文件版本 3.3 發行日期 20171002

國立臺灣師範大學
單位資訊系統委外開發案件檢核單

招標前計畫階段

項次	項目	檢核重點	建議產出文件	說明
1	平台環境	❍ Web 版/行動版 1. 是否載明系統作業伺服器環境 （例：Windows 2012 Server（含）以上 ） □是□否（原因：_____） 2. 是否載明資料庫伺服器環境 （例：Microsoft SQL Server 2012(含)以上 ） □是□否（原因：_____） 3. 是否載明使用者操作介面 （例：IE11.0、FireFox46.0.1、Google Chrome50.0 網頁瀏覽器之版本 ） □是□否（原因：_____） 4. 是否載明網路通訊方式 （例：HTTP/HTTPS ） □是□否（原因：_____） 5. 是否載明系統開發軟體 （例：VB.NET、JavaScript……等） □是□否（原因：_____） 6. 是否載明多（雙）語系 □是□否（原因：_____）		

項次	項目	檢核重點	建議產出文件	說明
		❍ APP 1. 是否載明 app 平台 （例：Android APP、iOS APP 等） □是□否（原因：_____）		
2	平台環境維護	1. 是否載明各類作業系統之安裝責任歸屬？ □是□否（原因：_____） 2. 是否載明各類作業系統維護責任歸屬？ □是□否（原因：_____） 3. 是否載明各類作業系統之系統憑證的費用問題？ □委外經費支出 □廠商支出 4. 是否載明各類作業系統之安全性設定責任歸屬？ □是□否（原因：_____） 5. 是否載明各類作業系統更新 Patch 責任歸屬？ □是□否（原因：_____）		無須全部載明，請依照需求確認
3	需求清單	1. 應釐清作業流程 □是□否（原因：_____） 2. 應釐清功能需求 □是□否（原因：_____）	1. 作業流程圖 2. 委外開發系統需求清單	請見附件 1「系統需求清單範本」
4	資料庫相關	是否介接其他資料庫/系統？ □是□否（原因：_____）		
5	舊系統相關	1. 若有相關連的舊系統，是否需要使用原資料庫？ □是□否（原因：_____） 2. 若有相關連的舊系統，是否需要介接舊資料		

項次	項目	檢核重點	建議產出文件	說明
		庫？ □是□否（原因：_____） 3. 若有相關連的舊系統，是否需要移轉資料庫軟、硬體設備？？ □是□否（原因：_____） 4. 若需要移轉資料庫的軟硬體設備，是否載明移轉責任歸屬？ □是□否（原因：_____） 5. 若需要移轉資料庫的軟硬體設備，是否載明相關移轉費用？ □委外經費支出 □廠商支出		
6	專案管理期程	1. 是否詳細定義專案管理期程？ □是□否（原因：_____） 2. 是否載明專案人力配置？ □是□否（原因：_____） 3. 是否載明專案組織架構？ □是□否（原因：_____）		專案管理時程需以「結標次日後 XX 日曆天」方式撰寫。
7	備份備援機制	分為三種：程式、資料庫、檔案 1. 是否規劃備份機制 □是□否（原因：_____） 2. 是否規劃備援機制 □是□否（原因：_____） 3. 若為自動化備份機制，是否有明定備份周期？ □是□否（原因：_____） 4. 若使用備援機制，是否有規劃備援週期？		備份：將系統、資料庫及設定檔，以檔案形式儲存至另一個儲存空間，且固定一段時間備份一次，並存放多代，主要是為了當系統發生問題時，可以減少系統停機

項次	項目	檢核重點	建議產出文件	說明
		□是□否（原因：_____） 5. 若使用備援機制，問題發生時的啟用、回復模式是否有規劃？ □是□否（原因：_____） 6. 是否加入業務永續運作演練? □是□否（原因：_____） 7. 若加入業務永續運作演練，是否載明延伸費費用歸屬？ □委外經費支出 □廠商支出		時間。 備援：當系統發生問題時，可手動或自動方式切換至另一個備用系統，即可讓系統正常運作，主要是為了當系統發生問題時，可以減少系統停機時間。

8	資訊安全	1. 選擇弱點掃瞄方式。 □校外掃描（請自行處理） □校內掃描 2. 選擇校內弱點掃瞄通過等級。 3. 系統上線後有重大變更，是否進行弱點掃瞄？ □是□否（原因：_____） 4. 是否需要進行資訊系統安全檢核？ □是□否（原因：_____） 5. 若選擇進行 App 開發，是否進行 App 資安檢測？ 是□否□（原因：_____） 6. 若需要 App 資安檢測，檢測費用歸屬問題？ □委外經費支出 □廠商支出 7. 系統上線後有重大變更，是否進行 App 資安檢測？ □是□否（原因：_____）		1. 校內弱點掃瞄相關說明：http://www.itc.ntnu.edu.tw/page4/super_pages.php?ID=page401&Sn=26 2. 其他資訊安全相關說明，請見附件 2「資訊系統委外開發 RFP 資安需求範本」 3. 資訊系統安全檢核：為加強伺服器安全管理，避免受到駭客攻擊。資訊系統安全檢核表下載請至：http://www.itc.ntnu.edu.tw/page7/super_pages.php?ID=page701&Sn=37 4. App 資安檢測相關規定，請見附件 3「國家發展委員會函」。

9	SSL 憑證及費用	1、是否需要 SSL 憑證？ □是□否（原因：_____） 2、若需要 SSL 憑證，憑證費用歸屬問題？ □委外經費支出 □廠商支出 3、若需要 SSL 憑證，憑證過期時的費用歸屬問題？ □委外經費支出 □廠商支出 4、維護案中若 SSL 憑證已過有效期限，是否需要再繼續使用？ □是□否（原因：_____） 5、維護案中 SSL 憑證歸屬問題？ □委外經費支出 □廠商支出		
10	無障礙認證	1、網頁製作是否需要符合無障礙環境作業規定？ 是□否□（原因：_____） 2、是否有額外經費預算進行無障礙作業環境設計網站？ 是□否□（原因：_____） 3、若需要無障礙認證，是否由廠商申請認證？ 是□否□（原因：_____） 4、若需要無障礙認證，是否載明符合檢測等級 AA 以上？ 是□否□（原因：_____）		依據國家通訊傳播委員會於 106 年 8 月 3 日頒訂之規定，請見附件 4「國家通訊傳播委員會函」。

項次	項目	檢核重點	建議產出文件	說明
11	智慧財產權	1. 是否載明軟體的智慧財產權歸屬？ 是□否□（原因：_____）		依採購組採購文件辦理
12	教育訓練	1. 是否需要教育訓練？ 是□否□（原因：_____） 2. 若需要教育訓練，是否載明教育訓練的場次，例如，驗收時前需舉辦多少場次？或是驗收後需要舉辦多少場次等 是□否□（原因：_____） 3. 若需要教育訓練，是否載明每次教育訓練的時間？ 是□否□（原因：_____） 4. 承辦人更換時是否需要舉辦教育訓練等等。 是□否□（原因：_____） 5. 若需要教育訓練，是否載明教育訓練是場地費支出的歸屬。 是□否□（原因：_____）		

項次	項目	檢核重點	建議產出文件	說明
13	系統帳號密碼驗證	1. 系統是否需要有登入機制？ 是□否□（原因：_____） 2. 若需要登入機制，是否需進行帳號密碼驗證？ 是□否□（原因：_____） 3. 若需要使用帳號密碼驗證，是否需使用校務行政帳號驗證？ 是□否□（原因：_____） 4. 若不需要使用校務行政帳號密碼驗證，是否有說明驗證方式？ 是□否□（原因：_____） 5. 若需要校務行政帳號驗證，是否註明「帳號密碼驗證機制需配合本校資訊中心辦理」。 是□否□（原因：_____）		
14	校務資料整合	1. 是否需與校務資料整合？ 是□否□（原因：_____）		
15	單一簽入機制介接	1. 是否要納入本校之校務正入口網？ 是□否□（原因：_____） 2. 是否需透過校務行政入口網進行代登入？ 是□否□（原因：_____） 3. 是否需透過校務行政入口 APP 進行代登入？ 是□否□（原因：_____）		

項次	項目	檢核重點	建議產出文件	說明
16	保固服務	1. 是否需要保固服務？ 是□否□（原因：_____）		依採購組採購文件辦理

履約管理階段

項次	項目	檢核重點	建議產出文件	說明
1	啟動會議	1. 系統功能細部討論 2. 甲方提出專案工作計畫書 3. 甲方提出系統設計規格書	1. 會議記錄 2. 保密切結書 3. 專案工作計畫書 4. 系統設計規格書	「保密切結書」請依照採購組文件
2	需求訪談會議		1. 需求訪談記錄表 2. 系統需求分析規格書	請見附件 5「需求訪談記錄表」
3	定期專案會議	1. 進度報告 2. 甲方更新開發文件	1. 會議紀錄 2. 「系統需求分析規格書」更新版 3. 「系統設計規格書」更新版	
4	舊資料轉檔	甲方提出轉檔計畫書	轉檔計畫書	
5	系統測試	甲方提出「系統上線測試計畫書」	1. 系統測試驗證紀錄單 2. 系統上線測試計畫書	請見附件 6「系統測試驗證紀錄單」
6	教育訓練	請檢視招標前計畫階段第 12 項，規劃教育訓練時間。	1. 教育訓練學員簽到表 2. 課程評估問卷表	請依照承辦單位需求評估是否增加「課程評估問卷表」

驗收階段

項次	項目	檢核重點	驗收文件	說明
1	系統功能驗收	請檢視履約管理全階段	1. 系統需求分析規格書 2. 系統設計規格書 3. 專案工作計畫書 4. 系統測試驗證紀錄單 5. 系統功能測試報告 6. 系統上線測試計畫書 7. 系統軟體正確版本的中文使用手冊、系統維護管理與障礙排除手冊等相關手冊 8. 正確版本的原始程式碼 9. 結案報告	
2	平台環境維護	1. 請檢視招標前計畫階段第 2 項。 2. 若選擇由廠商支付憑證費用，需有此驗收文件。	系統憑證證明	
3	資訊安全	1. 請檢視招標前計畫階段第 8 項。 2. 若選擇校內掃瞄，需有此驗收文件。 3. 請檢視是否完成資訊系統安全檢核表。 4. 若選擇進行 App 資安檢測，需有此驗收文件。	1. 伺服器申請弱點掃描__級通過確認單 2. 資訊系統安全檢核表 3. App 資安檢測報告及合格證書	

項次	項目	檢核重點	驗收文件	說明
4	SSO 介接或 LDAP 介接	1. 請檢視招標前計畫階段第 8 項。 2. 若選擇「是」，需驗證帳號是否能夠轉接。		
5	SSL 憑證	1. 請檢視招標前計畫階段第 9 項。 2. 若選擇由廠商支付憑證費用，需有此驗收文件。	憑證證明	
6	無障礙認證	1. 請檢視招標前計畫階段第 10 項。 2. 若選擇需符合無障礙環境規定，需驗證系統上是否有認證標誌。 3. 若選擇需符合無障礙環境規定，需驗證是否符合檢測等級 AA 以上。	系統上需有認證標誌	
7	教育訓練	1. 請檢視招標前計畫階段第 12 項。 2. 履約階段第 6 項	1. 教育訓練學員簽到表 2. 課程評估問卷表	「課程評估問卷表」為非必要文件
8	其他	請檢視履約管理階段第 1 項	保密切結書	

維運管理階段

項次	項目	檢核重點	建議產出文件	說明
1	系統上線後之修正	1. 是否有規劃正式上線後的各版本的版號規則? 是□否□（原因：_____） 2. 是否有規劃正式上線後的上版機制? 是□否□（原因：_____） 3. 是否有規劃上版後之系統查核機制? 是□否□（原因：_____） 4. 上版後是否修改相關文件 是□否□（原因：_____） 5. 重大修改後是否進行弱點掃瞄？ 是□否□（原因：_____） 6. 重大修改後是否進行 App 資安檢測？ 是□否□（原因：_____）	1. 版本號規則 2. 上版記錄與驗證紀錄單 3.1 修正「系統需求分析規格書」 3.2 修正「系統設計規格書」 3.3 修正「系統軟體中文使用手冊」 3.4 修正「系統維護管理與障礙排除手冊」 4. 伺服器申請弱點掃描__級通過確認單 5. App 資安檢測報告及合格證書	請見附件 7：「上版記錄與驗證紀錄單」

2	付款方式	1. 是否有規劃付款方式週期？ 是□否□（原因：_____） 2. 是否規劃付款時所需查核文件 是□否□（原因：_____）		

附件 1

國立臺灣師範大學單位委外開發系統需求清單

編號	需求項目	需求說明	該需求是否提供畫面或格式

附件 2

專案管理期程規劃範本

本案執行分為**六個階段**，各階段時程及應交付之項目如下表：

階段	時程	交付項目
第一階段： 專案工作計畫書	決標次日起 XX 日曆天內	1. 專案管理及工作計畫書 2. 召開專案啟動會議之會議記錄
第二階段： 系統分析	第一階段交付後次日起 XX 日曆天內	1. 訪談紀錄、作業流程圖 2. 系統分析規格書
第三階段： 系統設計	第二階段交付後次日起 XX 日曆天內	1.雛形系統展示 2.系統設計規格書(含: 資料庫架構圖、系統軟體架構、資料流程圖、資料表關連圖、資料庫物件清單、功能清單)
第四階段： 系統建置與程式開發	第三階段交付後次日起 XX 日曆天內	1. 符合本案功能需求之系統軟體 2.程式清單與說明 3.程式碼 4.系統上線測試計畫書
第五階段： 系統測試與舊資料轉檔作業	第四階段交付後次日起 XX 日曆天內	1. 系統功能測試報告 2. 舊資料拋轉後系統測試報告 3. 本案教育訓練開課計畫
第六階段： 教育訓練、系統上線啟用、系統驗收	第五階段交付後次日起 XX 日曆天內	1. 系統軟體之中文使用手冊、系統維護管理與障礙排除手冊等相關手冊 2. 交付/更新相關設計開發文件 3. 教育訓練成果報告，需包含上課簽到表、課程授課評估問卷 4. 系統驗收報告，需包含欲交付之系統軟體、工具與手冊等清單及資安檢測報告書資料 5. 系統軟體所使用到的相關原版軟體與合法取得證明 6. 本案承包廠商須於驗收完成後，提供系統軟體保固維護合約或證明一年。

資訊系統委外開發RFP資安需求範本

國家資通安全科技中心

中華民國105年6月

修訂歷史紀錄

版次	生效日期	修 訂 說 明
1.0	1050630	新編

文件說明

文件名稱	資訊系統委外開發 RFP 資安需求範本
資訊等級	☐機密　☐密　☐內部使用　☒普通
相關撰稿人	蔡宗霖
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：

本文件為政府機關資訊系統委外開發 RFP 資安需求範本，內容以資訊系統安全需求為主，依軟體安全特性各項類型，包含「機密性」、「完整性」、「可用性」、「身分驗證」、「授權與存取控制」、「日誌紀錄」、「會談管理」、「錯誤與例外處理」、「組態管理」，訂定共 50 項安全需求項目，並依據行政院資通安全會報頒布之「資訊系統分級與資安防護基準作業規定」，依資訊系統的安全分級(普、中、高)，參考 OWASP、SANS 等國際組織建議，進行安全需求項目分級與內容訂定。

本報告主要為提供機關於資訊系統委外，訂定建議書徵求說明書(RFP)時，有關系統資訊安全需求之參考依據，RFP 範本之主體，以經濟部工業局公布之建議書徵求說明書(RFP)範例作為基礎，增加:

3.2 系統安全需求

附件 1:系統安全需求項目查檢表。

以期能落實軟體安全發展生命週期之實踐，從源頭有效強化整體資訊系統之安全性，強化政府整體資安能量。

關鍵詞	軟體安全發展生命週期、資訊系統安全需求

建議書徵求說明書
（資訊系統委外開發 RFP 資安需求範本）

一、概述

簡述專案之背景、起因、現況及欲達成之理想。

二、專案性質描述

2.1 專案名稱“○○○○○○○○○”。

2.2 專案目標

明確條列本專案欲達成之目標。

2.3 專案範圍

明確條列本專案之範圍，含或不含之項目。

2.4 專案時程

要求計畫完成之時間。如簽約後○個月內完成。

2.5 專案費用

2.5.1 計價方式

敘述本專案之計費方式(如總包價法、服務成本加公費法)，及計費標準參考文件(如依行政院頒佈之「各機關資訊作業委外服務實施要點」所提供之計費標準)。

2.5.2 付款方式

簡述付款期數、條件、時間、程序....等。

說明:應用軟體委外是一種勞務性質的服務與一般硬體的採購是不一樣的，一般都採取分階段付款之方式。

2.5.3 需求變更

詳述在專案進行中如有新增及變更需求發生時並經雙方確認後，得依行政院頒佈之「各機關資訊作業委外服務實施要點」所提供之計費標準另議。

三、需求說明

3.1 整體需求說明

詳細條列系統之各項功能要求及系統作業流程並詳細說明之。

3.1.1 功能需求

3.1.2 系統作業流程說明

3.2 系統安全需求

以下依不同系統安全特性，分別說明相關之安全需求項目。機關可參考資訊系統分級及該系統之特性，自行選用適用之需求項目。所有系統安全需求項目之彙整查檢表，請參閱附件 1(註：僅 WEB 網站系統適用之安全需求，將特別標註 WEB)。

3.2.1 機密性

1. 機敏資料傳輸時，採用加密機制

適用分級：普、中、高。

說明：網站傳輸機敏資料時，採用 HTTPS(透過 SSL 或 TLS 等加密協定)協定以確保機敏資料以密文方式傳輸。

2. 使用公開、國際機構驗證且未遭破解的演算法

適用分級：中、高。

說明:不使用自行創造的加密方式。採用公開、國際認可之演算法，

例如 AES 對稱式加密演算法、RSA 非對稱式演算法及 SHA 安全雜湊演算法等。

3. 使用演算法支援的最大長度金鑰

適用分級：中、高。

說明：系統中採用密碼學演算法時，使用該演算法目前支援的最大金鑰長度，以減少被暴力破解解密之可能及弱點。例如 AES 256 bits、RSA 2048 bits 或以上、SHA-512 等。

4. 加密金鑰或憑證週期性更換

適用分級：中、高。

說明：產生網站 HTTPS 使用之憑證，應具備 3 年以下之使用年限限制，並於到期前進行更換。系統若另行使用自行產生之加密金鑰，亦需定期更換。

5. 加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制

適用分級：高。

說明:常見加密金鑰以檔案形式放置於作業系統中,並以路徑存取，此作法之安全性較採用獨立之硬體安全模組(hardware security module，HSM)來保護金鑰為低。採用獨立之硬體安全模組，通常將金鑰保護於硬體晶片環境以避免被竊取，同時具備多種驗證類型(IP、PIN 碼等)，對金鑰存取進行限制。

6. 機敏資料儲存時，採用加密機制

適用分級：高。

說明：機敏資料存於資料庫或其他儲存媒體時，採用對稱式或其他

加密方式，將機敏資料加密成密文後儲存，並於需要取得原文明文時解密還原。此作法可減少機敏資料因儲存媒體有其他存取管道而洩漏的風險。

3.2.2 完整性

1. 於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性

   適用分級：普、中、高。

   說明：對於使用者輸入欄位資料，採用正規表示式(Regular Expression)進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法。

2. 針對開放下載的資料，也提供資料之雜湊值(HASH Value)供使用者比對其完整性

   適用分級：中、高。

   說明：網站提供使用者下載的資料，於下載連結處，以安全雜湊演算法產生雜湊值(HASH Value)供使用者參考比對，並說明使用的雜湊演算法為何。

3. 具有防範 SQL 命令注入攻擊(SQL Injection)之措施

   適用分級：中、高。

   說明：系統於伺服器端具有防範 SQL 命令注入攻擊措施。例如 Prepared statements、Stored procedures、輸入驗證(Input Validation)等。

4. 具有防範跨站腳本攻擊(Cross-Site Scripting)之措施

   適用分級：中、高。

說明：系統於伺服器端具有防範跨站腳本攻擊(Cross-Site Scripting)措施。例如黑名單過濾跳脫特殊字元、白名單正規表示式驗證、輸出編碼等。此安全需求項目僅適用於 WEB 網站系統。

5. 驗證網頁重導(Redirects)與導向(Forwards)之目的地在合法名單內

適用分級：中、高。

說明：網站若提供網頁重導或導向之功能，必須確認使用者輸入欲重導向的網頁，其值在合法白名單內，以避免被利用來重導向至惡意網頁。此安全需求項目僅適用於 WEB 網站系統。

6. 重要系統資料或紀錄留存雜湊值以確保完整性

適用分級：高。

說明：重要資料或紀錄，以安全雜湊演算法產生並留存其雜湊值，後續可對資料再次產生雜湊值並與原先結果進行比對，以確保資料未遭到異動竄改。

3.2.3 可用性

1. 重要資料定時同步至備份或備援環境，並加以保護限制存取

適用分級：普、中、高。

說明：系統具備重要資料定時備份機制，依組織規範將資料同步至備份或備援環境，以避免系統毀損或資料綁架勒索對資料可用性之危害。重要資料於備份或備援環境應有保護限制存取措施，以避免增加其他資安風險。

2. 採用「高可用性」(High Availability) 架構(分散式或叢集伺服器架構)

適用分級：高。

說明：系統之服務水準，經評估後須滿足高可用性需求者，應考量採取分散式或叢集伺服器架構，以使當系統發生錯誤情況或硬體毀損時，服務仍能正常運作。

3.2.4 身分驗證

1. 除了允許匿名存取的功能外，所有功能都必須已通過身分驗證才允許存取

適用分級：普、中、高。

說明：網站除公開區域外，其他網頁皆需已進行身分驗證登入成功後，才得以存取(接續應檢查該使用者權限是否允許其存取該網頁或功能)。使用者若存取非公開區域，檢查機制發現其尚未通過身分驗證時，應不允許其存取頁面並將其導向至首頁或登入頁面。

2. 身分驗證機制位於伺服器端且採用集中過濾機制(例如使用 Filter 過濾器)

適用分級：中、高。

說明：系統應包含具有一致全面性、位於伺服器端，強制適用於全系統的授權及存取控制機制。例如使用 Filter 過濾器機制。

3. 身分驗證相關資訊(帳號、密碼等)不留存於程式原始碼中

適用分級：中、高。

說明：網站系統若具有與其他外部系統或資料庫等連線的需求，不可將連線之身分驗證資訊(帳號、密碼等)寫於程式原始碼中，應採用設定檔或於系統啟動時動態輸入之方式。身分驗證資訊若以參數方式留存於設定檔，應確認僅有執行該系統之作業系統帳號可以存取設定檔。

4. 確實規範使用者密碼強度（密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元）

適用分級：中、高。

說明：若採用密碼作為身分驗證機制，當使用者設定密碼時，需以正規表示式檢查密碼強度是否符合標準，例如密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元。

5. 使用者必須定期更換密碼，且至少不可以與前 5 次使用過之密碼相同

適用分級：中、高。

說明:使用者初次設定或異動密碼時,系統應留存設定密碼之時間，往後每次使用者成功登入後，必須檢查該組密碼是否已使用超過組織政策所規定的最長期限(例如，45 天)，若已超過時限則強制使用者更換密碼，使用者的前 5 次舊密碼應被保留(以雜湊值的形式)，新密碼應比對且不允許與前 5 次使用密碼相同。

6. 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 30 分鐘內不允許該帳號及來源 IP 繼續嘗試登入

適用分級：高。

說明：系統須具備帳戶鎖定機制，記錄使用者身分驗證錯誤次數，若錯誤次數達到組織資安規範之次數(例如，3 次)，則針對該帳號及來源 IP 進行鎖定一段時間(例如，30 分鐘)。鎖定時間後使用者再次進行身分驗證登入嘗試時，應將錯誤次數歸零。除帳號外亦鎖定來源 IP 的用意為防範攻擊多個帳號，使同一來源無法在某個帳戶鎖定後，又再行嘗試其他帳戶。

7. 身分驗證相關資訊不以明文傳輸

適用分級：高。

說明：系統傳遞身分驗證相關資訊(例如帳號密碼)時，採用加密傳輸，以避免該資訊被攔截或監聽竊取。

8. 密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數及雜湊後密碼

適用分級：高。

說明：系統儲存使用者密碼時，不宜儲存明文密碼，以避免遭到有心人士竊取。使用者設定密碼時，應針對該使用者產生一個亂數值，將使用者密碼結合亂數值，再以雜湊函式(HASH Function)處理產生雜湊值後，分別於不同欄位儲存使用者亂數值及雜湊值。後續使用者輸入密碼時，以輸入值添加當初設定密碼時產生的亂數，再次以雜湊函式處理，若產出結果同當初設定密碼時的雜湊值，則表示輸入密碼正確。

9. 採用圖形驗證碼(CAPTCHA)機制於身分驗證及重要交易行為，以防範自動化程式之嘗試

適用分級：高。

說明：系統若採用帳號密碼進行身分驗證，往往可能遭受到自動化程式以暴力破解方式嘗試登入。另外，系統重要行為若被獲知相關執行參數，亦可能被自動化程式嘗試偽冒合法使用者觸發。因此，採用圖形方式顯示一驗證碼於頁面上，並要求使用者辨別該圖形中文字之方式，或以其他足以辨識人為動作之方式(例如勾選特定選項)，將可以防堵自動化程式之嘗試行為。

10. 重要交易行為要求使用者再次進行身分驗證

適用分級：高。

說明：系統中重要交易行為，於執行前應再次確認獲得授權。要求使用者再次身分驗證是確認獲得授權的手段之一。另外此作法亦可有效防堵攻擊者透過其他方式取得使用者身分憑證後，直接偽冒使用者執行重要交易行為。

11. 採用多重因素身分驗證(兩種以上驗證類型)

適用分級：高。

說明：系統身分驗證或重要交易行為，可採用多重因素身分驗證以強化安全性。多重因素身分驗證意指具備兩種以上驗證類型，驗證類型一般區分為所知之事(Something you know)、所持之物(Something you have)及所具之形(Something you are)。所知之事類型常採用密碼、特定問題之答案等。所持之物類型常採用令牌(Token)、憑證、簡訊、電子郵件等。所具之形類型常採用生物特徵，如指紋、虹膜辨識等。

12. 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令牌(Token)，檢查傳回令牌有效性後，才允許使用者進行重設密碼動作

適用分級：高。

說明：密碼重設機制設計不良可能造成安全問題。常見錯誤是系統主動將密碼重新設定後寄送給使用者。使用者忘記密碼並啟動密碼重設機制時，應以使用者其他留存於系統的聯絡資訊，例如電子郵件或手機號碼，先要求使用者輸入該資訊，比對正確無誤後，發送一次性及具有時效性令牌(Token)，一般是亂數產生的英數字，使用者接收後須於時效內進行輸入回傳動作，系統檢查回傳令牌有效性後，允許使用者重設密碼。

3.2.5 授權與存取控制

1. 執行功能及存取資源前，檢查使用者授權

適用分級：普、中、高。

說明：系統中除了公開區域外，任何執行功能及存取資源動作前，應檢查使用者已通過身分驗證且使用者具備權限可執行該功能或存取該項資源。

2. 採用伺服端的集中過濾機制檢查使用者授權

適用分級：中、高。

說明：檢查使用者是否具備存取功能或資源之機制，應位於伺服器端且採用全面性集中控管機制(例如採用網站過濾器Filter機制)，明確設定檢查範圍。檢查機制位於伺服器端可以避免被攻擊者繞過檢查的問題，全面性集中控管可以避免人為疏漏導致可能有功能未檢查使用者授權之問題。

3. 對使用者/角色，僅賦予所需要的最低權限

適用分級：中、高。

說明：明確定義系統中角色及對應的權限，系統上線驗收時，應審查使用者賦予的角色及其取得的權限是否適當，系統上線後亦定期審查使用者所擁有的角色與權限清單。相關資訊宜提供系統介面以供查詢或匯出。

4. 軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限執行

適用分級：高。

說明：系統之軟體程序或伺服器服務，若以系統最高權限或管理員權限啟動，將造成攻擊者成功入侵伺服器時，可以取得作業系統最高權限。應於作業系統增加服務專用之使用者，並授予執行伺服器

服務及讀寫相關檔案的有限範圍權限，使其可以正常執行軟體程序作業，同時避免過高權限之風險。

5. 除特殊管理者權限外，其他角色或權限無法修改系統中授權資料及存取控制列表(ACL)

適用分級：高。

說明：存取控制列表是用來表示系統使用者具有哪些權限的清單，實際上可能由多張表格組成，包含使用者清單、角色清單、權限清單、角色與權限關聯清單及使用者與角色關聯清單等。系統應確保只有特定管理員權限可以透過介面或具備資料庫權限可以修改存取控制列表，一般使用者無存取控制列表之修改權限。

6. 重要行為由多人/角色授權後才得以進行

適用分級：高。

說明：設計軟體功能時將條件設定在兩個或多個以上，且需要滿足所有的條件才能完成作業時，稱之為職責分離(Separation of Duties)。系統重要行為可以採取須通過多人/角色授權後才得以進行之設計。職責分離可以減少單一人員或資源由於權限過大，所可能造成的安全危害。實行職責分離再加上行為的稽核記錄，可以防範內部舞弊的情況發生。

7. 具有防範「跨站請求偽造」(Cross-Site Request Forgery，CSRF)攻擊之措施

適用分級：高。

說明：「跨站請求偽造」攻擊發生情況為，攻擊者知道網站特定行為的執行參數，在使用者已通過網站身分驗證登入後，以欺騙使用者點選連結或其他方式，偽造使用者之請求進行該特定行為並帶入相關參數，以遂行惡意之目的。防範 CSRF 的措施主要有：1.重要

行為前先動態產生獨立而唯一的 request token，並於執行行為前檢查。2. 要求使用者重新身分驗證或證明該動作是人為進行(使用 CAPTCHA)。此安全需求項目僅適用於 WEB 網站系統。

3.2.6 日誌紀錄

1. 針對身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行日誌記錄

   適用分級：普、中、高。

   說明：系統留存日誌紀錄之目的包含程式除錯、行為歸責、稽核取證及法規要求等。記錄身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等，將有助於定期稽核系統行為及資安事件追查。

2. 日誌紀錄包含以下項目 1.識別使用者之 ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型或等級(priority)。5.事件描述

   適用分級：普、中、高。

   說明：日誌紀錄宜考慮包含：1.使用者 ID，不可為個資類型，避免共用帳號之情況。2.時間，系統應設定定期校時，應記錄至微秒等級。3.執行之功能或存取之資源名稱。4.事件類型或優先等級。5.執行結果或事件描述。6.事件發生當下相關物件資訊。7.網路來源與目的位址。8.錯誤代碼，便於事件追查。

3. 採用單一的日誌紀錄機制，確保輸出格式的一致性

   適用分級：中、高。

   說明：系統日誌紀錄應盡可能採用單一的 Log 機制，例如同一伺服器軟體應產出相同格式之日誌紀錄，以便於事件比對與追查。

4. 對日誌紀錄進行適當保護及備份，避免未經授權存取

適用分級：高。

說明：系統產生日誌紀錄後，應定時將日誌紀錄進行遠端備份，並將檔案設定存取權限限制，避免未經授權存取。

3.2.7 會談(Session)管理

1. 使用者的會談階段，設定該帳號在合理的時間(至多 30 分鐘)內未活動即自動失效

適用分級：普、中、高。

說明：會談(Session)機制目的為管理使用者與伺服器之間的連線狀態，通常於客戶端首次連線伺服器即建立一會談識別碼(Session ID)，並將使用者後續於系統中的相關資訊與該會談識別碼關連，以維持使用者相關資訊狀態。使用者於系統中若一段時間未進行活動，系統應有自動機制將該使用者的會談階段設為失效，以避免資安風險。

2. 使用者的會談階段在登出後失效

適用分級：普、中、高。

說明：系統應有手動機制，使用者明確進行登出後，將該使用者的會談階段設為失效。

3. 會談識別碼(Session ID)或使用者 ID 避免顯示於使用者可以改寫處(例如網址列)

適用分級：中、高。

說明：會談識別碼(Session ID)顯示於使用者可以改寫處，則有遭到暴力破解或嘗試猜測合法會談識別碼之可能性，應予避免。

4. 會談識別碼(Session ID)採亂數隨機產生且不可預測

適用分級：高。

說明：為避免會談識別碼(Session ID)被猜測，建議儘量使用各種開發架構(J2EE、ASP.NET、PHP)所提供的內建 Session ID 產生管理方式，而不要自己產生 Session ID ，以確保 Session ID 具隨機性與夠強健而不易被推測。

5. 使用者登入後，重新賦予會談識別碼(Session ID)

適用分級：高。

說明：針對會談識別碼(Session ID)的 Session Fixation 攻擊，攻擊者在目標使用者登入前置換掉其所使用的 Session ID，使用者登入後將取得系統權限，攻擊者利用其已知的這組 Session ID 便可以偽冒成目標。伺服器在使用者初次連結網頁時(通常為首頁)給予 Session ID，登入後若仍採用相同 Session ID 則具有此風險。

3.2.8 錯誤及例外處理

1. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息

適用分級：普、中、高。

說明：系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。

2. 所有功能皆進行錯誤及例外處理，並確保將資源正確釋放

適用分級：中、高。

說明：確保系統所有功能的程式碼，在程式的進入點之後，盡可能採用程式語言的 try-catch 陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的 finally 陳述，確保將該段功能程式碼所使用的資源正確釋放。

3. 具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)

適用分級：高。

說明：系統增加電子郵件或簡訊之通知機制，並就系統錯誤或例外狀況進行等級區分，當嚴重等級錯誤發生時，採用通知機制，使系統管理員或相關人員得以即時得知錯誤發生，進行後續處理。

3.2.9 組態管理

1. 管理者介面限制存取來源或不允許遠端存取

適用分級：普、中、高。

說明：管理者介面通常可執行系統中較高權限的功能(例如權限與人員管理)，其相對風險較高，因此應盡可能不允許遠端存取，僅允許透過內部網路存取，以避免有心人士從外部嘗試攻擊之可能。若有必要允許外部遠端存取管理者介面，應限制特定存取來源 IP，避免全面性開放存取。

2. 作業平台定期更新並關閉不必要服務及埠口(Port)

適用分級：中、高。

說明：就作業系統或平台之安全更新，定期評估、測試與更新。系統上線前，就作業系統或平台預設開啟的服務與埠口(Port)進行檢視與評估，盡可能關閉不必要之項目，並正面表列需要開啟該服務及埠口(Port)之理由。

3. 系統依賴的外部元件或軟體，不使用預設密碼

適用分級：中、高。

說明：表列系統所使用的外部元件與軟體，包含其版本資訊，並檢核確認未有使用預設密碼之情況。

4. 參數設定或系統設定存放處，限制存取或進行適當保護

適用分級：高。

說明：系統參數設定檔案，應設置適當檔案權限，避免被非授權存取。

5. 針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新

適用分級：高。

說明:對系統所使用的外部元件與軟體進行表列,包含其版本資訊。注意相關之安全漏洞通告(透過 CVE Details 網站、廠商安全通告等)，於系統驗收前確認採用之軟體與元件，已使用最新之穩定版本或該版本已排除所有已知安全漏洞。系統上線後，持續定期關注安全漏洞通告，若有相關之安全漏洞發生，評估該系統元件更新之必要性，於系統測試環境進行更新測試驗證後，才於正式環境進行更新。

3.3 技術需求

詳述對此系統之績效(Performance)水準要求、介面需求、資料之安全需求、為方便使用人員易於操作之需求、標準化之需求....等。

3.3.1 現有系統架構與環境說明

3.3.2 未來發展規劃

3.3.3 解決方案之需求

3.3.4 品質水準與測試之需求

3.3.5 安全控管之需求

3.4 環境需求

描述本專案電腦軟體/硬體及網路各項目整合與測試時所應遵循的方式與環境

3.4.1 硬體/軟體之作業環境

3.4.2 硬體/軟體之測試環境

3.4.3 網路作業環境

3.4.4 網路作業環境之測試

3.4.5 非交付硬體/軟體

3.5 管理需求

敘述對專案管理、廠商能力及專案人員之組成....等事項之需求，及對分包廠商之需求。

3.5.1 管理需求摘要

3.5.2 專案組織與人員能力需求

詳述對本專案作業有直接關係之廠商與分包廠商組織成員、及各參與人員能力條件之需求。

3.5.3 專案管理需求

視本專案之規模及性質，詳述對本專案作業程序之需求，及廠商執行本專案作業流程管控、資源管控、品質管控、安全管控、分包管理等工作人員與方法、工具之需求。

3.5.4 需求異動之管理

3.5.5 廠商實績之需求

3.5.6 保固與軟體維護需求

若有教育訓練之需求應詳述地點、對象、場次、人數、材料....等有關之需求。

3.6 交付產品與交付時程

詳述各階段時程應交付之產品、相關文件及其格式，若有特別指定使用之工具應具體說明。(有關軟體開發各階段之文件，請詳如經濟部工業局委託中華民國資訊軟體協會編製的「軟體技術文件指引手冊」)

四、智慧財產權之歸屬

詳述各相關開發之軟體及技術文件等之權利歸屬。一般而言，套裝軟體之智慧財產權皆歸屬於軟體廠商，使用單位僅擁有軟體使用權 。若為全額委託廠商訂製設計軟體之專案，則通常有下列二種方式:

a. 所有權歸委託單位，智慧財產權為廠商所有

廠商交付項目之所有權歸屬委託單位所有，委託單位得基於其內部使用及維護本專案系統之目的，修改或重製原始碼(Source code)或目的碼(Object code)。但為本專案之開發成果及所利用之資料或技術，其智慧財產權仍屬廠商或其原權利人所有，不因交付項目所有權歸委託單位而影響。

b. 所有權歸委託單位，智慧財產權為共有

廠商交付委託單位之產品或文件，其智慧財產權歸由雙方共有，任一方皆得各自單獨使用、收益、處理侵權事務與獲得賠償金，不須他方同意、不須分配利益。惟廠商為開發本專案所利用之資料或技術，其智慧財產權仍屬原權利人所有，不受影響。

五、驗收事項與權責

驗收事項與權責是應用軟體委外服務作業中非常重要的項目。委外單位應詳細說明驗收應交付之產品(如系統分析報告書、原始程式碼、....等。)、交付方式、交付時程、地點、交付產品的確認要件，確認單位，重要查核點及委外單位與廠商間之權利與義務....等。然應用軟體之交付不比硬體，經常會因經驗及立場之不同對事情之認知會有某種程度的差距。因此建議對文件之交付應有樣本作參考，程式之交付也應說明重要之查核點，如建置完成並經功能測試後○○%以上的功能符合原設計功能即同意視為系統交付完成。驗收事項中如有需要使用單位之測試報告時應明確說明負責測試單位....等。一但完成各項產品交付並經測試完成即可進入法定驗收程序。凡此種種應在合約書與 RFP 中詳細說明清楚。

六、建議書製作規定

詳述建議書之格式，裝訂方式、份數、交付地點、截止日期、逾期交付之處置等事項。

6.1 裝訂及交付

例如：

1. 裝訂

・用紙大小尺寸：例如：LETTER SIZE, A4, ...等。

・裝訂方式：以活頁方式裝定成冊。

・份數：一式 X 份。

2. 交付

・截止日期及時間。

・交付地點。

・交付方式。

6.2 建議書內容

視本專案之規模及性質，詳述候選承包廠商需提供之廠商基本資料與經驗能力說明、品質保證能力說明(如品保制度方法、ISO 9000 或 CMM 認證等)、解決方案規劃、建置計畫、專案組織人力說明(包括計畫主持人與主要工作人員之學經歷、實務經驗、技術認證等)、專案管理計畫、交付項目說明、測試驗收計畫、訓練計畫、費用預估….等內容及需檢附之相關證明文件。

附件1　系統安全需求項目查檢表

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
機密性	1.1 機敏資料傳輸時，採用加密機制	V	V	V	通用
	1.2 使用公開、國際機構驗證且未遭破解的演算法		V	V	通用
	1.3 使用演算法支援的最大長度金鑰		V	V	通用
	1.4 加密金鑰或憑證週期性更換		V	V	通用
	1.5 加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制			V	通用
	1.6 機敏資料儲存時，採用加密機制			V	通用
完整性	2.1 於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性	V	V	V	通用
	2.2 針對開放下載的資料，也提供資料之雜湊值(HASH Value)供使用者比對其完整性		V	V	通用
	2.3 具有防範 SQL 命令注入攻擊(SQL Injection)之措施		V	V	通用
	2.4 具有防範跨站腳本攻擊(Cross-Site Scripting)之措施		V	V	WEB
	2.5 驗證網頁重導(Redirects)與導向(Forwards)之目的地在合法名單內		V	V	WEB

	2.6 重要系統資料或紀錄留存雜湊值以確保完整性			V	通用
可用性	3.1 重要資料定時同步至備份或備援環境，並加以保護限制存取	V	V	V	通用
	3.2 採用「高可用性」(High Availability)架構(分散式或叢集伺服器架構)			V	通用
身分驗證	4.1 除了允許匿名存取的功能外，所有功能都必須已通過身分驗證才允許存取	V	V	V	通用
	4.2 身分驗證機制位於伺服器端且採用集中過濾機制(例如使用 Filter 過濾器)		V	V	通用
	4.3 身分驗證相關資訊(帳號、密碼等)不留存於程式原始碼中		V	V	通用
	4.4 確實規範使用者密碼強度（密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元）		V	V	通用
	4.5 使用者必須定期更換密碼，且至少不可以與前 5 次使用過之密碼相同		V	V	通用
	4.6 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 30 分鐘內不允許該帳號及來源 IP 繼續嘗試登入			V	通用
	4.7 身分驗證相關資訊不以明文傳輸			V	通用
	4.8 密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數			V	通用

	及雜湊後密碼				
	4.9 採用圖形驗證碼(CAPTCHA)機制於身分驗證及重要交易行為，以防範自動化程式之嘗試			V	通用
	4.10 重要交易行為要求使用者再次進行身分驗證			V	通用
	4.11 採用多重因素身分驗證(兩種以上驗證類型)			V	通用
	4.12 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令牌(Token)，檢查傳回令牌有效性後，才允許使用者進行重設密碼動作			V	通用
授權與存取控制	5.1 執行功能及存取資源前，檢查使用者授權	V	V	V	通用
	5.2 採用伺服端的集中過濾機制檢查使用者授權		V	V	通用
	5.3 對使用者/角色，僅賦予所需要的最低權限		V	V	通用
	5.4 軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限執行			V	通用
	5.5 除特殊管理者權限外，其他角色或權限無法修改系統中授權資料及存取控制列表(ACL)			V	通用

	5.6 重要行為由多人/角色授權後才得以進行			V	通用
	5.7 具有防範「跨站請求偽造」(Cross-Site Request Forgery，CSRF)攻擊之措施			V	WEB
日誌紀錄	6.1 針對身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行日誌記錄	V	V	V	通用
	6.2 日誌紀錄包含以下項目 1.識別使用者之 ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型或等級(priority)。5.事件描述	V	V	V	通用
	6.3 採用單一的日誌紀錄機制，確保輸出格式的一致性		V	V	通用
	6.4 對日誌紀錄進行適當保護及備份，避免未經授權存取			V	通用
會談(Session)管理	7.1 使用者的會談階段，設定該帳號在合理的時間(至多 30 分鐘)內未活動即自動失效	V	V	V	通用
	7.2 使用者的會談階段在登出後失效	V	V	V	通用
	7.3 會談識別碼(Session ID)或使用者 ID 避免顯示於使用者可以改寫處(例如網址列)		V	V	通用
	7.4 會談識別碼(Session ID)採亂數隨機產			V	通用

	生且不可預測				
	7.5 使用者登入後，重新賦予會談識別碼(Session ID)			V	通用
錯誤及例外處理	8.1 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息	V	V	V	通用
	8.2 所有功能皆進行錯誤及例外處理，並確保將資源正確釋放		V	V	通用
	8.3 具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)			V	通用
組態管理	9.1 管理者介面限制存取來源或不允許遠端存取	V	V	V	通用
	9.2 作業平台定期更新並關閉不必要服務及埠口(Port)		V	V	通用
	9.3 系統依賴的外部元件或軟體，不使用預設密碼		V	V	通用
	9.4 參數設定或系統設定存放處，限制存取或進行適當保護			V	通用
	9.5 針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新			V	通用

檔　　號：
保存年限：

附件3

國家發展委員會　函

地址：10020 臺北市中正區寶慶路3號
電話：(02)23165300 # 6821
傳真：(02)23712936
電子信箱：chlin@ndc.gov.tw
承辦人：林哲豪

受文者：教育部

發文日期：中華民國106年9月15日
發文字號：發資字第1061502464號
速別：普通件
密等及解密條件或保密期限：
附件：行動化服務調查統計表、填寫範例(行動化服務調查統計表.ods、行動化服務調查統計表-範例.pdf)

主旨：請於本(106)年9月30日前函復貴機關(含所屬)行動化服務調查統計表，請查照。

說明：

一、行政院於106年7月28日函頒修正「行政院及所屬各機關行動化服務發展作業原則」部分規定，納入政府機關開發之App須通過App資安檢測後方可上架，並擴大適用對象為行政院及所屬各級機關(構)、國立學校及國營事業。

二、本會業於本年8月31日召開「爭議訊息澄清專區介接機制暨政府App資安檢測作業原則說明會」，說明App資安檢測及績效管考作業方式，請各機關(構)配合上開作業原則進行App開發及管理。

三、為瞭解現行各機關行動化服務績效管理情形及資安檢測先期作業，請依附件格式彙整貴機關(含所屬機關(構)、國立學校、國營事業)行動化服務調查表，並於本年9月30日前函復本會，俾利彙整。

四、請貴機關依經濟部工業局106年2月訂頒「行動應用App基

本資安檢測基準」V2.1，依自行評定App類別於下列時間完成資安檢測作業：

(一)高級：106年12月底前。

(二)中級：107年3月底前。

(三)初級：107年5月底前。

五、本案如有任何問題，請洽承辦人林哲豪(電話：02-23165300 分機6821，電子郵件：chlin@ndc.gov.tw)。

正本：行政院資訊處、內政部、外交部、國防部、財政部、教育部、法務部、經濟部、交通部、衛生福利部、文化部、勞動部、科技部、僑務委員會、中央銀行、行政院人事行政總處、行政院主計總處、行政院環境保護署、行政院海岸巡防署、國立故宮博物院、行政院大陸委員會、金融監督管理委員會、國軍退除役官兵輔導委員會、行政院原子能委員會、行政院農業委員會、公平交易委員會、行政院公共工程委員會、原住民族委員會、客家委員會、中央選舉委員會、飛航安全調查委員會、國家通訊傳播委員會、不當黨產處理委員會、臺灣省政府、臺灣省諮議會、福建省政府、國家發展委員會檔案管理局

副本：電子公文交換章 2017-09-15 13:54:15

填寫範例

國家發展委員會App調查統計表

填表人： 林哲豪　Email：chlin@ndc.gov.tw　電話： 02-23165300 #6821

序號	提供機關	App名稱	上線日期（註1）	最近更新日期(註1)	作業系統	安裝/下載次數(註2)	開發建置成本（單位：元，註3）	每年維護成本（單位：元，註3）	資安檢測分類(註4)	App績效評估(註5)
1	國家發展委員會	e管家Plus	2014-8-1	2017-8-16	●Android ●IOS ○其他：	10,000 - 50,000	220,000	100,000	○初級 ●中級 ○高級	自評: ●維持上架(請具體說明並檢附相關證明文件或下載次數截圖畫面)： 下載次數逾1萬次，且近3個月內持續更新內容(如附件下載次數截圖畫面) ○下架：　年　月。
2					○Android ○IOS ○其他：				○初級 ○中級 ○高級	

◎填表說明：

註1、本次調查係以上架Google Play(Android)、App Store(IOS)或Windows等公眾服務之App，上線日期及最近更新日期無須區分作業系統，以該App上線及最近更新之日期填列。

註2、如該App有不同作業系統，請以下載次數較高者填列。

註3、開發及維護成本以單一App計算，加總IOS、Android及其他各作業系統版本之費用。

註4、依據經濟部工業局106年2月訂頒「行動應用App基本資安檢測基準」V2.1，請依App功能特性機關自行評定所需資安檢測分類：

(1)初級：無連網功能。

(2)中級：具連網功能。

(3)高級：具傳輸個人金融敏感資料或具付費功能。

註5、App下架指標：(1)上架逾1年下載次數未達1萬次以上、(2)系統版本逾1年或內容逾3個月未更新、(3)功能或性質相同。

如App績效符合下架指標，而機關仍需維持上架者，應簽報部會資訊長同意。

e管家Plus

國家發展委員會　工具

3+

★★★☆☆ 256

加入願望清單　安裝

其他資訊

發佈日期	安裝次數	目前版本
2017年8月16日	10,000 - 50,000	2.970
Android 最低版本需求	內容分級	互動式元素
4.2 以上	3 歲以上 瞭解詳情	共用資訊
權限	報告	提供者
查看詳細資訊	檢舉不當內容	國家發展委員會

開發人員
造訪網站
將電子郵件寄到 msg@ndc.gov.tw
隱私權政策

檔　　號：
保存年限：

附件4

國家通訊傳播委員會　函

地址：10052臺北市中正區仁愛路1段50號
傳　　真：02-23433699
聯 絡 人：楊子毅　02-33438423

受文者：教育部

發文日期：中華民國106年8月3日
發文字號：通傳資源決字第10643018800號
速別：普通件
密等及解密條件或保密期限：
附件：中華民國106年度中央政府總預算案審查總報告.PDF(106TM06090_1_0309465472719.PDF)

主旨：為保障身心障礙者資訊取得之權利，立法院決議要求各級政府機關與學校於建置之網站新設或改版時，應依據本會頒訂之「無障礙網頁開發規範2.0版」檢測等級AA以上進行設計，請 查照辦理並轉知所屬。

說明：依據中華民國106年度中央政府總預算案審查總報告辦理，詳如附件P.23-通案決議(三十六)。

正本：總統府公共事務室、行政院資訊處、立法院資訊處、監察院資訊室、考試院資訊室、行政院主計總處、行政院人事行政總處、中央銀行、行政院環境保護署、行政院海岸巡防署、國立故宮博物院、行政院大陸委員會、國家發展委員會、科技部、內政部、外交部、國防部、財政部、教育部、法務部、經濟部、交通部、文化部、衛生福利部、蒙藏委員會、僑務委員會、司法院資訊管理處、金融監督管理委員會、國軍退除役官兵輔導委員會、行政院原子能委員會、行政院農業委員會、勞動部、公平交易委員會、行政院公共工程委員會、原住民族委員會、客家委員會、中央選舉委員會、飛航安全調查委員會、臺北市政府、新北市政府、臺中市政府、臺南市政府、高雄市政府、桃園市政府、新竹縣政府、苗栗縣政府、南投縣政府、彰化縣政府、雲林縣政府、嘉義縣政府、屏東縣政府、宜蘭縣政府、花蓮縣政府、臺東縣政府、澎湖縣政府、金門縣政府、連江縣政府、基隆市政府、新竹市政府、嘉義市政府
副本：中華民國資訊軟體協會(含附件) 電子公文交換章 2017-08-04 01:09:12

附件 5

國立臺灣師範大學單位委外開發系統需求訪談紀錄表

專案名稱：	
訪談日期與時間：	
地點：	
參與人員：	
訪談內容紀錄	
上次訪談後需確認事項	
本次訪談內容紀錄	
下次會議議題	
與會人員簽名	

附件 6

國立臺灣師範大學單位委外開發系統測試驗證紀錄單

專案名稱：				
測試人員：				
測試日期：			測試次數：	
項次	測試功能	輸入/執行	輸出/現象	是否合格
				合格□ 不合格□
				合格□ 不合格□
				合格□ 不合格□

附件 7

國立臺灣師範大學單位

委外開發系統上版記錄與驗證紀錄單

專案名稱：			上版日期與時間：	
上版後測試人員：				
測試日期與時間：			版號是否正確：□是□否	
項次	測試功能	輸入/執行	輸出/現象	是否合格
				合格□ 不合格□
				合格□ 不合格□
				合格□ 不合格□