資通系統防護基準檢核表

單位(科/室)		**管理人**		**填表日期**	
系統名稱				**防護需求等級**	**□普□中□高**
建置廠商		**維護廠商**			
版本類別	**□公版 ■機關自用**			**維護合約**	
系統建置方式	**□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他_____**			**□無 □有，至_____為止**	

1.系統環境資訊	
作業系統	■Windows，版本:_2012 R2_____ □Mac OS，版本:_____ □Unix / Linux，版本: _____ □FreeBSD，版本: _____ □其他，作業系統名稱_____，版本:_____ 註：煩請寫出「種類」和「版本號碼」，如 Linux 請寫 CentOS 6.8、RHEL 6.8、Oracle Linux 6.8 或其他，而非只寫 Linux 6.8，以利查出明確漏洞資訊。
程式語言	□C/C++，版本:_____ □C#，版本:_____ □Java，版本:_____ □JavaScript，版本:_____ □Python，版本:_____ □PHP，版本:_____ □Visual Basic .NET，版本: _____ ■其他，語言名稱_ASP.NET___，版本:__4.8_____ 註：煩請填寫詳細版本，如 PHP 請寫 7.3.17 或其他，而非 PHP 7.0。
Web 伺服器	□無 ■有， □Apache HTTP Server，版本:_____ □Apache Tomcat Server，版本:_____ ■Microsoft IIS，版本：_8.0_____

<table>
<tr><td></td><td colspan="2">□Nginx，版本:_____
□其他，伺服器名稱_____，版本:_____
註：煩請填寫詳細版本，如 Tomcat 請寫 7.0.65 或其他，而非 Tomcat 7.0。</td></tr>
<tr><td>資料庫</td><td colspan="2">□無
■有，
□DB2，版本:_____ □Sqlite，版本:_____
□Oracle，版本:_____ ■MySQL，版本:Community Server 8.0.23
□PostgreSQL，版本:_____
□Microsoft Access，版本:_____
□Microsoft SQL Server，版本: _____
□其他，資料庫名稱_____，版本:_____
註：煩請填寫詳細版本，如 Oracle Database 請寫 12.1.0.1，而非僅寫 12。</td></tr>
<tr><td>網站框架</td><td colspan="2">■無
□有，
□Struts，版本:_____ □Spring，版本:_____
□ZK，版本:_____ □django，版本:_____
□.Net Framework，版本: _____
□其他，網站框架名稱_____，版本:_____
註：煩請填寫詳細版本</td></tr>
<tr><td rowspan="7">軟體元件清單</td><td>元件名稱</td><td>版本（煩請填寫詳細版本）</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

2.系統防護評量			
普、中、高級系統適用項目			
類別	安全控制措施	機關規範	機關檢視結果
存取控制	1. 建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。(帳號管理)	作業系統、應用系統、網路及資料庫使用者如需申請及註銷存取權限須填寫「系統使用權限申請／異動單」。	■是，請勾選已具備之程序： ■帳號申請 ■帳號開通 ■帳號停用 ■帳號刪除 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
	2. 對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。(遠端存取)	如有資訊設備連線之需求，須由申請人填寫「遠端連線申請單」，經相關權責主管核准後，執行權限開放。	■是，請勾選實作方式： ■於伺服器端進行權限檢查 ■其他 限制 IP 及連線軟體 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
稽核與可歸責性	3. 依規定時間週期及紀錄留存政策，保留稽核紀錄。(稽核事件)	系統需開啟系統日誌及適當稽核記錄功能，並將關鍵性系統主機之紀錄匯出存檔備查，並保留至少一個月。	■是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
	4. 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資	除預設之系統紀錄功能外，應考量紀錄以下事件：	■是，請勾選實作方式： ■稽核身分驗證事件 ■稽核資料存取事件

	通系統事件。(稽核事件)	(1)系統管理者及具備特殊權限帳號之登入成功及失敗事件紀錄。 (2)使用者帳號異動及對密碼檔案之讀取與變更。 (3)變更正式應用系統的程式原始碼及程式執行碼。 (4)對於作業系統設定檔之存取及變更。	■稽核系統功能錯誤事件 □其他 _____ □否，無稽核功能 □不適用，請說明： _____
	5. 應稽核資通系統管理者帳號所執行之各項功能。(稽核事件)	資通訊設備、應用系統與資料庫之管理者與操作者所有執行的管理或異動作業，應加以記錄。	■是 □否 □不適用，請說明： _____
	6. 資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一的日誌紀錄機制，確保輸出格式的一致性。(稽核紀錄內容)	應針對重要系統，在不影響效能運作下開啟相關日誌包括 (1)事件（成功或失敗）發生的時間。 (2)事件的資訊（如已處置檔案）或失效的資訊（如已發生錯誤並採取矯正措施）。 (3)所涉及的帳號和管理者或操作者。	■是，請勾選實作方式： ■事件類型 ■發生時間 ■發生位置 ■使用者身分識別 □採用單一的日誌紀錄機制 □其他 _____ □否 □不適用，請說明： _____
	7. 依據稽核紀錄儲存需求，配置稽核紀錄所	依據資通訊設備資源使用狀況及資源容量之需	■是 □否

	需之儲存容量。(稽核儲存容量)	求，適時進行系統調整與系統容量擴充規劃，以確保獲得必要之系統作業資源。	□不適用，請說明： _____
	8. 資通系統於稽核處理失效時，應採取適當之行動。(稽核處理失效之回應)	無明確規範	■是，請勾選實作方式： □關閉資訊系統 ■覆寫最舊的稽核紀錄 □停止產生稽核紀錄 □通知管理者進行故障排除 □其他 _____ □否 □不適用，請說明： _____
	9. 資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。(時戳及校時)	資訊設備及主機伺服器應盡可能與單一參考時間源同步。以確保系統時間的一致性。 資訊設備如無法設定單一參考時間源，則應約定同步之時間源，由設備管理員定期(至少每季一次)或於設備異動時進行系統時間同步作業。	■是 □否 □不適用，請說明： _____
	10. 對稽核紀錄之存取管理，僅限於有權限之使用者。(稽核資訊之保護)	各系統的系統紀錄存取，應限定僅由系統管理者或具讀取權限者存取。	■是 □否 □不適用，請說明： _____
營	11. 訂定系統可容忍資料	事故發生後，機房及核	■是，時間為

運持續計畫	損失之時間要求。(系統備份)	心業務資訊系統資料可被回復的最近時間點（參考備份頻率）。	30 天 □否 □不適用，請說明： _____
	12. 執行系統源碼與資料備份。(系統備份)	重要資料應定期備份。規劃備份時應包含系統設定、應用程式、資料庫備份等項目。 (1)資料庫備份:備份作業規劃若為日備份，則至少每週進行完整備份到備份媒體上，除有特殊要求外，此作業每次備份之完整備份至少保留二代。 (2)作業系統備份:單機無備援或無設置 RAID 架構之主機，應採取磁碟鏡像(Mirror)或是磁碟影像檔方式進行作業系統備份。作業系統若有異動，須進行完整資料備份，此作業每次備份之資料保留二代。 (3)應用系統備份: 具有安裝程式之應用系統，須至少備份應用系統之設定檔案。如有異動須對應用系統進行完整資料備份，此作業每次備份之資料保留二代。	■是 □否 □不適用，請說明： _____
識	13. 資通系統應具備唯一	無明確規範，基本上不	■是

別與鑑別	識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。(內部使用者之識別與鑑別)	允許共用帳號	□否，無法識別機關使用者，或允許共用帳號 □不適用，請說明： _____
	14. 使用預設密碼登入系統時，應於登入後要求立即變更。(身分驗證管理)	使用者初次登入電腦系統，應立即變更秘密鑑別資訊。	■是，要求立即變更預設密碼 □否，未要求變更預設密碼 □不適用(如未使用預設密碼)， 請說明：_____
	15. 身分驗證相關資訊不以明文傳輸。(身分驗證管理)	應保護對外服務應用系統之資訊交易(transaction)中涉及之資訊，以防止不完整的傳輸、錯誤選徑（mis-routing），未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。	■是，請勾選實作方式： ■使用 HTTPS 或 SSH 加密 □將身分驗證資訊加密或編碼後傳輸 □其他 _____ □否 □不適用，請說明： _____
	16. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 3 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。(身分驗證管理)	各系統應有設定連續秘密鑑別資訊登入錯誤次數限制，要有錯誤紀錄，必要時得停止該帳號之登入或鎖定該帳號。	■是，具備帳戶鎖定機制 □否 □不適用，請說明： _____

	17. 基於密碼之鑑別資通系統資訊應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(對非內部使用者，可以機關自行規範辦理。) (身分驗證管理)	密碼複雜度: (1)伺服器作業系統需有12個字元（含）以上；個人電腦作業系統及其他系統長度需有8個字元（含）以上。 (2)需有英文字母、數字組成，並儘可能包含英文大小寫字母或其他符號。 (3)避免使用個人公開的資料，如生日、電話號碼及身分證字號等。 (4)避免與帳號、單位名稱或電腦主機名稱相同。 最長效期: 應用系統管理員帳號或高權限帳號密碼至少每六個月變更一次。 使用者每隔六個月須變更密碼。	■是，請勾選實作方式： ■強制密碼複雜度 □強制密碼最短效期 ■強制密碼最長效期 □其他 _____ □否 □不適用，請說明： _____
	18. 使用者更換密碼時，至少不可以與前3次使用過之密碼相同。(對非內部使用者，可以機關自行規範辦理。) (身分驗證管理)	無明確規範	□是 □否 □不適用，請說明： _____
	19. 資通系統應遮蔽鑑別過程中之資訊。(鑑別資訊回饋)	無明確規範	□是，請勾選實作方式： □輸入密碼時顯示*或空白

			□其他 _____ □否 □不適用，請說明： _____
	20. 資訊系統應識別及鑑別非機關使用者(或代表機關使用者行為的程序)。(非內部使用者之識別與鑑別)	程式設計應具備檢驗登入身分識別與秘密鑑別資訊功能，秘密鑑別資訊如採密碼，其保護機制應考慮包含密碼長度限制、密碼組合限制、密碼錯誤次數限制與變更密碼歷史管理，並可將身分驗證之相關紀錄提供其他稽核工具使用。	■是，具備身分驗證機制 □否，未具備身分驗證機制 □不適用，請說明： _____
系統與服務獲得	21. 針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。(需求階段)	無明確規範	□是 □否 ■不適用，請說明： 系統已運行多年，後續如需維護將使用此表單進行確認
	22. 應針對安全需求實作必要控制措施。(開發階段)	系統負責人與委外廠商於系統正式開發前應建立下列系統文件： (1)應用系統需求規格文件 (2)應用系統設計文件 (3)應用系統測試文件	■是 □否 □不適用，請說明： _____
	23. 應注意避免軟體常見漏洞及實作必要控制措施。(開發階段)	留意國內外危機處理中心(TWCERT)宣佈重大安全弱點及廠商發佈之修	■是 □否

		正檔訊息。通知廠商或自行取得修正程式。	□不適用，請說明： _____
	24. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。(開發階段)	應用程式應設計各種例外狀況處理機制，以擷取錯誤資訊，並避免直接顯示原始完整錯誤資訊給予使用者。	■是 □否 □不適用，請說明： _____
	25. 執行弱點掃描安全檢測。 (測試階段)	透過網路存取之系統應執行適當之弱點掃描或滲透測試，弱點掃描或滲透測試應依據系統架構，以確認所開發的系統架構是否存在安全弱點或安全漏洞。	■是 □否 □不適用，請說明： _____
	26. 於部署環境中應針對相關資安威脅，進行更新與修補，並關閉不必要服務及埠口(佈署與維運階段)	與系統安全相關之修正程式應適時進行修補，必要時由廠商於測試後協助安裝；其他額外功能則視實際需求選擇性安裝。 系統上線前應完成必要之漏洞修補作業，相關作業完成後，需重新關閉因修補作業而開放之非必要網路服務。	■是 □否 □不適用，請說明： _____
	27. 資通系統相關軟體，不使用預設密碼。(佈署與維運階段)	無明確規範，基本上無使用預設預碼。	■是，資料庫或 Web 伺服器等軟體元件未使用出廠預設密碼 □否 □不適用，請說明： _____

	28. 資通系統開發若委外服務應將系統發展生命週期各階段依安全等級將安全需求(含機密性、可用性、完整性)納入委外合約。(委外階段)	規劃內容應涵蓋系統安全品質、運作環境及內外部資源使用之安全性，其相關資訊安全規範請參考「資訊作業委外安全管理辦法」辦理。	■是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
	29. 應儲存與管理系統發展生命週期之相關文件。(系統文件)	系統負責人與委外廠商於系統正式開發前應建立下列系統文件: 1. 應用系統需求規格文件 2. 應用系統設計文件 3. 應用系統測試文件 系統文件之管理無明確規範，基本上由系統負責人保管。	■是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
系統與資訊完整性	30. 系統之漏洞修復應測試有效性及潛在影響，並定期更新。(漏洞修復)	關鍵性主機於安裝修正程式前，需先行測試並詳細記錄修正程序，確認系統穩定運作無誤後，方可於正式主機進行修正。	■是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
	31. 發現資通系統有被入侵跡象時，應通報機關特定人員。(資通系統監控)	人員發現有資訊安全可疑事件時，發現人員需向「權責單位」進行資訊安全事件通報。	■是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
中、高級以上系統適用項目			
存取控	32. 已逾期之臨時或緊急帳號應刪除或禁用。	無明確規範，基本上於定期帳號清查時人工檢視並作適當處理。	■是，請勾選實作方式： ■人工審查 □系統自動刪除或禁用

制			□其他 _____ □否 □不適用，請說明： _____
	33. 資通系統閒置帳號應禁用。	無明確規範，基本上無閒置帳號。	□是，請勾選實作方式： □人工審查閒置帳號 □系統自動禁用閒置帳號 □其他 _____ □否 ■不適用，請說明： _無閒置帳號_____
	34. 定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	應每年執行使用者存取權限查核，查閱人員異動資料(到職、調職或離職)，抽檢到職、離職人員之權限申請、註銷或關閉作業紀錄並核對系統中之設定。	■是 □否 □不適用，請說明： _____
	35. 採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。	資訊存取權限之設定以工作所需之最小權限與最少資訊為原則，並由權責主管依據員工的工作職責或作業性質指派權限。	■是 □否 □不適用，請說明： _____
	36. 應監控資通系統遠端連線。	無明確規範	□是 □否 □不適用，請說明： _____

	37. 資通系統應採用加密機制。	應用服務系統如公共網路提供服務(如全球資訊網或其他對外網站等)，應設計透過適當安全通訊管道進行傳輸，以防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。	■是，請勾選實作方式： ■HTTPS 加密 □SSH 加密 □VPN 加密 □遠端桌面通訊協定(RDP)啟用加密 □其他 _____ □否 □不適用，請說明： _____
	38. 資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	僅提供必要之網路服務項目、通訊協定、與連線時間，所有行為不得與原有之網路安全相關限制、規定相抵觸。 臨時性廠商不開放連線申請，除有特殊需求，依相關規定辦理。	■是 □否 □不適用，請說明： _____
稽核與可歸責性	39. 應定期審查稽核事件。	系統管理者與操作者日誌應定期予以審查。	■是 □否 □不適用，請說明： _____
	40. 資通系統產生之稽核紀錄，應依需求納入其他相關資訊。	系統有提供紀錄功能應予啟動，若無則視系統之重要性，以書面方式紀錄之。	■是，稽核紀錄已納入所需資訊 □否，稽核紀錄內容未符合需求 □不適用，請說明： _____
	41. 系統內部時鐘應依機	資訊設備及主機伺服器	■是

	關規定之時間週期與基準時間源進行同步。	應盡可能與單一參考時間源同步。以確保系統時間的一致性。 資訊設備如無法設定單一參考時間源，則應約定同步之時間源，由設備管理員定期(至少每季一次)或於設備異動時進行系統時間同步作業。	□否 □不適用，請說明： _____
	42. 應運用雜湊或其他適當方式之完整性確保機制。	無明確規範	□是，請勾選實作方式： □提供稽核資訊之雜湊值 □使用異地備份進行完整性驗證 □使用目錄監控軟體偵測檔案異動 □其他 _____ □否 □不適用，請說明： _____
營運持續計畫	43. 應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	關鍵業務系統備份資料應至少每年執行資料回復測試並填寫「備份資料還原測試紀錄單」，以確認備份資料之可用性。	■是 □否 □不適用，請說明： _____
	44. 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。	機房及核心業務資訊系統運作中斷至恢復最低運作水準之條件下，其最大可容忍中斷的時間	■是，時間為 __72 小時_____ □否

		（考量實務現況）	□不適用，請說明： _____
	45. 原服務中斷，於可容忍中斷時間內，由備援設備取代提供服務。	無明確規範	□是 □否 □不適用，請說明： _____
識別與鑑別	46. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	程式設計應具備檢驗登入身分識別與秘密鑑別資訊功能，秘密鑑別資訊如採密碼，其保護機制應考慮包含密碼長度限制、密碼組合限制、密碼錯誤次數限制與變更密碼歷史管理，並可將身分驗證之相關紀錄提供其他稽核工具使用。	■是，請勾選實作方式： □CAPTCHA ■帳戶鎖定機制 □其他 _____ □否 □不適用，請說明： _____
	47. 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記(Token)。 註：密碼重設機制係指使用者忘記密碼之處理方式。	無明確規範	□是，請勾選實作方式： □寄發 EMAIL 驗證連結 □寄發簡訊驗證碼 □其他 _____ □否，請勾選實作方式： □寄發原始密碼 □寄發由系統自動產生之新密碼 □不適用，請說明： _____
	48. 資通系統如以密碼進	儲存於系統之密碼檔須	■是，請勾選實作方式：

	行鑑別時，該密碼應加密或經雜湊處理後儲存。	加密儲存。	■密碼加密儲存 □密碼雜湊儲存 □其他 _____ □否 □不適用，請說明： _____
系統與服務獲得	49. 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估。	應向系統開發單位或委外廠商確認相關系統修正或安全問題更新程式之影響與處理方式，以建立應用系統技術脆弱性資訊之取得管道，評估可能帶來之風險。	■是 □否 □不適用，請說明： _____
	50. 將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。	未明確規範，後續將以此表單進行安全需求之確認	■是 □否 □不適用，請說明： _____
	51. 於系統發展生命週期之維運階段，須注重版本控制與變更管理。	無明確規範，基本上變更前皆需進行備份。	■是 □否 □不適用，請說明： _____
	52. 開發、測試及正式作業環境應作區隔。	測試環境所使用之設備環境應予獨立，不應與提供線上服務之設備環境共用。	■是 □否 □不適用，請說明： _____
系統與資	53. 定期確認資通系統相關漏洞修復之狀態。	主機管理人員需確實檢視系統日誌（含各式通訊服務之連線紀錄）、系統資源使用狀態、系	■是 □否 □不適用，請說明：

訊完整性		統漏洞與修補程式安裝情形。	＿＿＿＿＿＿＿＿＿＿
	54. 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	無明確規範	□是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿＿＿
	55. 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	無明確規範	□是，請勾選實作方式： □目錄監控(如 Linux inotify 等工具) □使用雜湊機制 □其他 ＿＿＿＿＿＿＿＿＿＿ □否 □不適用，請說明： ＿＿＿＿＿＿＿＿＿＿
	56. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。	輸入欄位檢測：緩衝區溢位、輸入資料型態控管(SQL Injection)、防呆功能測試。	□是 □否，請勾選實作方式： □未檢查資料合法性 □僅實作於前端 □不適用，請說明： ＿＿＿＿＿＿＿＿＿＿
	57. 當發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無明確規範	□是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿＿＿
高級系統適用項目			
存取	58. 逾越機關所定預期閒置時間或可使用期限時，系統應自動將使	各應用系統均應規劃適當之閒置時間，使用者登入~~較具機密性之~~應用	□是，請勾選實作方式： □閒置___分鐘以上自

控制	用者登出。	系統後，若超過 15 分鐘無任何動作時，系統須設定將其帳號鎖定或登出 (特殊系統不在此規範)。	動登出 □其他 _____ □否，未自動登出 □不適用，請說明： _____
	59. 應依機關規定之情況及條件，使用資通系統。	無明確規範，基本上機關內部無限制，外部遠端連線限制 IP 位址。	□是，請勾選實作方式： □限定系統使用時段 □限定 IP 來源 □其他 _____ □否 □不適用，請說明： _____
	60. 監控資通系統帳號，如發現帳號違常使用時回報管理者。	無明確規範	□是 □否 □不適用，請說明： _____
稽核與可歸責性	61. 機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	無明確規範	□是，請勾選實作方式： □Email 通知 □簡訊通知 □其他 _____ □否 □不適用，請說明： _____
	62. 定期備份稽核紀錄至與原稽核系統不同之實體系統。	無明確規範	□是，請勾選實作方式： □手動備份 □自動備份至 Log 伺服

			器(如 syslog) □其他 _____ □否 □不適用，請說明： _____
營運持續計畫	63. 應將備份還原，作為營運持續計畫測試之一部分。	營運持續計畫每年進行測試/演練，項目由資訊安全緊急處理小組負責規劃，並由相關業務單位擬訂執行計畫，進行測試/演練過程並將結果填寫於「業務持續計畫/資安事故復原演練暨處理報告單」。	■是 □否 □不適用，請說明： _____
	64. 應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	無明確規範	□是 □否 □不適用，請說明： _____
識別與鑑別	65. (內部使用者之識別與鑑別)對帳號之網路或本機存取採取多重認證技術。	無明確規範	□是，請勾選實作方式： □使用自然人憑證或晶片卡 □使用生物特徵，如指紋 □使用黑/白名單限制來源 IP □其他 _____ □否

			□不適用，請說明： ＿＿＿＿＿＿＿＿
系統與服務獲得	66. 執行「源碼掃描」安全檢測。 (系統發展生命週期開發階段)	無明確規範	□是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
	67. 具備系統嚴重錯誤之通知機制。 (系統發展生命週期開發階段)	系統應具備輸入輸出錯誤檢查機制，並提示使用者輔助資訊。	□是，請勾選實作方式： □電子郵件 □簡訊 □其他 ＿＿＿＿＿＿＿＿ □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
	68. 執行「滲透測試」安全檢測。 (系統發展生命週期測試階段)	透過網路存取之系統應執行適當之弱點掃描或滲透測試，弱點掃描或滲透測試應依據系統架構，以確認所開發的系統架構是否存在安全弱點或安全漏洞。	■是 □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
系統與通訊保護	69. 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	資訊系統應保護敏感等級（含）以上之資料，防止洩漏或被竄改，必要時應使用資料加密等技術保護。	■是，請勾選實作方式： ■啟用 HTTPS □其他 ＿＿＿＿＿＿＿＿ □否 □不適用，請說明： ＿＿＿＿＿＿＿＿
	70. 使用公開、國際機構	無明確規範	□是

	驗證且未遭破解的演算法。		□否，請勾選實作方式： □HTTPS 允許 SSLv3 或 TLSv1.0 □HTTPS 使用 RC4、DES 或 3DES □HTTPS 使用 MD5 或 SHA-1 □其他 _____ □不適用，請說明：_____
	71. 支援演算法最大長度金鑰。	無明確規範	□是 □否 □不適用，請說明：_____
	72. 加密金鑰或憑證週期性更換。	無明確規範	□是 □否 □不適用，請說明：_____
	73. 伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	無明確規範	□是 □否 □不適用，請說明：_____
	74. 靜置資訊及相關具保護需求之機密資訊應加密儲存。備註：靜置資訊，指資訊位於資通系統特定元件，例如儲存設備上之狀態，或與系統相關需	無明確規範	□是 □否 □不適用，請說明：_____

	要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。		
系統與資訊完整	75. 資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	無明確規範	□是 □否 □不適用，請說明： _____
	76. 應定期執行軟體和資訊完整性檢查。	無明確規範	□是 □否 □不適用，請說明： _____