意的破壞，所有網路傳輸線路的實體線路應適當予以保護，如隱藏於地板下或隔間內。

e.電力纜線應儘可能與通訊纜線隔離，以避免相互幹擾。

f.經界定為與營運直接相關之網路設備，如路由器、交換器等，應放置於具有良好實體保護之區域。

g.網路傳輸線路應避免經過容易產生高溫或電磁幹擾的區域，以確保線路之適當運作。

h.主要連外網路傳輸線路，應設置備援線路。

i.為避免產生相容性衝突，網路傳輸之線材及設備之選用應採用符合國際標準規範之產品。

j.網路管理人員應定期檢測重要纜線上是否附著未經授權之設備。

E.變更管理

a.核心交換器及對外防火牆設備之韌體、組態、硬體、網路邏輯(包含 VLAN 與 VLAN Trunk 設定)與實體架構(包含實體線路)異動作業應經過申請程式進行變更，未經適當授權程式，不可任意修改。異動人員亦應於每一次異動作業完成後，留存異動紀錄。

b.當網路架構或網路設備之組態值變更後，網路管理人員應更新網路拓撲圖或相關輔助說明，並將變更後的網路設備組態值加以備份，集中保管。

c.通訊協定管理

F.遠端登入：

a.針對遠端登入行為進行控管，其中應設定連線閒置時間或最大連線時間。

b.對於遠端存取服務，應透過適當的申請核准後方可使用，且應使用安全的遠端連線機制。

c.遠端登入過程，應啟動稽核功能與安全性監控。

G.端連線作業限制

a.僅允許使用特定通訊協定。

b.僅允許存取特定的伺服器資源。

c.僅允許從特定的 IP 存取電腦資源。

(7)網路服務管理

A.網路管理人員應整理重要網路設備所提供之網路服務清單，當中應包含提供網路服務之業務目的、可使用之單位元、連線方式描述等資訊。

B.重要網路設備，如分割各網段之防火牆、核心交換器、對外部網段提供服務之網路負載平衡設備、對外之網路代理伺服器等，所提供之網路服務(如 HTTP、FTP、SMTP、POP3、DNS、TELNET、SNMP 等)，應有適當之管控機制，以確保該網路服務啟用之適當性。

(8)網路檔案服務(Network File Service, NFS)

A.由於 NFS 缺乏內建之安全機制,使用時應採取下列控制措施:

B.除經適當授權外，電腦主機嚴禁存取 NFS 伺服器。

C.應限定各主機存取檔案系統之類型(如唯讀等)。

D.禁止將 NFS 伺服器開放給任何放在外部網路的電腦主機存取，以避免遭到外部人士的入侵。

E.禁止未經授權於內部網路當中進行檔案分享，如透過網路上的芳鄰分享檔案、正式環境之 UNIX 主機未經授權安裝 SAMBA 軟體等。

F.除經適當授權外，所有檔案分享應透過檔案伺服器，並且依循申請程式，註明內容、分享對象及開放時間。該伺服器之資訊資產保管者應將逾期之檔案分享關閉，並通知申請人將不須使用之檔案移除。

(9)通訊協定傳輸安全考量

A.透過網路傳輸資訊時，應考量傳輸內容之正確與完整性，且確保其不被未經授權存取。

B.傳輸重要資料時，應將傳輸資料之機密等級與傳輸途徑予以適當之加密或其他安全機制防護。

C.傳輸使用之加密技術及安全機制須先經資訊安全人員評估。

D.稽核軌跡與網路資安事件處理。

(10)網路介接管理

A.與其他電信業者介接之網路，應明訂網路介接責任點，並於互連合約中予以說明。

B.部維護與其他業者之互連網路架構圖，並標示責任介接點。

C.建立互連網路之監控運機制，依照互連資訊，判斷告警產生的互連業者，並通知相關單位處理。

(11)網路流量管理

A.應事先定期收集關於災難、意外事件(如風災、水災)、社會現象、逢年過節或特殊節日等導致電信設備失效與網路壅塞之相關資訊，並彙集相關關鍵知識的 KPI 報表，提供分析比較之用。

B.針對特殊活動/災害事件，應收集相關時段話務資料進行比

較，瞭解網路使用狀況，以進一步分析判斷設備壅塞的相關資訊，作為設備擴充或話務分流改善參考。

C.交換機應具備網路過載及壅塞控制之機制，以偵測網路壅塞並避免網路壅塞時通訊集中之情況。

D.應制定設備壅塞的警戒值產生告警，經過評估後進行設備擴充或話務分流改善狀況。

(12)網路風險管理

A.應設定使用者電信服務供應商的提示以資識別。

B.NMC 網域啟用 Anti-spoofing 功能，偵測 IP spoofing。

C.採用適當的鑑權機制以防範來源造假，另 POI 來話對方局，應根據互連協議作必要的來源管控。

2.電子郵件服務管理

(1)安全防護

為加強電子郵件的安全防護，在電子郵件傳輸連線時，進行封包特徵的過濾檢查，如封包來源的網功能變數名稱稱、IP 位址、電子郵件地址、發信量及發信次數等。但是要深入解析郵件內容，以找出危險性過濾特徵，則要針對電子郵件安全管理系統於應用層進行電子郵件的本文及附加檔案之過濾檢查。

從電子郵件經由網路進入郵件閘道設備、郵件伺服器到用戶端電腦的過程中，因應發展出相關的郵件威脅防護技術，本指引將分類成加密技術、廣告信防制、與惡意郵件防制等，並依據資訊安全不同面向，介紹關於郵件服務可用性、郵件完整性，以及雲端與行動應用中需注意的資安事項。

(2)加密與機密性保護

A.傳輸加密機制

包括 SMTP、POP3、IMAP4 以及 Webmail 所使用的 HTTP 都支援透過 TLS (Transport Layer Security) 的傳輸加密方式來維持資料交換過程的機密性。一般熟悉的 HTTPS 是透過 TCP 埠號 443，在瀏覽器與網站主機間透過 TLS 加密方式來回傳遞資料；同樣地，郵件傳輸所需使用的各項協定包括 SMTP、POP3 及 IMAP4 也都有對應的標準埠號提供加密傳輸，而且需要使用的電子憑證，通常與 HTTPS 需要的相同、不需增加額外的憑證成本。

B.郵件加密機制

電子郵件可以冒名寄送且信件的內容可能遭到竄改，透過專屬於個人或機構的電子憑證及金鑰交換機制對電子郵件簽章或加密，將可提供郵件的「完整性」、「不可否認性」或「機密性」。其做法為經由憑證機構所簽發之電子憑證，將憑證存放在用戶的電腦中，使用者於傳送電子郵件時，可於電子郵件中加上數位簽章如同使用者簽名一般或做檔加密保護，增加電子郵件的安全性。

為維護最高安全性，須確保任何安全的郵件管理機制(如加密)要在特定使用者的電腦上執行，而該電腦也必須受到實體與電子化的保護。

(五)環境管理面

1.電腦機房實體環境管理

(1)進出 4G 應用服務系統之電腦機房大門應有門禁隔離設施以防止未經授權的存取，如使用門禁刷卡裝置、警報裝備、門鎖等，

確保經適當授權的人員始可進入，且應留存進出記錄。

(2)授權人員因工作需要，營運管理單位相關指定權責人員同意許可後始得進入機房，由機房管理人員陪同並記錄進出時間、事由、處理結果等事項。

(3)經發給門禁感應卡片者，不得轉借他人使用，否則如生變故，轉借人應付連帶責任。

(4)外賓參觀均由營運管理單位陪同下始得參觀，拍攝機房則須營運管理單位同意，否則一律不准拍照或攝影。

(5)門禁進出許可人員清單應定期被檢視一次，以確認進出許可授權之適當性。

(6)安全區域之劃分由 4G 應用服務系統營運管理單位行政部門執行，若有異動應公告區域劃分情形，以利 4G 應用服務系統營運管理單位員工瞭解遵行。

(7)所有人員進入 4G 應用服務系統營運管理單位管制區域內，均應佩帶 4G 應用服務系統營運管理單位核發之識別證件，且不得借予他人使用。如發現未佩帶識別證件之人員，且無 4G 應用服務系統營運管理單位員工陪同時，應主動要求出示識別證件或立即通知警衛。

(8)假日來賓進入營運管理單位洽公或工作，應於事前由營運管理單位陪同作業人員填具登記簿提出申請，經營運管理單位核准後方得作業；如為緊急狀況處理，應於事後補陳核；該登記簿至少保存一年，逾期依規定辦理銷毀。

(9)非 4G 應用服務系統營運管理單位員工來訪，應先進行登記及確認身分，並以電話通知受訪人員，由 4G 應用服務系統營運管理單位員工陪同，方可進入。

(10)監視管理

A.應隨時注意環境監控系統，若發現異常狀況應即刻通知維護廠商處理。

B.電腦機房應設置必要之監視設備，並針對重要與非常出入口裝設警報器或偵測系統，以作為警戒或記錄資訊安全事件之機制。

C.於機房出入口、電信室及機房內部...等區域，設置無死角 CCTV 監視點，24 小時進行監控錄影，CCTV 監控錄影以數位資料儲存、儲存期宜至少一個月。

D.監視系統為完全掌握監視範圍所有情形，採全天候動態錄影存證。

E.錄影存檔時間：考量調閱影像時效性及成本效益，錄影存檔時間宜為九十天左右。

F.需調閱監視錄影資料時，申請人應向資料管制科申請辦理，並會同管理員由其操作共同調閱。

G.主管機關之金融查核、4G 應用服務系統營運管理單位稽核單位，需相關單位代為申請核准後，由管理員負責調閱。

H.管理人員應定期校正監視系統之時間，以確保與其他重要系統之時間一致，以確保錄影檔案的正確性及可信度。

(11)環境管理

A.電腦機房溫度應保持 16 度 C~30 度 C 之間，相對濕度保持 25%~70%之間，有異常時應採取相關措施。

B.大樓出入口宜設 24 小時專職保全人員，負責過濾人員進出及安全巡邏。

C.電梯設置門禁卡管制，電腦紀錄出入人員及時間。

D.需有不同主機(水冷式、氣冷式)作為備援並提供恆溫恆濕下吹式系統。

E.中央電腦監控 24 小時專人監控，視當時環境溫濕狀況進行遠端操作。

F.安全區域之劃分由 4G 應用服務系統營運管理單位行政部門執行，若有異動應公告區域劃分情形，以利 4G 應用服務系統營運管理單位員工瞭解遵行。

G.機房內禁止抽菸、進食、飲水或存放私人物品。

H.人員進入機房之前應先脫鞋或更換乾淨拖鞋。

I.機房地板應由清潔人員定期清掃。

J.機房內及其四周宜定期實施防治鼠害及其它蟲害等措施，以保護電纜及各項設備之完整。

K.機房防火設施應定期檢查，滅火器有效期滿前一個月應予換新。

L.機房所有之電力系統與不停電設備應定期檢查。

M.有關機房環境之維護，除各項規定需由操作員每日自行遵守、執行者外，其餘作業均由有關單位主管監督執行，並留存相關紀錄備查。

(12)管制區域進出管理

A.管制區域進出管理應考慮以下控制措施

a.進出管制區域的大門應有門禁隔離設施以防止未經授權的存取，如使用門禁刷卡裝置、警報裝備、門鎖，或使用人

工值班駐守的接待區域等，確保僅有經過適當授權的人員始可進入。

b.因業務需要，如設備維護，而獲臨時授權進入管制區域之協力廠商廠商人員，工作時應由 4G 應用服務系統營運管理單位資訊人員陪同與監督，並確實填寫進出登記，詳載出入之時間、目的及處理事項。

c.因工作需求，需攜出入電腦資訊暨週邊設備等物品時，應於「資訊設備異動清單表」上詳載攜出入物品之種類、使用時間、目的及處理事項，經 4G 應用服務系統營運管理單位機房管理權責部門核准後始可攜出入。

d.機房之門禁進出許可人員清單應由 4G 應用服務系統營運管理單位門禁卡管理單位定期檢視，以確認進出許可授權之適當性。

e.貨物、設備及運送人員進入 4G 應用服務系統營運管理單位前，權責人員應確認身份無誤並檢視無異常狀況後方可進入，進入期間應有同仁陪同。

f.於進行機房例行性作業時，應填寫「機房作業檢核表」，進行系統容量、溫溼度等紀錄。

g.管制區域作業規範

h.在管制區域內工作，應考慮以下控制措施

i.管制區域之工作人員名單及工作內容，應依相關規定進行申請。

j.要求進入人員須佩帶 4G 應用服務系統營運管理單位核發之識別證，並應詢問無人陪同以及未佩帶證件的非 4G 應用服

務系統營運管理單位員工。

k.因業務需要而獲授權進入管制區域之協力廠商廠商人員，工作時應由 4G 應用服務系統營運管理單位業務負責人陪同與監督。

l.管制區域內禁止吸煙與飲食、另禁止放置易燃、易爆物品。

m.人員離開管制區域時，應確認門窗已確實關閉並鎖上。

n.危險或易燃材料儲存、物品裝卸作業應與管制區域保持安全距離。

o.消防設備、空調設備、不斷電系統與監視設備等支援性設備之規劃、設置、管理與檢視由 4G 應用服務系統營運管理單位行政部門或機房管理權責部門負責。

p.管制區域應設置必要之監視設備，以作為記錄資訊安全事件之機制，監視紀錄宜至少保留一個月。

2.資訊設備管理

(1)設備管理

A.資訊設備應置於具有門禁管理、空調、電源供應穩定、防火、耐震與抗洪之管制區域內，以避免非法存取或破壞行為。

B.資訊設備保管者須實施基本維護，且被授權的維護人員才能對資訊設備進行維護。

C.資訊設備維修應以就地維修為優先，如需設備送修，應將存放於硬碟之機密性資料予以移除。

D.機房各項電腦設備之設置與搬遷，會同機房管理人員或設備保管人員處理。

E.機房電腦設備發生故障，系統管理人員應立即聯繫相關系統負責人及主管或代理人後，再通知維護廠商進行修護。

F.廠商維修機器之零組件或異動系統設備設定值時,應獲核准後始可准許變更。

G.若因維修機器之零組件或異動系統設備，需要將零件或設備攜出入，應留有紀錄。

H.伺服器暨資訊設備進出機房時，系統管理人員應進行伺服器暨資訊設備進出資訊部機房申請，經核可後方可進出機房。

I.電腦設備之臨時性保養維護,應由設備保管人員視需求填寫提出申請，經核准後，依規定委由專業廠商辦理電腦設備之保養維護，進出機房時須填寫機房門禁進出管製錶；例行性保養維護應依相關設備維護合約所規範之維護項目進行保養維護，維護廠商進出機房時亦須填寫機房門禁進出管製錶並由設備保管人員陪同進出機房。

J.廠商如需攜帶可攜式設備連接至公司資訊設備使用，需填寫電腦設備暨可攜式電腦攜入單經由單位主管簽核與同意後，才允許將可攜式設備攜入公司使用。

K.資訊設備經評估不堪使用或不再使用時，應由資訊設備擁有者指派人員對其儲存設備進行破壞或採取其他可確認資訊無法再利用之機制，經安全管制人員確認其狀態，方可進行處分、報廢或變賣。

(2)設備保養

A.依據供應商建議的保養週期與規格進行設備維護。

B.由具有合格及經授權的維護人員進行修理與保養設備。

C.保存電腦機房設備之維護紀錄及定期維護報告書。

D.電腦機房設備原則上不允許攜出局外，如有需要攜出，應先清除設備內儲存媒體之機敏資料，確保設備內機敏資料不被讀取。

E.機器設備之維護作業，須由設備保管人員或機房操作員陪同維護廠商工程師辦理，必要時得會同相關人員或水電技工協同辦理。

(3)設備使用

A.批次作業及備份作業，若在處理上能預知可能發生之異常情況，業務負責人員應事先提供批次作業中斷對策表供機房操作員依內容作業。

B.非經常性且須即時處理之緊急作業等特殊作業，均應先報准後，協調相關人員再行處理，並於事後補行申請程式。

(4)媒體管理

A.磁帶置放之場所應留意其實體安全控制措施，避免未經授權人員存取。

B.應考量業務性質定期進行網路附接儲存(NAS)備份，同時每週將網路附接儲存(NAS)資料手動備份到磁帶。

C.應定期進行備份媒體之盤點並將媒體盤點紀錄呈權責主管覆核。

D.每隔週進行備份媒體異地儲存。

(5)正式主機開關機作業

A.申請若對業務有重大影響之正式主機開關機的需求，應填具

變更申請單提出申請，並經由申請單位主管核可，估可行性及影響範圍，指派專責人員填寫開關機時機、開關機程式、及各應用系統配合處理事項之負責人員以及測試人員後始可執行（如遇緊急狀況，可先口頭報備，經核可後先行執行開關機作業，再後補申請表）。

B.開關機公告：執行人員須於關機前公告系統開、關機時間（如遇緊急狀況，可先口頭報備，經核可後先行執行開關機作業，再後補公告。

C.開關機時機確認：正式系統除緊急狀況，以不影響公司業務運作，方可執行，開關機前務必確認復原程式是否妥當。

(6)主機臨時作業

若需正式主機配合系統異動測試，申請單位應填具變更申請單經核可後，依作業程式處理。

(7)主機新增作業

如為新增之主機作業，應由申請單位經辦填具應填具變更申請單提出申請，經申請單位主管核可後依作業程式處理。

(8)主機系統設備異常處理

A.系統管理人員發現系統中斷、故障或異常時，應先行檢查，由電源、設備燈號及訊息來進行判斷，並依相關故障標準作業排除問題。

B.若非故障標準作業程式可處理，應與相關系統負責人員或維護廠商聯絡，請其支援及故障排除或到場進行檢測維修；並告知相關權責主管及相關應用系統負責人。

C.機房設備發現問題，機房管理人員應立即通報，協同系統管

理人員處理，並提供必要之協助，若未能立即徹底解決時，將問題發生時間、問題內容記錄緊急公告並通報相關單位。

D.機房操作員應隨時注意機房作業環境，如有非計劃性停電、空調故障、火災、水災、地震、空襲等狀況，應立即通報權責單位主管與水電技工，進行故障處理。

E.機房內之各項設備如發生故障，機房操作員應根據電腦系統之問題，即時通知水電技工或相關科人員到場研判其故障類型，並設法排除故障，以恢復運轉。若無法自行解決者，應立即通知廠商調派支援人員前來修護。如修護時間需超過半小時者，應立即報告上級主管協調採取應變措施。

F.設備故障及重大事件排除或處理後,機房操作人員應於機房操作日誌記錄故障發生時間、通報處理情形與解決時間。機房操作日誌應每日送交權責主管簽核並留存。

(9)連線線路異常處理原則

接收出現線路連線異常訊息，應立即做下列處理並將故障訊息應詳加紀錄於緊急公告，應通報相關業務單位。

A.判斷是否影響交易，並儘速通知相關主管及系統負責人員。

B.檢查備援(主要)線路是否正常。

C.緊急報修電信廠商，並後續追蹤故障查修情形。

(10)資訊設備報廢

A.資訊設備經評估不堪使用或不擬使用時，應將其硬碟格式化、覆寫資料等方式予以清除硬碟內資料或採取實體破壞等方式以確保資料不可讀，經權責單位主管確認後，方可進行報廢。

B.資訊設備進行移交時，應將硬碟低階格式化或覆寫資料等方式予以清除資料，由權責單位主管確認其狀態後，方可移交。

C.測試設備使用完畢後歸還廠商時，需確認硬碟上屬於 4G 應用服務系統營運管理單位的資料皆以格式化或覆寫資料方式予以清除，並由權責單位主管確認其狀態後，始可歸還。

(11)無人看管之資訊設備

A.無專人看管之資訊設備應放置於有獨立門禁或有 24 小時監控管制區域，以限制非經授權人員存取。

B.無人看管之資訊設備或公用設備，如放置於非管制區供使用者使用，應設定連線時間，或使用者不再使用時 10 分鐘後系統自動登出系統。若資訊設備位於 4G 應用服務系統營運管理單位外，則需加強實體安全控管且應定期檢查設備之線路連接與設備之設定以確保設備安全。

(12)安全區域管理

A.安全區域規劃

a.應對安全區域範圍進行劃分，以保護重要區域及資訊處理設備等資產。

b.安全區域之規劃應由單位主管指派權責人員執行，由門禁系統管理單位進行公告，若有異動應公告區域劃分之變動情形，以利員工瞭解遵行。

c.危險或易燃材料儲存、物品裝卸作業應與安全區域保持安全距離。

d.堆放及儲存在安全區域內之大宗物品，如電腦零組件，應放置於規定地點，並排列整齊。

e.建築物應考慮具有耐火性及避震性。

f.應有足夠之煙、熱偵測器及警報設備。

g.應有足夠之滅火設備。

h.緊急逃生路線應明確標示，並應有緊急照明裝置。

i.應設置自動滅火設備，並具有手動啟動功能。

j.應符合相關營建及消防法令之規定。

k.管制區域所有可能潛入的風險點(如門口、窗戶)附近應設置適當之監控或警示設備。

l.管制區域應設於較高處，以防水患。

m.管制區域之地板、天花板等應具有不易燃性。

n.除電腦主機所需之冷卻水管路外，一般水管或蒸氣管應設於電腦機房外。若需經過電腦機房之水管，須確認其不會有漏水之慮。

o.貨物、設備及運送人員進入 4G 應用服務系統營運管理單位安全區域時，權責人員應通知相關部門協助確認身分無誤後，方可進入。

B.人員進出管理

a.安全區域之進出應設置門禁管制，並實施適當之身份驗證機制或管控措施。

b.所有人員進出安全區域，均應佩戴核發之通行證件，且不得借予他人使用。如發現未佩戴通行證件之人員，且無員工陪同時，應主動要求出示識別證件。若為非營運管理單位員工(如來賓、廠商、本行其他單位員工等)來訪，則應先進行登記及確認身份。

c.因業務需要，由廠商長期派駐之協力廠商服務人員，應依據相關規定提出申請，協力廠商服務人員出入安全區域必須佩戴通行證件。

d.安全區域之出入門戶應盡可能設置自動關閉機制，並應養成隨手關門之習慣。

e.新人報到前，應申請辦公區域進出權限。若 4G 應用服務系統營運管理單位員工遺失辦公區域之門禁卡，應向門禁管理單位申請補發。

f.訪客及協力廠商服務人員，應於訪客登記簿進行登記並提供證件。由接待人員確認身份後，提供訪客證給訪客或協力廠商服務人員，由 4G 應用服務系統營運管理單位員工陪同方可進入辦公區域。訪客進出之紀錄宜至少保留 3 個月。

g.辦公區域門禁刷卡權限清單應由權責單位主管定期檢視一次，以確認授權之適當性。

h.設定辦公區域門禁刷卡系統之權限應由權責單位主管指派人員管理，並定期檢視該系統權限之適當性及留下紀錄 。

i.人員進出辦公區域，應佩戴核發之識別證件，且不得借予他人使用。如發現未佩戴識別證件之人員在辦公區域，且無公司員工陪同時，公司員工應主動要求出示識別證件。

j.公司員工於離職，訪客或協力廠商服務人員於作業結束後應繳回識別證。

k.辦公區域之出入門戶應儘可能設置自動關閉機制，或養成隨手關門之習慣。

C.辦公區域管理

a.具有資料複製功能之設備，如影印機、傳真機、掃描機等，應放置於辦公區域固定地點。若因業務需要而放置於外部單位人員工作區域，應經權責主管核准後始可使用，並於專案結束時移除。

b.列印、影印或傳真收發機密等級文件時，應立即領取，並同時取走原始文件，不可任意棄置，以避免機密資訊外洩。

c.無人領取之傳真機、影印機、印表機原始檔或列印檔，應予以銷毀。

d.會議室使用後，應立即清除白板與桌面資料。

e.人員應使用門禁卡進出辦公區域，若離職時應將門禁卡繳回人事單位。

f.未經辦理會客換證手續，勿逕行帶領非 4G 應用服務系統營運管理單位員工進入門禁管制區域。(主管賓客由秘書負責辦理換證手續)

g.勿於辦公區內，使用個人高用電量之電器品(如咖啡爐、電暖器等)。

h.使用具有資料複製功能之辦公室設備(例如：影印機、傳真機、掃瞄機等)，接收重要業務機密資料時，當事人應在旁等候，避免遺漏機密/重要資料。

i.下班後應將經辦之機密性或敏感性資料，妥善收藏。

j.下班後應將個人保管之電腦及週邊設備關機。

k.無人看管之資訊設備(包含個人電腦)，應立即登出或以密碼鎖定，以防止未經授權的使用。

l.應瞭解使用消防滅火相關裝備設施及逃生動線。

m.勿隨意撕除個人電腦封條。

n.廠商及訪客攜帶之電腦，不得連入公司內部網路系統。(受訪關係員工負告知責任)

o.非經授權許可，非公司之電腦(含個人電腦)，4G 應用服務系統營運管理單位員工不得攜入公司並且禁止連入內部網路系統。

p.非經授權許可，勿利用其他外接式儲存設備((包含筆記型電腦、個人數位助理 PDA、燒錄機、…等))，拷貝公司業務機密。

q.遺失門禁卡應及時告知管理部門換發，勿超過三日。

r.員工離職時不得將業務資料拷貝攜出，必要時需再簽訂保密切結書，始能離職。

s.員工辦公區域以外設備使用所提供的實體安全保護等級，

應與爲辦公區內同類設備提供的同等或更高。如在外使用之可移動的資訊設備，應設置密碼保護以確保資料的安全，當內存機密等級以上之資料時，應考量於設備中加設加密機制。

t.桌面與螢幕淨空

個人辦公桌面應維持清潔，下班前應將業務上使用之文書歸檔整理，並依據資訊資產之分類原則，將機密檔放置於上鎖的檔櫃中。

個人作業不再使用之機密文書資料，應使用碎紙設備或其他銷毀方式進行銷毀，避免有心人士收集資訊。

除監控用電腦外，使用個人電腦與無人使用之資訊設備應設置螢幕保護程式，以防範他人伺機窺探。

u.電腦軟體的管理

公司使用之軟體應有版權或授權使用證明。

各電腦應建立軟體清單，並定期檢查所使用之軟體是否皆屬合法軟體，詳細作業內容請參考電腦軟體管理相關規範。

業務專用電腦嚴禁載入業務以外之軟體。

為避免資料外洩與病毒攻擊之威脅，使用個人電腦不得從事以下行為：

- 不得拷貝非法軟體於公司內使用。
- 不得安裝及使用點對點等大量佔用網路頻寬資源的軟體。
- 不得下載及使用盜版軟體、音樂及電影等。

●不得從事網路遊戲、網上賭博或聊天等活動。

v.可攜式儲存媒體的管理

公司之磁帶、磁片、光碟片等各式可攜式儲存媒體應於封面或明顯處標示該儲存媒體用途。

可攜式儲存媒體於使用完畢後，若無保留之需求，應將內容刪除，無法刪除者應妥善保管或銷毀之。

w.儲存媒體之保存及運送

媒體運送時，應注意非法存取、濫用或破壞等事項，重要資料應指定授權人員負責運送，並考量將儲存資料亂碼化、加密及其它確認資料安全之機制。

重要媒體運送時，應考量控管措施，如存放於上鎖之儲存容器、不同的運送路線、分批運送等。

x.電話及傳真機之控管

使用公司電話應儘可能避免談論公司機密資訊。

應儘可能避免使用傳真機傳送機密資訊，若傳送對象用途固定，可採取簡碼方式控管。

y.可攜式電腦環境

攜帶公司之筆記型電腦外出至公共場所時，應注意設備遺失及資訊外洩之風險。

公司之可攜式電腦攜帶外出時，應提出申請。

有關可攜式電腦設備應遵循之相關控管，應依據可攜式電腦設備管理規範辦理。

z.複製能力設備之控管

使用具有複製能力之設備（例如：影印機、印表機、傳真機等）應遵循安全區域管理程式相關規定及設置使用管制程式(如：使用密碼等)，以防外部人員擅自使用；並指派人員定期檢查是否有涉及個人資料之檔長時間未取走情形。

aa.行動裝置之控管

攜帶公司所配發之行動裝置或受公司管制之行動裝置，應進行安全防護措施設置及異常監控，並注意裝置遺失及資訊外洩之風險。

非 4G 應用服務系統營運管理單位配發之行動裝置，原則上不開放使用公司內部網路，如需使用公司內部網路應取得權責主管及資訊單位核可後方可使用。

有關行動裝置應遵循之相關控管，應依據行動裝置安全管理規範辦理。

bb.監視設備之設置

各管制區域應設置監視設備，做為監控與記錄安全事件之機制。監視設備之規劃、設置、管理與覆核由相關單位辦理。監視設備攝影紀錄應保持清晰可供辨認。

上述監控系統之監控紀錄宜建立媒體備份異地儲存。

D.公共區域管理

公共區域相關管理措施如下：

a.機密與內部限閱等級之檔禁止任意放置於公共區域。

b.分機表及通訊錄等具有聯絡資料及身分之檔應避免張貼於

公共區域。

c.應避免於公共區域討論業務及工作內容。

d.機密等級為機密與內部限閱之檔禁止任意放置或張貼於公共區域。

e.會議室使用後，應立即清除白板上資訊。

E.協力廠商服務人員工作區域管理

a.協力廠商服務人員應於獨立之協力廠商服務人員工作區工作。如因工作需求需於管制或辦公區域工作時，應受營運管理單位人員監督。

b.協力廠商服務人員經授權主管核可後發予門禁卡，均設定於上班期間始可進入；非上班期間則須由人員陪同。

c.協力廠商服務人員工作區須為獨立之網段，與區域網路有所區隔，不得連線所有正式環境之伺服器，如因特殊需求需連線至正式環境之伺服器或網頁，須以透過申請單載明使用原因、使用項目、連線設備、正式環境之電腦主機或網頁及使用期間(限於簽訂之合約期限內)，經核可後由網路管理人員設定，以確保安全。

d.協力廠商服務人員於進行開發或維護工作期間，除有特殊情形申請核准外，皆需於協力廠商服務人員工作區進行作業。

e.於協力廠商服務人員工作區使用期間內，隨時保持辦公桌面及環境清潔整齊。

f.協力廠商服務人員工作區電腦設備與連線使用規範：

協力廠商服務人員如需使用自行攜入之電腦設備,需由設備

使用人填寫申請單並依申請單所列規範及切結事項逐項填寫，並完成防毒軟體安裝及掃毒檢查後，送交營運管理單位檢核後方能使用。

受委託機構或委外人員執行系統開發維護工作時，其使用之電腦應於開發維護環境進行。並依其使用範圍核予適當之權限。

協力廠商服務人如需使用網路連線、網域帳號或其他系統使用權限， 需填寫申請單並交由營運管理單位核定後，依給定之網路埠、IP 位址及協力廠商人員專用帳號進行設定使用。

網路連線之使用申請，需註明使用起訖時間，每次以使用三個月為限，繼續使用須重新申請並更改密碼。

自備合法使用軟體，使用電腦設備應安裝防毒軟體。

駐點辦公期間依規範申請臨時識別證，人員變更應另行申請，以維護人員識別正確性，落實執行門禁管理；專案完成後，專案負責人應迅速繳回臨時識別證。

駐點辦公使用電腦設備應依規範申請攜出入許可。

專案負責人應負責監控委外駐點人員接觸資料，嚴格禁止使用正式資料，落實個人資料保護。

營運管理單位不定時進行抽查，如有發現未經申請或違反規定之使用情事， 應要求立即停用。

與廠商簽署合約應包含本行資料(含客戶資料)保密及使用合法軟體，並同意本行人員檢查電腦設備資料。

g.廠商進入機房操作系統，須簽立委外廠商保密切結書並遵

守相關事宜。

h.維護廠商抵達後，需先於廠商簽名簿簽到，並立即通知該案負責人。

i.維護廠商如有攜帶文件、設備、工具等物件，需於機房進出管制簿廠商簽名時註明，攜出設備時須填寫資訊設備帶出清單，並告知資訊室該案負責人。

j.維護廠商工作之項目、內容、時間等依維護合約規定進行，如有未盡事宜，依資訊室該案負責人之說明。

k.維護廠商該日(次)之工作需詳細填寫工作單(廠商自備)，經相關單位該案負責人簽名確認後始得離開。

l.維護廠商之工作地點由相關單位該案負責人告知,如有變動需知會資訊室該案負責人，並保持工作地點之整潔，於離開前恢復工作地點之原狀。

m.維護廠商於工作時間與工作地點內，須遵守院內與資訊室相關行政規定(如機房管理辦法)且不可吸煙，吃檳榔，喧嘩等。

n.維護廠商之工作時間需配合本院之上班時間，如非上班時間，請註明

o.原因並經相關單位該案負責人與值班人員確認簽字。

p.維護廠商離開時，需於廠商簽名簿簽退，並通知資訊室該案負責人或值班人員。原攜帶文件、設備、工具等物件，請資訊室該案負責人或值班人員確認無誤後攜回。

q.如須使用本單位之相關設備時，需填寫設備借用單並完成借用手續。維護工作完成後，依歸還手續完成設備歸還。

借用人應善盡保管之責，若有損壞，維護廠商需負賠償之責。

r.使用本院或資訊室之文具、紙張、電話、傳真、電子郵件等耗材與通訊設備時，須遵守院內與資訊室相關行政規定。

s.維護期間所取得之任何本院或資訊室之檔與資訊，不得以任何方式洩漏予不相關之人員或第三者，維護廠商有善盡保密之責。

(六)安全檢測要求

為有效瞭解及管理行動應用 App 之安全弱點，須定期行動應用 App 進行安全檢測，如：行動應用 App 安全檢測、滲透測試或弱點掃描..等，並產生檢測評估報告，列舉所發現的安全弱點並描述對行動應用 App 安全影響程度，而負責開發行動應用 App 之單位應針對弱點項目擬定改善方式，降低弱點被利用進行攻擊 App 的可能性。

1.行動應用 App 安全檢測

(1)基本資安檢測基準

資安技術人員應依經濟部工業局之「行動應用 App 基本資安檢測基準」對 4G 應用服務系統行動應用 App 進行安全檢測。「行動應用 App 基本資安檢測基準」之檢測項目係依據「行動應用 App 基本資安規範」之「4.技術要求」資訊安全技術要求事項內容，其檢測基準項目分為檢測項目及參考項目兩類，檢測項目為必要符合之項目，行動應用 APP 符合檢測基準之檢測項目，代表使用者在未破解行動應用裝置之作業系統層保護時（如：root、jailbreak），行動應用 APP 具有基本資安水準，檢測項目詳見「行動應用程式基本資安檢測基準」；參考項目因下列原因，故不要求進行實際檢測，僅供參考，如下:

A.與品質有關，未直接影響行動應用程式安全性。

B.因檢測所需時間、複雜度或目前尚無通用檢測方法，造成檢測難以執行或重複檢測時結果不一致。

C.僅供開發者參考，非實際執行檢測之項目。

「行動應用 App 基本資安規範」為針對行動應用 App 之屬性分類，訂定各分類之安全要求項目，分為三類：第一類為純功能性，第二類為具認證功能、具連網行為，第三類為具交易功能（包含認證、連網行為）;「基本資安檢測基準」為針對行動應用 App 之功能性對安全要求程度，訂定檢測安全等級，再依其檢測安全等級訂定檢測項目，檢測安全等級分為三個等級，分級如下:

表8　檢測安全等級

檢測安全等級	檢測內容
初級	主要檢測無連網之基礎功能安全性，檢測方式可採自動化工具檢測，並輔以適當之人工檢測，或純人工檢測；
中級	主要檢測連網及認證安全性，檢測方式採人工檢測方式為主
高級	主要檢測付費資源安全性，檢測方式採人工檢測方式為主

資料來源：本計畫整理

資安技術人員應將行動應用 App 依據「行動應用 App 基本資安規範」進行分類，若為第一類純功能性行動應用程式可送測初級（含）以上之安全檢測，若為第二類具認證功能與連網行為行動應用程式可送測中級（含）以上之安全檢測，若為第三類具交易功能行動應用程式須送測高級之安全檢測，當行動應用 App 通過其所屬安全等級之要檢測項目後，即表

示 App 具備該安全等級之基本安全技術要求。有關行動應用程式分類與檢測基準安全等級之對應表格如下：

表9　行動應用程式規範分類與基準分級檢測對應表

檢測基準安全等級 / 行動應用程式分類	初級檢測功能相關之安全性	中級檢測連網及認證安全性	高級檢測交易相關之安全性
第一類 純功能性	★	V	V
第二類 具認證功能與連網行為	—	★	V
第三類 具交易功能（包含認證、連網行為）	—	—	★
★代表為必要送測之檢測等級，V 為可自由選擇通過之檢測等級			

資料來源：本計畫整理

資安技術人員應針對每一檢測項目，訂定其檢測編號、檢測項目、檢測分級、檢測依據、技術要求、檢測基準及檢測結果等欄位，且應依照行動應用程式安全訂定基本資安檢測基準的五大面向:行動應用程式發布安全、敏感性資料保護、付費資源控管安全、行動應用程式使用者身分認證、授權與連線管理安全及行動應用程式碼安全進行檢測，其五大面向說明如下:

A.行動應用程式發布安全

主要適用於發布行動應用程式之相關資訊安全檢測基準，包括發布、更新與問題回報等。

a.行動應用程式發布

b.資安技術人員應針對「行動應用程式發布」之檢測項目進行檢測，須於「行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途」之中級檢測結果為「符合要求」，始符合資訊安全技術要求事項；否則未符合。

c.行動應用程式的來源

d.行動應用程式應於可信任來源之行動應用程式商店發布。

e.行動應用程式發布說明

f.行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。

g.行動應用程式更新

行動應用程式應於可信任來源之行動應用程式商店發布更新

行動應用程式應提供更新機制

h.行動應用程式應於安全性更新時主動公告

i.行動應用程式安全性問題回報

資安技術人員針對「行動應用程式安全性問題回報」之檢測項目進行檢測，於「行動應用程式開發者應提供回報安全性問題之管道」之中級檢測結果為「符合要求」，始符合資訊安全技術要求事項；否則未符合。

j.動應用程式問題回報

行動應用程式開發者應提供回報安全性問題之管道，如聯

絡網頁、電子郵件、電話或其他類型聯絡方式。

行動應用程式開發者應於適當期間內回覆問題並改善

B.敏感性資料保護

主要適用於敏感性資料與個人資料保護之相關資訊安全檢測基準，包括敏感性資料蒐集、利用、儲存、傳輸、分享及刪除等。

a.敏感性資料蒐集

資安技術人員應針對「敏感性資料蒐集」之檢測項目進行檢測，須於「行動應用程式應於蒐集敏感性資料前，取得使用者同意」、「行動應用程式應提供使用者拒絕蒐集敏感性資料之權利」之中級檢測結果為「符合要求」，始符合資訊安全技術要求事項；否則未符合。

b.行動應用程式敏感性資料蒐集聲明

行動應用程式應於蒐集敏感性資料前，取得使用者同意。

行動應用程式提供使用者拒絕敏感性資料蒐集機制

行動應用程式應提供使用者拒絕蒐集敏感性資料之權利，並在使用者拒絕蒐集之情況下，不得仍蒐集該使用者之敏感性資料。

c.敏感性資料利用(參考項目)

行動應用程式應於使用敏感性資料前，取得使用者同意

行動應用程式應提供使用者拒絕使用敏感性資料之權利

行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼

行動應用程式應提醒使用者定期更改通行碼

d.敏感性資料儲存

資安技術人員應針對「敏感性資料儲存」之檢測項目進行檢測，須於「行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中」、「敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存」、「敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取」、「敏感性資料應避免出現於行動應用程式之程式碼」之初級檢測結果為「符合要求」；於「行動應用程式應於儲存敏感性資料前，取得使用者同意」、「行動應用程式應提供使用者拒絕儲存敏感性資料之權利」之中級檢測結果為「符合要求」，始符合資訊安全技術要求事項；否則未符合。

e.行動應用程式敏感性資料儲存聲明

行動應用程在儲存敏感性資料前，應於可信任之應用程式商店或行動應用程式內聲明，並取得使用者同意

f.行動應用程式提供使用者拒絕敏感性資料儲存機制

行動應用程式應提供使用者拒絕儲存敏感性資料之權利，且使用者拒絕敏感性資料儲存的情況下，行動應用程式不得將敏感性資料儲存於行動裝置。

g.行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途。

h.行動應用程式敏感性資料儲存限制

i.行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔

中。

j.行動應用程式敏感性資料儲存保護

敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存，如金鑰有效長度應為 128 位元以上之先進加密標準（AES）且行動應用程式應採用三重資料加密演算法 Triple DES）。

k.行動應用程式敏感性資料儲存控管

l.敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。

m.行動應用程式敏感性資料硬碼（Hard Code）

n.敏感性資料(如密碼、身分驗證資訊或對稱式加解密演算法之金鑰)應避免出現於行動應用程式之程式碼

o.敏感性資料傳輸

資安技術人員應針對「敏感性資料傳輸」之檢測項目進行檢測，於「行動應用程式透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。」之中級檢測結果為「符合」，始符合資訊安全技術要求事項；否則未符合。

行動應用程式敏感性資料傳輸

行動應用程式透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密，如採用 TLS 1.1（含）以上版本加密協定、採用金鑰有效長度為 2048 位元（含）以上之 RSA 加密演算法或採用金鑰有效長度為 224 位元（含）以上之橢圓曲線加密演算法（Elliptic Curve

Cryptography）。

p.敏感性資料分享

資安技術人員應針對「敏感性資料分享」之檢測項目進行檢測，於「行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意」、「行動應用程式應提供使用者拒絕分享敏感性資料之權利」、「行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取」之中級檢測結果為「符合要求」，始符合資訊安全技術要求事項；否則未符合。

行動應用程式敏感性資料分享聲明

行動裝置內於不同行動應用程式間，在分享敏感性資料前，應於行動應用程式內或可信任之應用程式商店聲明，並取得使用者同意。

行動應用程式提供使用者拒絕敏感性資料分享機制

行動應用程式應提供使用者拒絕分享敏感性資料之權利，且使用者拒絕後行動應用程式不得有分享敏感性資料之行為。

行動應用程式敏感性資料分享權限控管

行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取。

敏感性資料刪除

行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能

C.付費資源控管安全

本面向主要適用於付費資源控管之相關資訊安全檢測基準，包括付費資源之使用與控管等。

a.付費資源使用

資安技術人員應針對「付費資源使用」之檢測項目進行檢測，須於「行動應用程式應於使用付費資源前主動通知使用者」、「行動應用程式應提供使用者拒絕使用付費資源之權利」之高級檢測結果皆為「符合」，始符合本資訊安全技術要求事項；否則未符合。

行動應用程式付費資源使用聲明

行動應用程式應於使用付費資源前主動通知使用者，其內容應包含付費資源名稱、數量、金額及付費方式。

行動應用程式拒絕付費資源使用機制

行動應用程式應提供使用者拒絕使用付費資源之權利，且使用者已拒絕付費時，不得有付費行為。

b.付費資源控管

資安技術人員應針對「付費資源控管」之檢測項目進行檢測，須於「行動應用程式應於使用付費資源前進行使用者認證」、「行動應用程式應記錄使用之付費資源與時間」之高級檢測結果須為「符合要求」，始符合資訊安全技術要求事項；否則未符合。

行動應用程式付費資源使用者認證

行動應用程式應於使用付費資源前進行使用者身分認證

行動應用程式付費資源紀錄

行動應用程式應記錄使用之付費資源與時間，包含付費資源名稱、付費時間及付費金額之記錄。

D.身分認證、授權與連線管理安全

主要適用於行動應用程式身分認證、授權與連線管理之相關資訊安全檢測基準，包括使用者身分認證與授權及連線管理機制等。

使用者身分認證與授權

資安技術人員應針對「使用者身分認證與授權」之檢測項目進行檢測，須於「行動應用程式應有適當之身分認證機制，確認使用者身分」、「行動應用程式應依使用者身分授權」之中級檢測結果為「符合要求」，始符合本資訊安全技術要求事項；否則未符合。

行動應用程式使用者身分認證機制

行動應用程式應有適當之身分認證機制，確認使用者身分。

行動應用程式使用者身分授權

行動應用程式應依使用者身分授權。

連線管理機制

資安技術人員應針對「連線管理機制」之檢測項目進行檢測，須於「行動應用程式應避免使用具有規則性之交談識別碼」、「行動應用程式應確認伺服器憑證之有效性」、「行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發」、「行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料」之中級檢測結果為「符

合要求」，始符合資訊安全技術要求事項；否則未符合。

行動應用程式交談識別碼規則性

行動應用程式應避免使用具有規則性之交談識別碼，其交談識別碼特性如下:

採用長度為 128 位元（含）以上之交談識別碼。

交談識別碼與時間、使用者提交資料、具規則性之數字或字串無直接關聯或難以偽造。

交談識別碼應具備登出失效機制。

行動應用程式伺服器憑證有效性

行動應用程式應確認伺服器憑證仍於有效期間內、未被註銷（Revoke），且憑證之主體名稱與主體別名包含連線之伺服器網功能變數名稱稱，此外行動應用程式應使用憑證綁定（Certificate Pinning）方式驗證，以確保連線之伺服器為行動應用程式開發者所指定。

行動應用程式伺服器憑證簽發來源

行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發。

行動應用程式連線安全

行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸敏感資料。

E.行動應用程式碼安全

主要適用於行動應用 APP 開發之相關資訊安全檢測基準，包括防範惡意程式碼與避免資訊安全性漏洞、行動應用 APP 完

整性、函式庫引用安全與使用者輸入驗證等。

a.防範惡意程式碼與避免資訊安全性漏洞

b.資安技術人員應針對「防範惡意程式碼與避免資訊安全性漏洞」之檢測項目進行檢測，須於「行動應用程式應避免含有惡意程式碼」之初級檢測結果為「符合要求」，於「行動應用程式應避免資訊安全性漏洞」之中級檢測結果為「符合要求」始符合本資訊安全技術要求事項；否則未符合。

行動應用程式惡意程式碼

行動應用程式應避免含有惡意程式碼，以符合蒐集敏感性資料前，取得使用者同意、敏感性資料儲存聲明、敏感性資料分享聲明、使用付費資源前主動通知使用者之技術要求，且不得對其他行動應用程式或行動作業系統之檔案，在未授權情況下，嘗試進行查詢、新增、修改、刪除、存取遠端服務及提權等行為。

行動應用程式資訊安全性漏洞

行動應用程式為避免產生資訊安全性漏洞，應採取下列措施

應避免將敏感性資料儲存於暫存檔或紀錄檔中

針對敏感性資料儲存與傳輸應使用適當且有效之金鑰長度與加密演算法進行安全加密

分享敏感資料應避免未授權之行動應用程式存取

應有適當之身分認證機制，確認使用者身分

應避免與未具有效憑證之伺服器，進行連線與傳輸資料

函式庫引用安全

應針對使用者輸入之字串，進行安全檢查

應有相關注入攻擊防護機制

不得存在已知安全性漏洞

c.行動應用程式完整性

d.行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性。

e.函式庫引用安全

f.資安技術人員應針對「函式庫引用安全」之檢測項目進行檢測，須於「行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本」之中級檢測結果為「符合要求」，始符合本資訊安全技術要求事項；否則未符合。

行動應用程式函式庫引用安全

行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，且不得存在已知安全性漏洞。

g.使用者輸入驗證

資安技術人員應針對「使用者輸入驗證」之檢測項目進行檢測，須於「行動應用程式應針對使用者輸入之字串，進行安全檢查」之初級檢測結果為「符合要求」，於「行動應用程式應提供相關注入攻擊防護機制」之中級檢測結果為「符合要求」，始符合本資訊安全技術要求事項；否則未符合。

行動應用程式使用者輸入檢查

行動應用程式應針對使用者輸入之字串，進行安全檢查，如字串驗證型別以及字串驗證長度。

行動應用程式注入攻擊防護機制

行動應用程式應防護使用者注入相關攻擊機制，如下

防護輸入 SQL Injection 字串

防護輸入 JavaScript Injection 字串

防護輸入 Command Injection 字串

防護輸入 Local File Inclusion 字串

防護輸入 XML Injection 字串

防護輸入 Format String Injection 字串

防護輸入 Intent Injection 字串

(2)檢測方式

資安技術人員在未取得原始碼情況下進行測試，初級檢測以自動化工具進行檢測，中級、高級檢測以自動化工具及人工方式檢測，並進行逆向工程取得程式碼後檢測，使用原始碼掃描工具進行掃描並搭配人工分析。針對各級檢測使用之方式進行說明。

A.自動化（Automatic）檢測

初級檢測採用自動化方式進行檢測，檢測方式之類型主要包含:

a.使用者介面導向：以使用者操作介面為主進行自動化測試，包含自動化進行使用者之操作、畫面截圖等功能。在

測試中可運用此類工具建構測試個案

b.資料導向：能夠自動識別測試標的資料欄位或標籤，傳遞或填入不同的資料，並經由追蹤資料流向及回應結果，判斷可能存在之安全問題。

B.人工（Manual）檢測

中級、高級檢測主要以人工方式進行手動檢測，檢測過程中採靜態分析與動態分析混合使用，並可依實際之檢測需求，使用逆向工程或以中間人(man-in-the-middle)攻擊方式進行。

a.靜態分析（Static Analysis）

靜態分析透過手動或工具對可執行碼進行逆向工程取得程式碼，藉由欲存取之敏感性資料、行動裝置資源，例如：行動應用程式中的 AndroidManifest.xml、iOS Entitlements、WMAppManifest.xml 等檔案，檢查所要求之權限是否如「附錄二、行動應用 App 基本資安檢測資料調查表」所述；檢查測試標的所引用的函式庫版本是否存在常見弱點與漏洞，或是否有引用不當的函式庫，例如：引用存在已知漏洞版本的函式庫之瀏覽器行動應用程式訪問惡意網站時，惡意的網站可能造成敏感性資料外洩；檢查敏感性資料是否採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存；檢查逆向工程後之程式碼是否出現可識別之敏感性資料;檢查是否將敏感性資料儲存於暫存檔或紀錄檔中等方法，確認存在的安全性漏洞或問題。

b.動態分析（Dynamic Analysis）

動態分析在測試標的執行階段中引入動態的使用者輸入或資料、參數的傳入等應用程式行為，以分析測試標的執行

階段的各項行為或狀態。動態分析可檢測測試標的在模擬器、實體設備及遠端連線、網路存取狀態、資料傳遞等不同的行為，可應用於檢查敏感性資料傳輸與儲存，是否使用適當且有效之金鑰長度與加密演算法進行安全加密，例如使用封包側錄、檢查系統 Log 等方式，於程式執行中，查看是否存在可識別之敏感性資料；檢查是否將敏感性資料應儲存於受作業系統保護之區域，例如：程式執行後，檢查 SD 卡或可共同存取區域是否存在可識別之敏感性資料。

C.程式碼分析（Code Analysis）

中級、高級檢測以逆向工程取得之程式碼進行分析，分析方式可採原始碼掃描工具進行掃描後搭配人工分析掃描結果。

D.執行碼分析（Binary Code Analysis）

除上述檢測方式外，還可搭配其他檢測或分析方法如執行碼分析。執行碼（binary code）可分為仲介碼（byte-code）及機器碼（machine code）。依不同類型之可執行碼分析，應採用適當之虛擬機器、實體設備進行手動或自動化工具檢測。

(3)檢測結果與產出

檢測結果產出，應包含在測試過程中的所有紀錄與結果，並應依所有檢測項目判定標準說明測試標的檢測結果為「符合要求或不符合要求」檢測結果與產出應包含但不限於：

A.檢測標的

B.檢測範圍之宣告

C.檢測時程

D.檢測方式、環境與使用之工具

E.檢測執行人員與負責之項目

F.測試項目為「符合要求或不符合要求」之判定

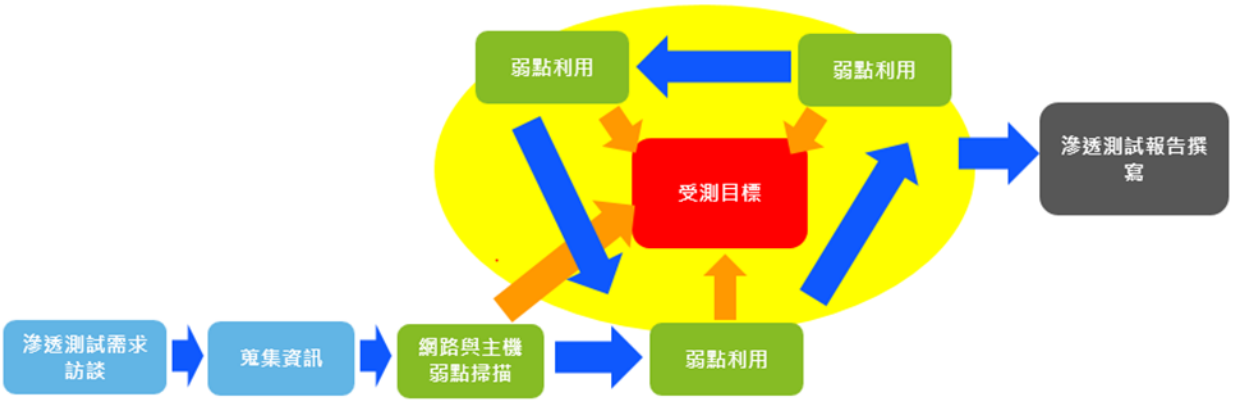
G.測試過程紀錄及佐證資料，不符合要求之檢測項目應於報告中提供

2.應用系統滲透測試

資安技術人員應定期針對 4G 應用服務系統網站進行滲透測試，並可參考目前於國際間具公信力及參考價值的滲透測試文件，如 OWASP 測是指引、ISECOM （the Institute for Security and Open Methodologies）的開放原始碼安全測試方法手冊、SANS 的滲透測試相關文件。

滲透測試的目的是透過一個惡意攻擊者的角度來評估 4G 應用服務系統網站，利用技術和非技術的漏洞，找出資安防護機制存在的弱點或安全問題，以確定對網站可能造成的影響，並於檢測作業完畢後提供完整的評估報告及修補建議。

滲透測試的主要階段為：「需求訪談」、「資訊蒐集」、「網路與主機掃描(弱點掃描)」、「弱點利用」、「滲透測試報告撰寫」。資安技術人員應就以下各階段進行 4G 應用服務系統網站滲透測試作業。



資料來源：本計畫整理

圖6　滲透測試的基本流程

(1)需求訪談

滲透測試需求訪談的主要目的如下

A.討論並確認測試範圍

資訊技術人員執行滲透測試前為避免測試範圍變動，需明確定義滲透測試範圍。4G 應用服務系統網站需包含特定網域、IP 區段、主機、特定應用程式等，透過限制執行範圍目的在於保護網站內有價值性或敏感性的資料。資安技術人員進行滲透測試時可參考下列測試項目範例測試 4G 應用服務系統網站是否有存弱點。

表10　測試項目範例

類型	測試類別	測試項目
網站服務	設定管理	至少包含： 應用程式設定測試 檔案類型處理測試 網站爬行測試

類型	測試類別	測試項目
		後端管理介面測試 HTTP/HTTPS 協定測試
	使用者驗證	至少包含： 使用者帳號列舉測試 測試機敏資料是否透過加密通道進行傳輸
	連線管理	至少包含： Session 管理測試 Cookie 屬性測試 Session 資料更新測試 Session 變數傳遞測試 CSRF 測試
	使用者授權	至少包含： 目錄跨越測試 網站授權機制測試 權限控管機制測試
	邏輯漏洞	至少包含： 網站功能測試 網站功能設計缺失測試 附件上傳測試

類型	測試類別	測試項目
	輸入驗證	至少包含： XSS 漏洞測試 SQL Injection 測試 LDAP Injection 測試 XML Injection 測試 SSI Injection 測試 XPath Injection 測試 Code Injection 測試 OS Commanding 測試 偽造 HTTP 協定測試
	Web Service	至少包含： WSDL 測試 XML 架構測試 XML 內容測試 XML 參數傳遞測試
	Ajax	至少包含 Ajax 點測試等項目： 輸入驗證缺失測試 權限控管測試 套件弱點測試

資料來源：本計畫整理

B.確認測試之環境

若是正式營運環境進行 4G 應用服務系統網站滲透測試，則需考量是否會因檢測作業而影響到營運服務。若是測試環境則必須考量其檢測結果是否會與真實的環境有所差異。

C.確認攻擊手法

滲透測試執行期間若需要執行具侵入性質的檢測作業應先經過確認，並於議定之適當時間且具備適當應變措施與風險評估後，資訊技術人員才進行檢測作業，例如能否使用阻斷式服務或是社交工程等攻擊手法。

D.確認是否允許資料下載或刪除

由於檢測的 4G 應用服務系統網站上可能存放機密性或高價值性的資料，故必須確認是否允許對資料進行下載或刪除。

E.確認執行時間和日期

明確規範檢測作業執行日期與時間，包含確認每日可以執行的時間。

F.確認內部相關部門是否知悉

採用告知相關部門的方式其好處是在檢測過程中若可取得其配合，則有助於測試順利進行，例如要求提供所需資訊以減少檢測作業時間，但也必須考量若內部網管人員知曉要進行滲透測試後，為了避免被檢測出安全弱點而暫時性的加強系統及網路的防護性，這種狀況下所得到的檢測結果未必與平時的運作情況相符。若選擇不告知相關部門則可以測試其對於發現網路攻擊與防護的相關能力，但資安技術人員須考量是否會有營運的風險。

G.確認是由外部還是內部執行

外部滲透測試是由資安技術人員直接在網際網路上進行，內部則於組織內部網路進行。

H.制定溝通原則及時機

雙方需具備暢通的聯絡管道,當 4G 應用服務系統網站在過程中發生問題或發現遭到入侵的足跡等事件，需要能夠即時聯絡到相關人員，並中止測試。另外，需建立安全的資訊交換管道，例如測試過程的相關資訊提供、測試結果報告的提供等，皆需透過安全管道交換以確保機密性。最後應定期討論執行進度，以確保雙方都能掌握目前的執行情況進度，並說明是否有發生重大的問題。

I.撰寫執行計劃書

開始執行之前，將訪談階段的所有結論都寫進計畫書。受測單位主管與資安技術團隊主管需要簽署這份檔，必要時包含參與人員也需簽署。

(2)資訊蒐集

此階段已正式開始執行滲透測試。資訊蒐集是滲透測試的必要步驟。

A.滲透測試分類

滲透測試進行方式依照所提供的資訊多寡可分為以下三類：

a.黑箱測試

黑箱測試是完全不提供任何資訊，或是僅告知受測目標的網址，其餘一切有賴資安技術團隊發揮其能力及創意來進行資訊蒐集。

b.白箱測試

白箱測試會提供完整網路的相關資訊，目的在加速檢測作業的進行,以求盡可能利用一切資訊找出 4G 應用服務系統

網站的弱點，同時也比較小的機會讓 4G 應用服務系統網站遭到破壞。而由於這些資訊有其敏感性及機密性，故通常是由組織內部人員執行檢測作業時才會使用的方式。

c.灰箱測試

灰箱測試是指介於黑箱與白箱之間的測試方法，對於不是完全清楚 4G 應用服務系統網站的資訊，無法主動提供完整的訊息，僅能提供少部分資訊給資安技術團隊，其餘資訊仍需要資安技術團隊進行蒐集。

(3)網路與主機掃描

此階段的目標主要在於資安技術人員使用網路足跡追蹤的結果來探索正在進行活動的 4G 應用服務系統網站，進行弱點識別，找出可能的弱點，以增加其後漏洞利用成功的機率。透過與網站互動，包含採用連接埠掃描(Port Scanning)、作業系統與服務偵測、網路流量分析等活動，試圖取得網站的相關資訊，例如開啟的連接埠列表、使用的作業系統、開放的服務、網路應用程式名稱與版本，並利用針對這些訊息查詢是否存在已知的弱點可進一步加以利用。

(4)弱點利用

此階段為資安技術人員實際利用前面階段所發現的弱點，嘗試取得 4G 應用服務系統網站的權限。為證明弱點可以實際造成威脅及取得權限後進行更深入的滲透測試。但由於實際利用弱點時，可能情況將造成網站無法回應或當機，故應根據這些漏洞發現規劃相對應的弱點利用情境，應經網站管理者同意後再執行。如果有需要的話，甚至可以截取測試過程中的封包內容以供後續追蹤使用。

(5)滲透測試報告撰寫

滲透測試最後一個階段是針對已經完成的滲透測試活動進行總整理，並產出一個報告向 4G 應用服務系統網站管理者進行說明，資安技術人員依據測試過程中所顯示的安全事件進行統整，並分析其潛在風險的嚴重性，並以淺顯易懂的方式呈現出來。同時在必要的情況下也可能會需要提供原始的評估資料(例如封包流量等)，作為管理者後續的分析或證據使用。

3.應用系統弱點掃描

為避免 4G 應用服務系統因為自身弱點成為駭客攻擊對象，資安技術人員須定期對 4G 應用服務系統伺服器進行弱點掃描，並於弱點掃描報告說明所發現的弱點對系統帶來的影響以及建議改善的方式。

(1)定期掃描

資安技術人員應定期執行 4G 應用服務系統伺服器弱點掃瞄，評估是否應採取適當的管控措施，以處理所面臨之風險。

(2)弱點控管

若 4G 應用服務系統主機存在之弱點需採取管控措施，應經過適當的評估並留下相關紀錄。

(3)修補弱點

修補系統主機所存在之弱點時，應優先修補高風險(含)以上的弱點。經評估若有無法修補之高風險項目，應提出補償性措施來控制風險，避免該高風險項目成為駭客攻擊目標。

(4)選定弱點掃描工具

使用弱點掃描工具應確認工具本身的版本及弱點資料庫是否為

最新，避免使用到過期的資料庫進行掃描，使得產出的掃描結果失真。

(5)撰寫弱點掃描報告

當弱點掃描完成後，應將產出的結果於報告中呈現，其報告內容應包含目標基本資訊、執行時間、工具的版本、工具的弱點資料庫版本、弱點風險等級、弱點說明及改善建議。

二、事中應變機制

(一)資訊安全事件管理

以委外方式辦理個人資料或機敏性檔案銷毀或刪除作業時，應要求協力廠商委外廠商執行銷毀或身除作業後，檢附個資或機敏性資料檔案已實際被銷毀或刪除之證明文件或檔案，如：執行前的資料或檔案照片，以及執行銷毀中的資料檔案照片，或者資料銷毀或刪除執行的影片，除留存紀錄證明資料已按照標準流程進行銷毀或刪除以供備查外，同時也能監督協力廠商委外廠商是否有依照合約內容履行其所應交付的服務。

1.事故之定義、目的、範圍、角色、責任、管理承諾、與各機關間之協調及符合性。

2.制訂相關程式，並促進事故應變政策及各項控制措施之實作。

3.應定期審查事故應變政策及事故應變程式等相關檔，確保制度之合適性及程式之完整性。

(1)資訊安全事件定義

凡於作業環境中，因下列事項導致資訊資產之機密性、完整性、可用性遭受影響，足以危害內部運作與權益之事件。

A.內部資安事件：發現（或疑似）遭內部人為惡意破壞毀損、

作業不慎等事件。

B.外力入侵事件：發現（或疑似）電腦病毒感染、駭客攻擊（或非法入侵）等事件。

C. 天然災害：颱風、水災、地震、雷擊等。

D. 突發事件：火災、爆炸、重大建築災害、電力中斷及資訊網路骨幹（主幹寬頻）中斷事件等。

(2)事故應變之角色權責

資訊安全事件管理應制定相關權責，將管理機制流程化，確保職權獨立性分工及事件之可追蹤性。主要可劃分成下列幾種腳色權責：

A.事件發生單位

B.通報受理視窗

C.相關系統或業務負責人

D.相關系統或業務負責單位主管

表11 事故應變之角色權責

角色	權責	
事件發生單位	通報	若發生疑似資訊安全事件，事件發生單位應主動通報受理視窗，並協助確認、排除資訊安全事件。
通報受理視窗	受理、通知相關人等	通報受理視窗於受理事件通報時，應研判是否為資訊安全事件，並轉知相關系統或業務負責人處理。

角色	權責	
相關系統或業務負責人	處理、回報結果	相關系統或業務負責人為資訊安全事件之第一線處理人員，應回報資訊安全事件之發展與處理情況至單位主管，並於各級資訊安全事件之規定時限內排除及解決異常狀況。
相關系統或業務負責人主管	分析、追蹤	相關系統或業務負責單位主管應評估事件等級並研判資訊安全事件影響範圍與程度，追蹤資訊安全事件之發展與處理情況。

資料來源：本計畫整理

(3)事故通報程式

A.事件發生單位發現疑似資訊安全事件時應即時聯繫通報受理視窗，並填寫相關程式表單交由通報相關窗口處理。

B.通報受理視窗在接獲資訊安全事件通報後，應通報相關系統或業務負責人。相關系統或業務負責人應立即進行回應與處理，並將事件發展與處理情況回覆通報受理視窗。若研判無法於時限內處理完成者，應立即通報直屬主管。

C.相關系統或業務負責人應立即進行回應與處理，並將事件發展與處理情況回覆通報受理視窗。若研判無法於時限內處理完成者，應立即通報直屬主管。

D.相關系統或業務負責單位主管，負責評估事件等級並研判事件影響範圍與程度，若事件影響範圍廣泛或情節嚴重者，如嚴重影響營運等級資訊安全事件，立即通報高層主管。

E.若事件影響範圍廣泛或情節嚴重者，如嚴重影響營運等級資訊安全事件，相關系統或業務負責單位主管應立即通報資安事件相關權責主管，由其召集相關人員，協調緊急應變處理事宜。

F.應依據事件評估之結果,建請資訊安全權責主管決定是否啟動「資訊作業營運持續計畫」,若需通知其他內、外部單位，則可由資安事件相關權責人員決議後通知。

(4)事故處理

系統或業務負責人為資訊安全事件之處理人員，於接獲資訊安全事件通報後，應依相關作業規定立即進行處理，並應向權責主管與資訊安全事件通報受理視窗回報資訊安全事件之處理狀況與進度，以及填寫相關表單針對事件發生起訖時間、設備資

料、受影響系統及損失評估與處理過程等事件發生始末。系統或業務負責人之權責主管應協助並督導系統或業務負責人處理資訊安全事件。

A.資訊安全事件之處理階段

資訊安全事件之處理應包含抑制、消除及回復等三階段。

a.抑制係指降低資訊安全事件所造成之危害與損失，如隔離中毒之設備。

b.消除係指移除資訊安全事件對資訊資產所造成之威脅，如清除病毒、切換至備援線路。

c.回復係指將受資訊安全事件所影響之資訊資產回復至正常狀況，如系統回復、重新連結網路等。處理資訊安全事件時，應辨識資訊安全事件之發生來源，並考慮根除資訊安全事件因素及回復資訊資產。

若資訊安全事件屬資訊系統遭外界侵入或資料處理之破壞，則無論歸屬於何種等級，資訊單位應密切注意資訊安全事件之發展與處理情形，收集相關資料，進行記錄與分析，以作為研擬矯正措施之參考，並適時反應、追蹤進度紀錄，以保持紀錄之完整性，同時應考量證據蒐集和保存，以利後續案件偵辦。

B.資訊安全事件之處理程式

a.營運管理單位應建立資訊安全事件的通報程式及管道，並訂定通報後應採行之行動及措施，以便迅速有效處理資訊安全事件。

b.營運管理單位所有相關人員應隨時注意系統或資訊服務設

施之安全弱點以及可能面臨之威脅，並迅速告知業務負責單位及人員立即處理。

c.營運管理單位全體人員、與營運管理單位有業務往來之廠商及其員工、臨時雇員，對於發生資訊安全事件、資訊系統或資訊服務之弱點、違反資訊安全政策或相關規範或面臨外部之威脅時，應隨時保持警戒並進行通報。

d.營運管理單位元受理視窗接獲(疑似)資訊安全事件通報，於評估資訊安全事件等級並研判影響範圍與程度後，轉知相關系統管理人員處理且依照通報程式進行通報。

e.所有資訊安全事件均應立即通報並留下紀錄，以作為後續進行問題處理、分析事件發生頻率與研擬改善措施之基礎。

f.事件紀錄應包含其發生問題、時間、處理方式、向上通報過程與協調相關單位等資訊。

g.資訊安全事件如涉及法令、法規，須確認處理措施符合相關法令、法規之要求，並於處理過程中留存證據及紀錄。

h.資訊安全事件於緊急應變處理結束後，相關系統或業務負責單位主管應根據相關紀錄，加以適當評估檢討並找出問題癥結後，採取必要之矯正措施並留存相關紀錄。

C.資訊安全事件之處理順序

處理資訊安全事件時，應依資訊安全事件等級排定優先順序。若為緊急變更則應依相關規定辦理。

發生影響營運等級之事件時，資訊安全事件處理相關權責人員應研擬並選擇有效的資訊安全事件處理措施。有效的處理措施應考慮下列因素：

a.業務影響分析：可能會因資安事件造成之內外部影響。

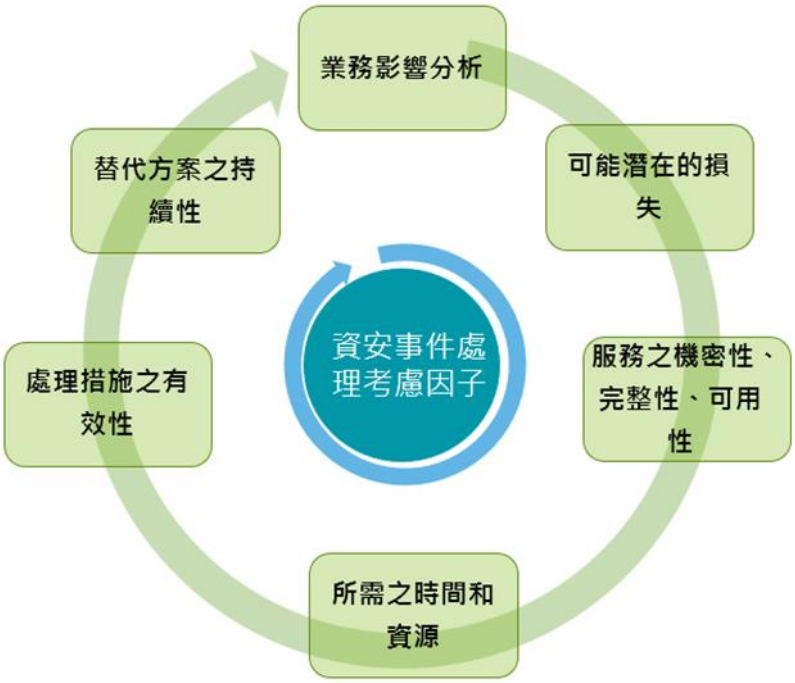
b.可能潛在的損失：因資安事件所波及商譽、營運、人事成本等潛在性的損害。

c.服務之機密性、完整性及可用性：資安事件所影響之資料等相關資訊服務之各層面影響。

d.所需要的時間和資源：當營運受影響時，復原所需之時間及人員及資源等各項彌補措施之安排。

e.處理措施之有效性：彌補措施對於事件處理的有效性。

f.替代方案之持續期間：當正式方案上線前，其代替之方案可維持正常營運狀態的時間。



資料來源：本計畫整理

圖7　資安事件處理考慮因數

D.資訊安全事件之處理方式

a.處理過程自動化

應考慮採用自動化的機制程式支援事故處理過程。如線上事件管理系統。

b.重新組態

可依照現行資訊系統之可行性執行元件動態重新組態，元件動態重新組態包括如：更改路由器規則、存取控制清單、入侵偵測/防禦系統參數、防火牆及閘道器之過濾規則等，做為事故應變功能的一部分。另外，也可考慮潛在需要，執行資訊系統的動態重新組態，例如：阻止攻擊、誤導攻擊者，及隔離系統元件，進而限制違規或被破壞的損壞程度等，縮短回應時間，以解決複雜的網路威脅。

c.持續運作

應識別事故的類別和對應事故類別應採取的回應行動，以確保機關持續的任務和維運功能。

d.資訊關聯

機關應瞭解並彙整各樣資安事故資訊，以強化資安之認知及危機感，以利由全方位的角度看待事故，及作出迅速且有效之回應。如惡意網路攻擊、勒索軟體等威脅事件等。

e.自動關閉資訊系統

如偵測到違反相關安全之規定，應執行可組態的功能來自動關閉資訊系統，避免潛在之威脅。

f.內部人員威脅-特定功能

機關應實作內部人員威脅的事故處理機制，將其內化於內部控制項目中，確保事故處理之即時性及恰當性。

g.內部人員威脅-跨機關協調

應對跨機關之元件或要素之內部人員威脅，提供協調事故處理的機制，包含資訊接收者、資訊擁有者、資訊系統擁有者、人力資源辦公室、採購辦事處、人員及實體安全辦公室、操作人員和風險主管(功能)等。

h.與外部機關關聯

機關應與外部單位進行事故資訊之分享與交流，來達成以全方面的視角來看待事故的認知及執行更有效的事故應變。如可與外部專業資安事件鑑識機構協、資訊安全風險管理之廠商、軍事/聯盟夥伴、客戶和多層次開發商等，以利機關從不同角度瞭解資訊安全事件之起因及趨勢，進而強化機關於資安事件之防禦及回應。

i.動態回應功能

機關應採用動態回應功能，以有效回應安全事故。如強化控制措施描述對安全事故(如惡意網路攻擊期間敵人的行動)更換部署或及時回應的新功能，及在資訊系統層級實作的功能等。

E.資訊安全事件之記錄及追蹤

資訊安全事件皆須留存相關紀錄，應包含下列各項：

a.發生時間：資訊安全事件之處理及追蹤過程應詳實記錄，必要時應留存紀錄或軌跡以利分析。

b.通報及處理單位/人員：資訊安全事件通報受理視窗應蒐集與追蹤系統或業務負責人回報資訊安全事件之處理狀況與進度。

c.資訊安全事件之描述：處理資訊安全事件時，導致影響其他資訊資產之機密性、完整性與可用性，應告知相關資訊資產使用者、保管者及擁有者並留存紀錄。

d.處理經過及結果：資訊安全事件如涉及法規或犯罪部分，須確認處理措施符合法規要求，並注意處理過程中證據留存事宜。資訊安全事件之紀錄，應由相關單位彙整資料並於資安處理會議中報告。

e.回復正常之時間：資訊安全事件之表單、紀錄及報告等檔，由指定單位保管留存。

F.資訊安全事件改善及回饋

a.資訊安全事件回復後，相關單位須審視資安事件通報及處理相關表單，並考量下列措施：

b.重新審視資訊安全管理制度，檢驗是否有不足之處，並建議改善或新增控管措施，由相關權責單位核定後公佈。

c.重新設計控管措施時，應注意控管措施之有效性，如對於事件發生之種類、數量及成本，是否可有效降低。

d.人為因素造成之資訊安全事件，應由各單位權責主管對相關失職人員，再施以適當之教育訓練或召開會議檢討缺失，並視情節重大性予以適當之處分。

e.資訊相關單位應定期彙整資訊安全事件紀錄，定期檢閱資訊安全事件之有無再發生，並考量建構知識庫與監控規則。如同類型之資訊安全事件再發生，應協同相關處理人員重新分析事件發生之根因，以確保矯正措施之有效性。

f.系統或業務負責人之權責主管應對發生頻率較高或投入復原成本較高之資訊安全事件提出改善計畫，陳單位主管核定後，以作為系統提昇或系統規劃之參考。

G.重大事件之矯正措施

事件等級如為嚴重影響營運等級，相關權責單位應將資訊安全事件檔化紀錄後，送交系統或業務負責人填寫發生原因、矯正措施、改善期限及負責人員，簽核後留存備查。

(5)事故監控

可考慮採用自動化機制來協助安全事故的追蹤及事故資訊的收集和分析，如網路監控設備、線上監控的電腦事故應變中心(CIRCs)或事故的其他電子資料庫等，用於追蹤安全事故，以及收集和分析事故資訊的自動化機制。除此之外，也應定期追蹤事故後續發展及確保檔化資訊系統的安全事故。

其中，檔化之資訊系統安全事故報告檔內容需包括以下內容：

A.事故之維護紀錄

B.事故之狀態

C.其他與事故相關之必要資訊，如取證、評估事故的詳細資訊、發展趨勢和處理過程等。

(6)事故應變

A.事故應變計畫

a.機關應擬定事故應變計畫，其內容應包含以下幾點：

b.事故應變相關之組織人員權責。

c.定義可量測可追蹤之事故。

d.提供事故應變功能之方法。

e.提供機關內部的事故應變功能的量測指標。

f.定義能維持和妥善支援事故應變功能的資源和管理機制。

g.相關權責人員所需之教育訓練及技術技能。

事故應變計畫應定期審查，確保其中權責分配之執行力，並將相關權責公告給事故應變人員，使其知曉自身被賦予之責任。機制之有效性以及計劃之合適性也藉由更新事故應變計畫進一步檢視，其相關處理系統或機關的變更及計畫實作、執行或測試過程中遭遇的各樣問題。此外，也能確保事故應變計畫之隱密性，免受未授權的洩露和修改。

B.事故應變協助

機關應提供事故應變支援及資源，整合到機關事故應變功能，提供資訊系統使用者意見及協助，以利安全事故處理及

報告。事故應變支援與資源包括：服務台、援助組和鑑識取證服務等，視事件需求而定。

a.自動支援資訊及支援的可用性

機關應採用自動化機制來提高事故應變相關的通報資訊及支援的可用性。如自動化機制可以提供使用者獲取事故應變協助的推升能力，使用者可以主動到網站查詢相關資訊，或由主管機關以一般分送或有針對性的主動機制發送資訊給使用者，使各機關掌握最新事件資訊。

b.與外部供應商交流

為因應快速變動之外在環境環境及不斷激增之潛在威脅，應考慮與外部單位進行事故資訊之分享與交流，來達成以全方面的視角來看待事故的認知及執行更有效的事故應變。其中之好處如下：

建立事故應變功能和外部供應商資訊系統防護功能間的直接合作關係。

建立與外部供供應商聯合之資訊安全防禦網，委由外部供應商提供機關資訊系統和網路未授權活動的保護、監控、分析、偵測，和回應之協助(如 CIRT 或 SOC 等組織)。

(二)資安事件證據保全

為了保留數位證據的完整性、正確性、一致性及符合性，保留資安事件之證據可由不同角度瞭解事件影響層面，藉而建構出資安事件發生之過程，並作以事後調查及追蹤之有利輔助及依據。就總體而言，數位證據有容易複製、容易修改及不易追溯等特性，因此在數位證據採集及保存上更需小心謹慎，方可顧及證據之完整性及正確性。

電子儲存媒介或系統中所存放的數位證據，主要可分為以下幾種分類：

1.文字資料

2.聲音或影像

3.圖片、符號或其他資料

其中，因數位資料之揮發性，保存數位資料之設備也應被視為蒐集資料之重要證物。 例如：

1.電腦、周邊設備及數位儲存媒體。

2.網路連線設備。

3.監視錄影系統。

4.其他能儲存數位資料之裝置。

數位證據取得要遵循合法、自願、真實的原則，因此當機關發生資安事件之際，需以有效的方式蒐集證據，且於第一時間進行數位證據保全，維持原證據的狀態確保後續件事分析工作能有效進行。

數位證據取得需注意以下原則：

表12 數位證據取得原則

	數位證據取得之原則
1.	為避免爭議，不以未經授權之方式取得證據。
2.	於蒐集證據當下，應確保相關第三公正方於現場一同檢視，避免後續作業產生之誤解及爭議。
3.	證據之蒐集應於事件發生後盡快完成，確保數位證物維持原本狀態。
4.	將證據蒐集及保全之過程留存檔化紀錄。

	數位證據取得之原則
5.	注意數位證據儲存放置之實體環境。
6.	應進行證據備份機制，避免原始證據於採集及保全階段遭到破壞。

資料來源：本計畫整理

1.人員職掌

於數位證據的保全過程中，依照不同角色指派工作可確保過程中之環結辨識，保障證據之原始性及完整性。證據保全程式中主要的角色如下：

(1)現場記錄人員：

於現場狀況協助證據保全人員於證據蒐集及運送的過程中，進行過程之紀錄。

(2)證據保全人員：執行數位證據辨識、採集、封存及運送作業。

2.證據保全準備階段

於環境中正式進行數位證據採集之前，需確保制定流程化之證據保全流程，確保人員之調配及相關事前資料之瞭解，並將此流程與資訊安全管理機制進行整合，確保相對應之應變程式及對應之權責分配，以進行必要之安全防護措施。相關之準備措施如下：

(1)授權之正當性：秉持數位證據取得要遵循合法、自願、真實之原則，確保經授權之相關程式。

(2)人員之合適性：現場記錄人員及證據保全人員除需具備相關之專業性知識與技術，也應接受教育訓練。

(3)環境及事件之確認性：於至現場前預先瞭解事件狀況，以利後續證據採集之方向，必要時也能立即進行現場訪談。

(4)證據蒐集之適切性：確認相關採集及保全作業工具之準備，確保事前工作之預備，避免突發狀況之發生。

資料來源：本計畫整理

圖8　數位證據保全之準備階段

3.證據保全操作階段

證據保全操作階段可依證據採集之程式分為以下幾種階段：

(1)數位證據辨識

A.維護現場完整

a.執行數位鑑識調查作業時，應符合證據監管鏈原則。應避

免異動及改變現場相關原始磁碟及數位證據，以防止破壞其證據能力。

b.數位鑑識人員未抵達現場時，如系統設備處於開機情況下，請勿關機，反之亦然，以避免改變數位證據原始狀態。

c.現場記錄人員應協助管制事件現場，並確保僅經授權之人員進出管制現場。於證據蒐集之現場，現場記錄人員應要求在場人員停止操作作業，確保現場狀況保存之完整性。

d.現場記錄人員也應協助現場秩序之維持，並針對事故相關系統設備週遭附近人員進行現場疏導作業，避免在場人員接觸數位證據，且非相關業務承辦人員在未經授權之狀況下不得進出事故現場。

B.判斷相關之數位證物

現場記錄人員應視現場狀況以靜態或動態之方式，如錄影、拍照或其他適切之方式記錄現場，並注意以下事項：

a.非必要情況下，勿觸碰或移動現場相關證物。

b.將相關數位設備所在位置加以記錄（如電腦系統、周邊設備、筆記型電腦、攜帶式媒體及儲存媒體等），並可考慮以拍照或錄影方式記錄。

c.若要以拍照方式記錄電腦系統及週邊設備，應注意其記錄之照片除擺設位置外，也應包含電腦主機之重要面向（正、背及側面）。光碟片、隨身碟、記憶卡或其他可攜式儲存媒介也應視其類型紀錄其正反面之照片。

d.電腦設備或儲存媒體蒐集：

表13　電腦設備或儲存媒體蒐集注意事項

系統狀態	情境範例	注意事項
系統可關機	營運系統可暫停使用	事故單位應停止使用該系統，並完整保留相關設備，待證據保全人員到場進行相關作業。 如系統有需拆卸之需求，需由現場記錄人員全程錄影記錄，以避免日後之爭議。 若系統有連接其他外接裝置或外接儲存媒體時，應交由專業數位證據保全人員進行封緘作業，並由現場記錄人員全程拍攝拆卸及取出之過程。如需以拍照方式存證，需注意紀錄拆卸前後之對照、線材之連結方式及現場拆卸實況紀錄等，確保證據採集之公正性及一致性。
系統無法關機	伺服主機系統無法中斷服務	應於相關鑑識單位監督下進行資料轉移之作業。 現場記錄人員亦需錄影或拍照存證，並針對資料轉移之儲存媒體之廠牌、容量、序號等相關資訊進行文件化紀錄，待日後比對之用。

資料來源：本計畫整理

C.揮發性資料擷取

為避免部分存在於記憶體之重要資料於資訊設備關機後消失

不見，應考量取得涉及資訊設備之可揮發性資料，如運行中之程式、網路連線狀態或記憶體內容等。

a.可視不同資訊人力資源分配進行揮發性及邏輯性資料擷取。

b.數位證據保全人員應考量資安事故之類型及現場狀況，如涉及事故之相關重要設備處於開機狀態下，若需擷取揮發性資料，需避免儲存於記憶體中之重要資料因系統關機而消失。

c.數位證據保全人員如需擷取邏輯性資料，如作業系統資訊、網路狀態、執行程式資訊、系統 稽核日誌紀錄及使用者上網行為紀錄等，亦需考量資安事故類型及現場狀況後再視需求進行。

d.在專業數位證據保全人員檢視及陪同下，防火牆設備、入侵偵測或防禦設備、紀錄保存與資安事件分析設備、防毒設備、流量控管或網路監控設備、應用系統及資料庫等設備，可視狀況由應用系統或網路管理人員將稽核日誌檔案匯出，由數位證據保全人員對其進行邏輯性資料擷取。

D.證據封緘作業

a.現場記錄人員應於數位證據封緘過程中進行全程錄影記錄。

b.應確實清點現場所蒐集之各項數位證據，並依照其相關之類別進行文件化紀錄。若有相關規範之資訊安全表單編號或事故證據編號，應遵循編號之方式進行之。

c.數位證據應考量其包裝保護措施，避免運送過程中發生碰撞與震動突發狀況。

d.封緘電腦週邊設備時，也應將其完整相關周邊一併進行封緘。

e.數位證據保全人員應注意數位證據之檔化紀錄之保存，相關表單及檔應妥善保存密封，非經許可不可擅自開封。

f.將數位證據攜出前，應妥善點屬是否有缺漏，並清點檔化清單，並留存相關紀錄，以供後續對照之用。

E.證據運送作業

a.數位證據於運送過程中應確保運送環境之安全性及合適性，避免實體環境之幹擾或影響證據之原始狀態，並應進行全程監看作業。

b.證據於運送至其預定地點後應進行交付清點作業，並留存交付日期、時間及收交付人等相關紀錄，確保證據確實交付於相關權責人等。

c.數位鑑識分析作業得委由外部專業鑑識人員，可根據案情之類型及特性，考量聯繫司法機關或外部專業鑑識單位進行後續數位鑑識分析作業之協助。

d.鑑識調查分析作業應以檢驗證據副本/映射檔為原則，切勿直接檢
驗原始數位證據。

三、事後處理機制

(一)資安事件排除後復原、回復及驗證

資安事件發生後應根據事件類別採取相對應之處理措施，辨識資安事件之發生來源進行處理，並考慮根除資安事件因素及回復資訊資產。處理過程應包含抑制、消除及回復等三階段。抑制係指降低資通安全事件所造成之危害與損失，如隔離中毒之設備；消除係指移除資通安全事件對資訊資產所造成之威脅，如清除病毒、切換至備

援線路；回復係指將受資通安全事件所影響之資訊資產回復至正常狀況，如系統回復、重新連結網路等。以確保能於最短時間內使事件相關之任務回復正常運作，其相關紀錄宜至少保存五年。

(二)資安事件發生後之改善及追蹤作業

資安事件之受理通報視窗應蒐集並追蹤系統或業務負責人回報資安事件處理狀況及進度，資安事件之處理及追蹤過程應詳實記錄，必要時應蒐集相關資料或軌跡進行記錄與分析，以作為研擬矯正措施之參考，並適時反應、追蹤進度紀錄，以保持紀錄之完整性，同時應考量證據蒐集與保存，以利後續案件偵辦。

處理資安事件時，若導致影響其他資訊資產之機密性、完整性與可用性，應告知相關資訊資產使用者、保管者及擁有者並留存紀錄。事件如涉及法規或犯罪部分，須確認處理措施符合法規要求，並注意處理過程中證據留存事宜。

1.資安事件應變處理完成後，盡速完成資安事件處理報告

資安事件應變處理完成後，其相關完整紀錄應由資安事件之處理負責單位進行彙整，並依據組織之處理流程進行報告，其相關之表單、紀錄、報告等檔應根據組織規定妥善保管，相關檔宜至少保存五年。

2.事件處理報告應包含下列內容，皆須留存相關紀錄

(1)事件發生簡述

事件發生簡述應至少包含發生時間、通報及處理單位/人員、資安事件之描述。

(2)事件應變過程及時序

事件應變過程及時序應至少包含事件之處理經過及結果、回復

正常之時間

(3)資安事件根因分析

為降低未來類似資安事件重複發生，應進行資安事件之根因分析，徹底瞭解事件之發生原因為何，以利未來達到。

(4)檢討、改善方案與計畫

應依據事件根因分析結果，提出改善方案與計畫，並依計畫進行檢討與改善，如有需要應適時修正相關緊急應變作業程式與控管措施。資安事件若為人為因素造成，應針對相關失職人員，施以適當之教育訓練或召開會議檢討缺失，並視情節重大性予以適當之處分。

3.應定期追蹤實施改善措施的成效

組織應定期彙整資安事件紀錄，定期檢閱資安事件之有無再發生。若同類型之資安事件再發生，應協同相關處理人員重新分析事件發生之根因，以確保改善措施之有效性。

4.應考量建立當次資訊安全事件相關監控規則，以利未來類似事件發生之偵測與處理

組織於事件後應檢討其應變處理過程、結果及影響，並擬訂預防類似事件發生之措施，考量建立資訊安全事件知識庫與相關監控規則，對發生頻率較高或投入復原成本較高之資安事件提出改善計畫，以作為系統提昇或系統規劃之參考，以利於第一時間偵測資安事件之發生並著手即刻處理。

5.應檢視制度規範的完備性及對資訊業務單位提供必要的資安訓練與宣導，並應綜合評估過去發生的資安事件紀錄，歸納發生模式，提出制度規範修改建議

資安事件處理完畢後，應重新審視組織之資訊安全管理制度，檢驗是否有不足之處，並建議改善或新增控管措施。修正相關作業程式、控管措施時，應考量其有效性，如對於事件發生之種類、數量及成本，是否可有效降低。

肆、結論

本指引主要探討 4G 應用服務系統營運之組織管理面、資料管理面、系統管理面、網路管理面與環境管理面及等各項資訊安全問題進行探討，進而歸納各構面於營運上所須遵循之基本資安以及宜參考之進階資安要求，以達到民眾安心使用 4G 應用服務系統，確保資通安全及民眾權利的保障的願景。

考量資訊科技日新月異，為使本參考指引符合資訊安全控管之需求，建議定期編審本指引，以期有效提供 4G 應用服務系統營運管理單位之遵循準則。

伍、參考文獻

[1] Web 應用程式安全參考指引與實作手冊

[2] 安全軟體設計參考指引

[3] 安全軟體測試參考指引

[4] 安全軟體發展流程指引

[5] 行動應用 App 安全開發指引

[6] 行動應用 App 基本資安規範

[7] 行動應用 App 基本資安檢測基準

[8] 加速行動寬頻服務及產業發展方案（104 年－106 年）

[9] The Open Web Application Security Project (OWASP)

[10] The Western Association of Schools and Colleges (WASC)

[11] CWE/SANS Institute