資訊安全管理制度
(Information Security Management System)
實施程序書
(Implementation Procedure)

安全等級：■普通□限閱 □機密

版次：2.0

生效日期：中華民國 111 年 6 月 21 日

版本修訂紀錄表

文件版本	修訂日期/文號	修訂內容	修訂單位	修訂人	文件管制員
1.0	110 年 5 月 24 日	文件初版	行政室	葉○○	葉○○
2.0	111 年 6 月 21 日	文件二版	主任秘書室	葉○○	葉○○

目　錄

圖 目 錄

壹、 目的

斗六市公所（以下簡稱本所）為強化本所資訊安全管理作業，除遵循上級機關及政府資訊安全管理業務機關(行政院資通安全處)，相關資訊安全作業內容外，並採用國際標準資訊安全管理標準(ISO/IEC 27001)，建立一套適合本所資訊安全防護機制，確保本所資訊安全作業符合相關法令要求外，達到機密性、完整性及可用性之作業要求，使本所資訊安全管理擁有可信賴之服務環境。

貳、 依據

一、 資通安全管理法

二、 國家機密保護法

三、 個人資料保護法

四、 文書處理手冊

五、 **ISO/IEC 27001 (Information technology — Security techniques — Information security management systems — Requirements)**

六、 **ISO/IEC 27002 (Information technology — Security techniques — Code of practice for information security management)**

七、**ISO/IEC 27005(Information technology — Security techniques —Information Security Risk Management)**

八、**ISO/IEC 27006 (Information technology — Security techniques – Requirements for bodies providing audit and certification of information security management systems)**

九、**ISO/IEC 27007 (Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing)**

十、**ISO/IEC TS 27008(Information technology — Security**

techniques — Guidelines for the assessment of information security controls)

十一、 ISO/IEC 27009 (Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements)

十二、 ISO/IEC 27010 (Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications)

十三、 ISO 31000 (Risk management — Guidelines)

十四、 IEC 31010 (Risk management — Risk assessment techniques)

參、 適用範圍

本所全體同仁與相關利害關係人員。

肆、 作業單位

全所各單位

伍、 名詞定義與說明

一、 機密性－Confidentiality

使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

二、 完整性－Integrity

保護資產的準確度(accuracy)和完全性(completeness)的性質。

三、 可用性－Availability

經授權個體因應需求之可存取及可使用的性質。

四、 適法性－Adaptability

符合事件(故)發生時，可採用或遵循之規範(specification)與法律(legal)的性質。

五、 資產－Asset

對組織有價值的任何事物。

六、本所負責人

即本所市長，負責指派資訊安全長協助督導、管理與執行本所資訊安全作業。

七、資訊安全長－chief information security officer

(一) 由本所市長負責指派人員擔任，督導全所資訊安全管理與執行作業。

(二) 審視及核准資訊安全管理制度實施程序書內容。

八、資訊安全管理委員會－Information Security Management Committee

委員由各單位主管擔任成立委員會，除每年定期審視本所資訊安全業務管理與執行概況，於必要時召開資訊安全委員會會議，研討本所資訊安全管理方針。

九、 資訊安全管理小組－Information Security Management Team

(一) 由主任秘書室秘書擔任小組組長肩負管理代表之責，協助資訊安全長，推動資訊安全相關作業，另審視及核准本程序書之相關表單之建立。

(二) 小組成員負責撰寫、增修、登錄、發行、廢止、公告、備份及保管共同性文件、表單(及紀錄)與各項資訊安全管控作業。

(三) 小組成員負責審查各需求單位所擬定之契約並確認契約內容無違反本所應遵循之相關法律規定或傷害本所之權益。

(四) 小組成員負責實施與測試資訊系統業務持續應變演練作業事宜，並於事故發生時進行處理。

十、 資訊安全處理小組－Information Security Processing Team

(一) 由各單位主管擔任，負責各單位資訊安全執行、通報與管理作業。

(二) 各單位主管負責各單位資訊資產審視所選擇適切的控制措施。

(三) 落實各單位受委託保管資訊資產之控制措施暨風險評鑑作業措施確認。

(四) 各單位負責撰寫、增修、登錄、發行、廢止、公告、備份及保管各單位自行使用之資訊安全管理文件與表單(及記錄) 。

(五) 各單位負責委外相關服務需求的提出及適當管理之安全需求擬定與廠商服務相關契約內容、人員資格審查與服務交付之確認。

(六) 各單位負責配合資訊系統業務持續應變演練實施與測試事宜，並於事故發生時配合處理。

(七) 資訊資產管理－Information Asset Management

1. 資訊資產風險擁有者－Risk owner

   由各單位主管擔任各單位所使用之資訊資產管理之責，並兼任資產風險擁有者。

2. 資訊資產負責人－person in principal

   負責資訊資產之平日安全管理責任，包括：選擇適切的控制措施、委託資訊資產保管人實施控制措施及確保被委託的責任是否履行無誤。

3. 資訊資產保管人－user or trustee

   負責落實受委託保管資訊資產之控制措施，以達成資訊資產負責人所委託之保護管理責任。

十一、 資訊安全稽核小組－Information Security Audit Team

由本所政風室主任擔任小組組長，小組人員由政風室成員擔任，負責資

訊安全稽核作業管理。

十二、 個人資料－personal information

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、社會活動及其他得以直接或間接方式識別該個人之資料。

十三、 個人資料檔案－profile information

依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

十四、 業務持續計畫－Business Continuity Plan (BCP)

確保重要業務在遭受重大不可抗力之災害或其他人為破壞時，能夠使其功能迅速有效的回復到正常操作狀況的計畫。

十五、 資訊安全事件－Information security incident

泛指對資訊系統之機密性、完整性或可用性方面造成危害的突發事件。

十六、 個資安全事件－personal security incident

泛指對資訊系統內之個人資料外洩之疑慮造成危害的突發事件。

十七、 文件借閱者－Document borrower

僅限借閱相關文件

十八、 紀錄創制者－Record maker

本所全體同仁與相關利害關係人員，依相關權責，利用本制度內表單，填製資料，使該表單具有內容且具價值之有資料表單稱為紀錄。

十九、 文件之有效性－Effectiveness of documents

取得與使用的文件都能反映該文件的最新狀態（如版本、最新修訂日期以及是否已經廢止等）。

二十、 文件之定義－Definition of documents

(一) ISMS 文件

為達成本所資訊安全政策目標要求，執行某項活動所規定之方法。

(二) ISMS 紀錄、表單

依據 ISMS 文件所敘述內容於必要證據文件化之表單，表單所填寫之實際作業內容謂之紀錄。

(三) 外來文件

外來文件指非由本所自行制訂且有必要列管的文件，例如設備廠商提供之文件、手冊…等均屬外來文件；或自外購買、索取或由網路網站下載相關檔案。

(四) 法律法規文件

由本(中華民國)國經行政院審議三讀通過且由總統公布，行政院頒布執行，謂之法律文件；經本所或上級主管機關核准令頒，謂之法規文件。

二十一、文件之鑑別－Identification of documents

(一) 文件可以紙本文件與電子文件存在。文件包含二個要件：文件主體及相關表單。

(二) 文件之頁首或頁尾，須註明文件名稱、編號、版次及頁次等資訊。

(三) 版本異動，於小數點後累進；重大變更之版本異動，於小數點前累進。

(四) 文件於制訂、修訂、廢止、發行之各項管制過程中，均以文件編號為鑑別依據，並依文件編碼系統編碼管理，文件編號統一由資訊安全小組管理分配，已分配之文件編號不得重複使用。

(五) 資訊安全相關之管制性/機敏性資訊文件須標示【機敏/管制文件，禁

止翻印引用】及【管制文件，需翻印引用請洽本所資訊安全文件管制單位】字樣。

二十二、電腦鑑識－Computer Forensics(CF)

為一種運用科學的技術與方法，對數位證物實施蒐集、分析、鑑定與保存等作為。

二十三、數位證據－Digital Evidence(DE)

對電腦(資訊)系統或設備找尋與案件有關的數位證據之系統化活動或作為，而經此系統化之作為所呈現的證據，可做為法庭所接受之證據。

二十四、電腦病毒－Computer Virus(CV)

是一種在人為或非人為的情況下產生的、在用戶不知情或未批准下，能自我複製或運行的電腦程式。

二十五、行動裝置－Mobile Device(MD)

為口袋大小的計算裝置，通常有一個小的顯示螢幕，觸控輸入，或是小型的鍵盤。

二十六、資訊系統開發、變更、維護管理－Information system development, change, maintenance management

(一) 系統使用人員－System users

資訊系統終端使用者。

(二) 系統需求人員－System requirements

資訊系統因應使用要求所提出使用需求，故系統使用者有時可能也是系統需求人員。

(三) 系統設計人員－System designer

資訊系統接受需求後繼行程式設計開發。

(四) 系統維護人員－System maintenance

已完成開發之系統進行維護之人員。

(五) 系統測試人員－System tester

系統完成開發後進行負載、功能及安全等測試之人員。

(六) 系統版控管理人員－System version control manager

以開發之系統為確保軟體與未修改前之差異，所建立之差異管理作業人員。

(七) 系統變更管理人員－System change manager

依據所提出之系統需求提出軟體變更作業。

(八) 系統更新管理人員－System update manager

因應需求將新修訂之軟體更新之作業人員。

(九) 系統上線管理人員－System on-line management staff

將預計更新之軟體賦予軟體編號及需求更新之內容，之管制作業。

陸、 處理步驟

一、訂定與審視資訊安全政策

(一) 應依據本所組織與業務目的，審慎評估資訊安全作業需求與目標，並確保本所關鍵性(核心)業務持續運作不中斷。

(二) 本所經上級機關核定，屬資通安全責任等級 C 級公務機關。

(三) 各項安全管理規定必須遵守政府相關法令、法規（如：國家機密保護法、檔案法、著作權法、個人資料保護法、資通安全管理法及政府資訊公開法…等）之規定。

(四) 鑑別內部與外部的利害關係人以及參與本所資訊安全保護的程度，並辨識工作人員的職責及權責。

(五) 本所高階主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。

(六) 定期召開高階會議以確保資訊安全維護之整體持續改善。

(七) 定期提供全體同仁資通安全訓練課程，提昇人員資安認知。

(八) 定期訂定資訊內部稽核計畫，檢視本所資訊保護之情形，依稽核報告擬定及執行矯正措施。

(九) 本所全體同仁若未遵守本政策或發生任何違反本政策之行為，將依相關規定處理。

(十) 本所視各項安全執行情況對有功人員予以獎勵。

(十一) 本所各單位之資訊安全專責人員負責資訊安全各項事宜。

(十二) 本所全體同仁皆須遵守本所資安事件通報機制，通報所發現之資訊安全事件或資訊安全弱點。

(十三) 依據資通安全管理法，進行管理面、技術面及認知與訓練，並適當安全管理。

(十四) 為符合本政策目標，應進行風險評估與管理，以有效管理資訊資產面臨之風險，降低風險至可接受範圍。

(十五) 明確規範資訊系統及網路服務之使用權限，防止未經授權之存取動作。

(十六) 本所所有往來供應商皆須簽署保密協議書，並遵守本所資訊安全政策以及相關資訊安全規定，不得未經授權使用或濫用本所各類資訊資產。

二、訂定與審視資訊安全組織管制作業

(一) 資訊安全組織

1. 為確保本所資訊安全管理制度運作，建立「資訊安全管理制度-實施程序書-推行小組成員暨利害關係人名冊(表單編號:DL-ISMS-02_01)」，藉此推行小組進行各項管理作業，推行小組建立說明如下：

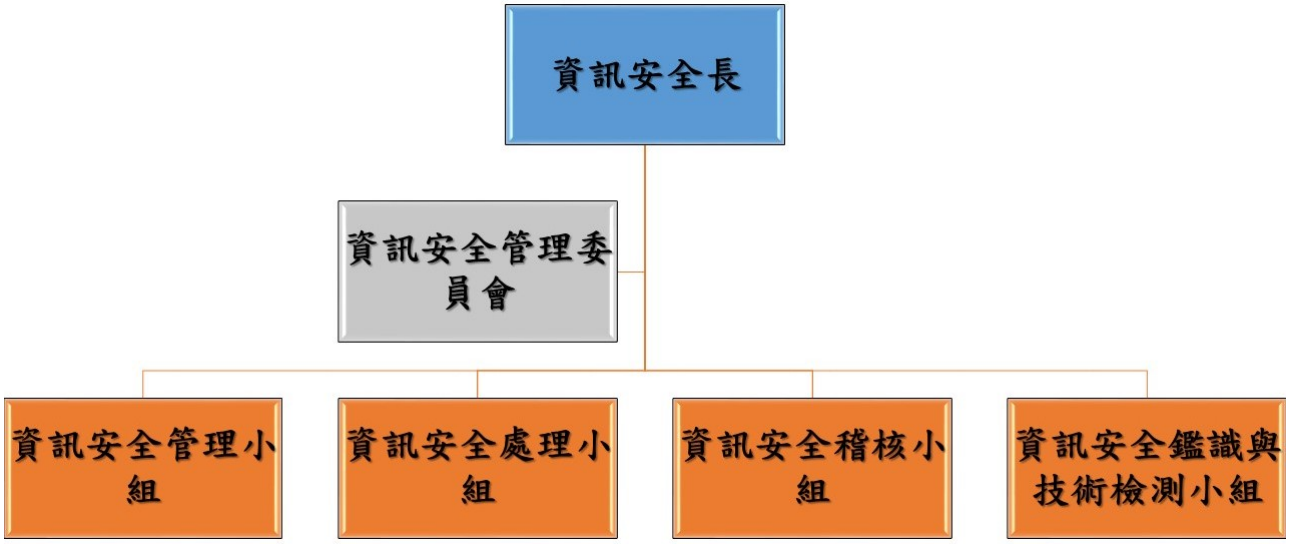

圖 1、組織架構圖

2. 小組成員組織架構說明：詳如本程序書「伍、名詞定義與說明之第七、八、九、十、十一及十二項」。
3. **人員能力需求:**人員資格與能力除依據行政院資通安全法規定與上級機關要求，須取得相關證書及訓練外，應依據本所各項關鍵(核心)作業與利害關係人要求適時修訂。
4. **利害關係人管理：**應依據本所資訊安全管理作業所需(如資訊服務利害關係人/供應商：契約維護廠商、UPS 廠商、發電機廠商、網路供應商、電力公司及消防隊等)，建立「資訊安全管理制度-實施程序書-推行小組成員暨利害關係人名冊(表單編號:DL-ISMS-02_01)」，確保內、外部利害關係人均依據相關需求取得相關資訊。
5. 資訊安全推行小組(即資通安全推行小組，下同)每年至少應開一

次會議(形式不拘) 。

6. 資訊安全推行小組召集人(即本所資通安全長為本所主任秘書，以下同)得視需要，臨時召開資訊安全推行小組會議，會議論內容及資料準備詳如本程序書「伍、管理考核之管理階層審查作業」，並由「資訊安全管理小組」協助備妥相關管理審查作業資料及會議準備作業與記錄。

(二) 專職(責)人力及經費配置

1. 專職 (責)人力及資源之配置

(1) 依據資通安全管理法 C 級公務機關要求，設置資通安全專職(責)人員 1 人。

(2) 資訊安全承辦單位為本所主任秘書室，於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升本所資通安全專業人員之資通安全管理能力。

(3) 本所資安專職 (責)人員專業職能之培養 (如證書、證照、培訓紀錄等應依據資通安全責任等級分級辦法之規定(C 級公務機關要求) 。

(4) 本所資訊安全長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

(5) 本所專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

2. 經費之配置

(1) 本所資通安全推行小組於規劃配置相關經費及資源時，應考量本所資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

(2) 本所於規劃建置資通系統時，應一併規劃資通系統之資

安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

(3) 本所資通安全資源之需求，應配合本所預算規劃期程向資通安全推動小組提出，視整體資通安全資源進行分配，經資通安全長及行政程序核定後，進行相關建置。

(4) 本所資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

(5) 本所資訊需求除上級機關配賦，其餘由本所負責規劃。

三、訂定與審視文件與紀錄管制作業

有關文件管理之程序，應建立「資訊安全管理制度-實施程序書-文件一覽表(表單編號: DL-ISMS-03_01)」可分為文件之新增、異動、發行、廢止與備份。茲分述於下：

(一) 文件之新增、異動與廢止應建立「資訊安全管理制度-實施程序書-文件新增變更廢止核准單(表單編號: DL-ISMS-03_02)」:

1. 共同性文件之增修應由「資訊安全管理小組」負責定期(每年至少 1 次)與不定期之評估。
2. 本所各單位自行使用文件由各單位「資訊安全處理小組」負責定期及不定期之增修訂。
3. **文件之不定期增修與審核時機，包括下列所述**

(1) 新增業務或業務變更時，致使現行文件內容不適用時。

(2) 相關標準或法令修改，致使現行文件內容不適用時。

(3) 定期之資訊安全評估或稽核後發現文件須改善時。

(4) 其他原因致使現行文件內容不適用時。

(二) 文件之發布

須簽奉核准後，以通報方式通知公告，並放置於內部網站，提供本所人員查閱參考，如需列印成紙本參考，除非必要，且經「資訊安全管理小組」同意始可以列印紙本(作業表單除外) 。

(三) 文件之保管

1. 核准發行之文件由「資訊安全管理小組」統一保管，各單位自行使用之文件由相關各單位文件管理人員保管。
2. 文件除非必要，均以電子檔型態存在，且經「資訊安全管理小組」同意始可以建立紙本儲存保管。
3. 文件需依存放媒體機密性等級進行安全管制。
4. 文件保管之版次，至少保存最近 3 個以上版次之文件，過時版本須於文件封面註明「作廢」字樣以示區別。
5. 紀錄（含影本），應保存 2 年，並得依實際需求調整之，惟調整時必須於相關文件載明。監視錄影紀錄至少須保留 3 個月。
6. 共同性記錄由「資訊安全管理小組」負責保管，各單位自行建立之業務管理範圍者，由紀錄創制者自行保管。
7. 紀錄創制者必須將紀錄建檔，以便查閱，必要時得建立索引
8. 紙本共同性文件借閱時，文件借閱者需填寫「資訊安全管理制度-實施程序書-管制文件借閱申請登記表(表單編號：DL-ISMS-03_03)」，向「資訊安全管理小組」借閱，經同意後由「資訊安全管理小組」印製成本紙本文件，且標註借閱者相關訊息(如借閱人、借閱期限及借閱規則等)借閱，文件借閱者歸還文件後進行銷毀作業，各單位自行建立之業務管理範圍之文件借閱時，則須徵得紀錄創制者或其各單位主管同意。
9. 取得外來文件後，應檢查其完整性，由取得外來文件單位提供資訊，交由資訊安全管理小組登錄於「資訊安全管理制度 -

實施程序書-資訊安全外來文件一覽表(表單編號:DL-ISMS-03_04)」。

(四) 文件之報廢

1. 文件之報廢(銷毀)應視其機密等級,採取適當之方式進行銷毀。
2. 文件報廢，統一由「資訊安全管理小組」執行報廢（銷毀）處理作業，由「資訊安全稽核小組」進行報廢（銷毀）監看作業
3. 文件或儲存設備、媒體之銷毀應保留相關核准文件、清冊、銷毀過程錄影或照片、監毀紀錄等。
4. 文件若已過時無效，需廢止者，由文件權責單位通知「資訊安全管理小組」公告廢止。
5. 針對文件機敏資料(含個人資料部分)檔案之刪除與銷毀，應確認機敏資料檔案轉移、刪除及銷毀等流程均已完成,避免資料洩漏。
6. 個人資料刪除或銷毀後，應將「資訊安全管理制度-實施程序書-個人資料權利行使申請表(表單編號: DL-ISMS-03_05)」妥慎保存，刪除及銷毀證據保存期限依『個人資料保護法』及『檔案法』相關規定辦理。
7. 當個資蒐集之特定目的消失、或保存期限屆滿，權責單位應檢討該項業務之相關個資檔案是否有符合『個人資料保護法』之規定，而具有保存之正當性，如無保存之正當性，應立即辦理個資檔案之刪除或銷毀。
8. 當事人請求刪除且符合刪除之相關規定者，應立即進行刪除或銷毀,但因執行職務或業務所須或經當事人書面同意者,不在此限。
9. 因業務移轉相關個資檔案隨案移轉後，本所保存該項業務之個資檔案，經檢討無保存之正當性者，應立即進行刪除或銷毀。
10. 發現違反個人資料保護法規定蒐集、處理或利用個資，應即停止

處理或利用該個人資料，並由各權責單位主動進行刪除或銷毀。

11. 個資刪除或銷毀方式：執行個資刪除或銷毀時，應取得權責主管核可同意，並依個資之形式及載體形式，選用適當之刪除或銷毀方法。

(五) 文件歸屬及種類

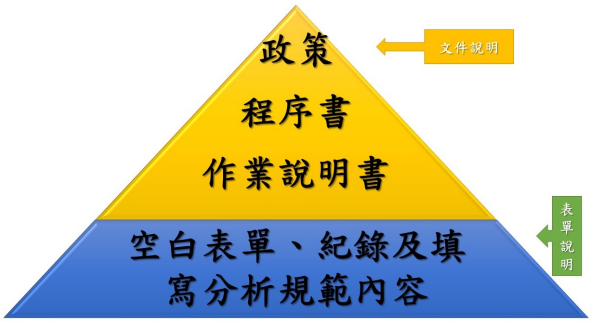

圖 2、ISMS 文件示意圖

(六) 文件編碼方式

1. 資訊安全文件主目錄，如下述

(1) 壹、目的

(2) 貳、依據

(3) 參、適用範圍

(4) 肆、作業單位

(5) 伍、名詞定義

(6) 陸、處理步驟

(7) 柒、政策、程序書、作業說明書、工作指導書、操作說明、計畫書、作業規範、管理辦法(ISMS 文件中文字名稱示意)之修訂及公告。

(8) 捌、 作業表單

2. 文件納入文件管制時應予以編號，編號方式得採用英數字混和方

式編號，不限字數格式，「資訊安全管理制度-實施程序書-文件一覽表(表單編號: DL-ISMS-03_01)」上應註記文件編號。

3. ISMS 文件：DL-ISMS -△△△△，△△△△表示文件英文代號 4 碼，中文名稱部分；XX 政策、XX 程序書、XX 作業說明書、工作指導書、操作說明、計畫書、作業規範、管理辦法、XX 表示文件中文字。
4. ISMS 文件空白表單：DL-ISMS -△△△△-⊿⊿-○○，△△△△表示 ISMS 文件英文代號 4 碼，⊿⊿表示 ISMS 文件處理步驟之章節編號(如本文件處理步驟二、訂定與審視資訊安全組織管制作業；範例：DL-ISMS -02-○○)，○○表示表單、合約、填寫規則之流水號。
5. 使用上級機關所訂定之表單，如原始表單具有編號，除保留原始表單編號外，仍依「本程序書陸、處理步驟三、訂定與審視文件與紀錄管制作業(六)文件編碼方式 6.四階空白表單」編號模式，重新編製本所之專用編號。
6. ISMS 文件記錄：DL-ISMS -△△△△-⊿⊿-○○-□□□-□□-□□，△△△△表示 ISMS 文件英文代號 4 碼，⊿⊿表示 ISMS 文件處理步驟之章節編號(範例：如本文件處理步驟二、訂定與審視資訊安全組織管制作業；標示為；DL-ISMS -02-○○)，○○表示表單、合約、填寫規則之流水號，□□□-□□-□□□第 1～3 碼為記錄製作民國年，第 4～5 為記錄製作月份，第 6～8 碼為記錄製作流水號(範例：如本文件處理步驟二、訂定與審視資訊安全組織管制作業，第一份表單於 109 年 5 月份第 3 次撰寫此份紀錄，標示為；DL-ISMS -02-01-109-05-003) 。
7. 外來文件：DL-ISMS -UN- -△△△△△-○○， 表示非 ISMS

文件流水號 2 碼，△△△△△表示非 ISMS 文件利害關係人(自然人或團體)、供應商、上級機關、其他相關單位 3~5 碼，○○表示非 ISMS 文件利害關係人(自然人或團體)、供應商、上級機關、其他相關單位之流水號(範例：DL-ISMS-UN-01-YLHG-01)YLHG 代表雲林縣政府英文代號。

8. 資訊安全文件版本控管

(1) 發布之文件，版本由 1.0 開始

(2) 文件內容修訂，不涉及參與單位或作業權責之變動者，其版本變更僅調整小數位，如：V1.0→V1.1

(3) 文件內容修訂，若涉及參與單位及作業權責之變動、文件數量之增減者，其版本變更調整整數位，小數位歸零，如：V1.3→V2.0。

(七) 文件及紀錄借閱

1. 資訊安全文件借閱方式(詳如本文件處理步驟三、訂定與審視文件與紀錄管制作業(三)文件之保管 8.紙本共同性文件借閱時，文件借閱者需填寫「資訊安全管理制度-實施程序書-管制文件借閱申請登記表(表單編號: DL-ISMS-03_03)」) 。

2. 資訊安全紀錄得以任何形式之媒體保存於方便調閱之場所，並保持於適切之環境，以防止損壞、變質及遺失。

3. 文件或記錄負責人須將文件或紀錄建檔，必要時得建立索引。

4. 記錄借閱時必須徵得記錄負責人同意。

5. 管制/機敏文件（包括外來文件）之借閱，需填寫「資訊安全管理制度-實施程序書-管制文件借閱申請登記表(表單編號: DL-ISMS-03_03)」，向「資訊安全管理小組」或記錄創作者借閱，有關「資訊安全管理制度-實施程序書-管制文件借閱申請登記表

(表單編號: DL-ISMS-03_03)」由「資訊安全管理小組」或記錄創作者負責保管。

6. 借閱者不得於所借閱的資訊安全紀錄上加以標記或書寫。
7. 借閱者歸還資訊安全文件或紀錄時，紀錄創作者，應於「資訊安全管理制度-實施程序書-管制文件借閱申請登記表(表單編號: DL-ISMS-03_03)」填寫歸還日期並簽字確認已歸還。

(八) 外來文件

1. 外來文件指非由本所自行制訂且有必要列管的文件，例如供應商提供之文件、手冊等均屬外來文件，利害關係人、參考文件、合約，表報等。
2. 外來文件在取得新修訂版或停止使用時，應登錄於「資訊安全管理制度-實施程序書-資訊安全外來文件一覽表(表單編號: DL-ISMS-03_04)」。

四、界定本所組織全景及利害關係者需求與期望

(一) 組織業務宗旨與目標及關注方需要與期望的鑑別

根據 ISO/CNS 27001 第四章組織全景及參考 ISO/IEC 31000 所述，組織內外部環節，藉由彙整組織內人員與相關利害關係者之意見，透過規劃、執行、監督與改進等基本的管理過程，並填寫「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」加以治理，程序說明如下：

1. 在鑑別組織全景時，首先須取得最高管理階層(資訊安全長)對組織業務宗旨與目標的看法與共識。其次，鑑別組織外部關注方及其需要與期望，以及內部關注方及其需要與期望。外部關注方可能包含：上級主管機關、其他行政機關及民眾。
2. 綜整組織業務宗旨與目標及各關注方需要與期望的內容，記載於

「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」。

(二) 資訊系統分類分級暨防護基準等級判定

依據『資通安全責任等級辦法，附表九資通系統防護需求分級原則』為確保本所資通系統防護作業，進行詳細之資訊系統分類分級與評估「資訊安全管理制度-實施程序書-安全等級評估表(表單編號: DL-ISMS-04_03)」並彙整全所資訊系統安全評估後，產生「資訊安全管理制度-實施程序書-資訊系統清冊(表單編號: DL-ISMS-04_04)」，依據所評估之系統防護需求分級並對映至『資通安全責任等級辦法，附表十資通系統防護基準』控制措施構面與措施內容，與本所資訊安全管理制度(ISMS)文件，逐一進行對應與尋求可行之具體措施。

(三) 評估組織全景風險(高階風險)

1. 根據本所已彙整之關鍵活動(核心業務)與使用之資通系統結合內、外部意見及本所現有可用資源，審視本所資訊安全運作方式，擇選可達成之資訊安全應辦事項，作為執行之活動，相關活動填寫於「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」所鑑別出的每一項關鍵活動(核心業務)與使用之資通系統，應根據其「機密性」、「完整性」、「可用性」及「適法性」之要求，進行分析其可能存在的風險，評估之準據「資訊安全管理制度-實施程序書-組織全景風險鑑別未符合可能衝擊情境分析(表單編號: DL-ISMS-04_02)」加以辨別，確認是否納入細部風險評估作業，除依據本規範外，並應考量本所現行狀況及預算等因素。

2. 須納入細部風險評估作業於「資訊安全管理制度-實施程序書-組

織全景風險評鑑表(表單編號: DL-ISMS-04_01)」之「機密性」、「完整性」、「可用性」及「適法性」之「風險因應對策」中標註需進行細部分析作業(包括資訊安全目標、BIA 及資訊資產風險評鑑作業)，並參考本實施程序書「陸、處理原則、五、建立資訊資產分類分級管理作業」進行詳細之評估後，根據相關細部分析特性與可能風險，再深入納管與尋求解決方案。

3. 毋須納入細部風險評估作業，則於「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」之「機密性」、「完整性」、「可用性」及「適法性」之「風險因應對策」中詳述資訊安全控制措施，確保各項「內、外部議題」之作業過程均受控管。

(四) 控制目標、控制措施和因應對策的鑑別

1. 鑑別出的每項風險，決定是否採取適當的因應對策或接受風險，將計畫採取的因應對策及預估殘餘風險值敘述於「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」，並確認各項風險與 ISO 27001 控制條款間之關係，彙整到「資訊安全管理制度-實施程序書-適用性聲明書（SOA）(表單編號: DL-ISMS-04_05)」。

2. 部分無法對應 ISO 27001 控制條款的風險處理對策，亦應妥善分析處置，確實對每一項「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」鑑別出的需求與目標進行風險管理。

(五) 組織全景利害關係人清單與本所執行單位對映

1. 本所各項組織全景風險鑑別後，應逐一填入「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號:

DL-ISMS-04_01)」中「組織全景利害關係人清單」，每項「利害關係者聯絡資訊」與「本所業務或服務或使用系統之執行單位」，其內容包括「利害關係者聯絡資訊」之「負責人員姓名」、「溝通方式」、「溝通頻率」及對至「本所業務或服務或使用系統之執行單位」之「執行服務單位名稱」、「執行服務單位負責姓名」、「執行服務單位聯絡管道」。

(六) 組織全景評鑑紀錄作業

1. 針對上述過程執行，應呈現於「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」，並將整個組織全景風險評鑑過程紀錄，陳報「資訊安全管理委員會」，使得「資訊安全管理委員會」可以清楚地了解本所業務要求以及內、外部議題作業過程的期望，與本所實施 ISMS 範圍的差異，以及可能存在的風險，以期給予最高的注意力及保證程度的等級，提供相關關注方信心。
2. 組織全景評鑑應至少每年審查一次，並在有任何關於業務流程的改變、組織結構變更，或關注方產生新需要或期望時，應修訂「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」。
3. 當變更較為明顯且必要時，應一併修訂「資訊安全管理制度-實施程序書-適用性聲明書（SOA）(表單編號: DL-ISMS-04_05)」。

五、建立資訊資產分類分級管理作業

依據主管機關要求，適當管理本所資訊資產之處理，參考國際標準(如：ISO27005)以最佳實務之方法，建置本所資訊資產分類分級作業 。

(一) 資訊資產分類

1. 定義：資料經過處理後成為有特殊價值的資訊，或以文件形式存

在的資產，例如：註冊商標/著作權、業務資訊、工作相關資訊、機關/單位資訊、組織相關紀錄、使用者資訊、產品資訊、資料庫、測試資料、備份資料、合約內容、系統文件、操作手冊、教育訓練教材、計畫、規範、程序書及其他相關資訊。

2. 分類：本所相關資訊資產依其性質不同，分為 5 類：資訊、軟體、硬體、服務、人員，詳如「資訊安全管理制度-實施程序書-資訊資產分類說明(表單編號: DL-ISMS-05_01)」，並依據資訊資產屬性及單元之代號，簡述如下：

(1) 資訊(Information；IM)

甲、數位文件(Digital document；DDO)

乙、紙本文件(Paper document；PDO)

(2) 軟體(Software；SW)

甲、商業軟體(Commercial software；CSO)

乙、開源軟體(Open source software；OSS)

丙、自行開發軟體(Internal development software；IDS)

丁、委外開發軟體(Outsourcing development software；ODS)

(3) 硬體(Hardware；HW)

甲、電腦設備(Computer equipment；CEQ)

乙、儲存設備(Storage equipment；SEQ)

丙、網路設備(Network equipment；NEQ)

丁、防護設備(Protective equipment；PEQ)

戊、行動裝置(Mobile device；MDE)

己、儲存媒體(Storage media；SME)

庚、通訊設施(Communication facilities；CFA)

辛、監控設施(Monitoring facilities；MFA)

壬、環境設施(Environmental facilities；EFA)

(4) 服務(Service；SE)

甲、資訊服務(Information service；ISE)

乙、通訊服務(Communication service；CSE)

丙、網路服務(Internet service；NSE)

丁、電力服務(Power service；PSE)

戊、環境服務(Environmental service；ESE)

己、監控服務(Monitoring service；MSE)

庚、印刷服務(Printing Service；PRS)

辛、郵遞服務(Mail service；MAS)

(5) 人員(Staff；ST)

甲、編制人員(Formal Staff；FST)

乙、臨時人員(Temporary Staff；TST)

丙、委外人員(Outsourcing Staff；OST)

3. 本所資訊資產之機密等級，應定期審核，視實際需要予以調整。

(二) 資訊資產鑑別

1. 資訊資產鑑別係依據本所「資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)」，表列中各項關鍵活動業務或服務流程，進行更細部資產鑑別作業。

2. 各項關鍵業務或服務流程據以鑑別出細部資訊資產後，作為該資訊資產負責人，並建立「資訊安全管理制度-實施程序書-資訊資產清冊(表單編號: DL-ISMS-05_02)」。

3. 本所各項資訊資產負責人應定期更新與維護所管轄之資訊資產清冊，並陳報本所各組及所屬單位初審後，由資訊管理小組彙整全單位審核。

4. 各組及所屬單位資訊資產清冊，統由推行小組成員項下之資訊安全管理小組專人彙整後，予以統一編號，以確保資訊資產編號及清單之完整性。

5. 為保護本所所管理各類相關資訊資產，各項資訊資產負責人應定期維護所屬資訊資產清冊，並遵守本作業說明書之其他相關規定。

(三) 資訊資產價值鑑別

1. 資訊資產鑑別價值，以關鍵活動業務或服務流程為主軸，由每位作業流程負責人負責審視與其負責之業務相關之資產，以鑑別出資訊資產以及其他與資訊安全管理有關的資產與相對應之負責人員，流程分析方法請參見「圖 3、資產流程分析方法」，透過流程分析方法。

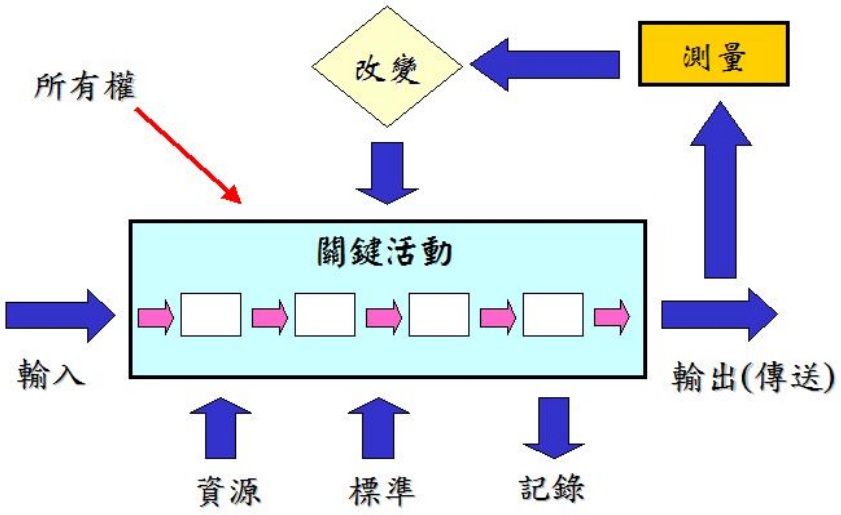

圖 3、資產流程分析方法

(1) 輸入：資訊資產所有人將相關資產資料輸入關鍵活動業務或服務流程中。

(2) 資源：為確保所輸入資料為關鍵活動業務或服務流程所需，需透過所有資源盤點，確保所輸入之資產能有限被關鍵活動業務或服務流程使用。

(3) 標準：所輸入之資產應按照關鍵活動業務或服務流程之標準程序進行檢視，確定資產所產生之價值。

(4) 紀錄：在所有關鍵活動業務或服務流程產生中，需詳細記錄每項資產作業與內容。

(5) 輸出：確認所有關鍵活動業務或服務流程均已完成，並傳送出來，作為關鍵活動業務或服務流程終止。

(6) 量測：透過計量或計數之衡量，確保所輸出之資產關鍵活動業務或服務流程資訊，是否為所需之資產活動。

(7) 改變：經過量測作業後，如有未達關鍵活動業務或服務流程要求者，應再次輸入重新進入關鍵活動業務或服務流程，確保能再次確認與衡量資產作業是否符合標準。

2. 各項資訊資產負責人應鑑別所管轄資訊資產之價值。

3. 部分資訊資產鑑別過程中，可能涉及多項關鍵活動業務或服務流程，應以最高風險關鍵活動業務或服務流程做為評估考量依據。

4. 資訊資產價值詳如「資訊安全管理制度-實施程序書-資訊資產價值評估標準表(表單編號: DL-ISMS-05_03)」應考量資訊資產機密性、可用性及完整性。

5. 首次評估資訊資產機密性、完整性及可用性等級時，無須考量現有之控管措施。

6. 各資訊資產價值為資訊資產之機密性、完整性及可用性評估值取最大值：

資訊資產價值 = MAX(機密性評估值、完整性評估值、可用性評估值)

7. 各資訊資產之價值評估因各類資訊資產之特性可參考以下原則：

(1) 人員資產之價值評估應依據該人員所負責之權責項目評鑑其機密性及完整性為主。

(2) 當相同作業之資料、軟體和硬體資產分別辨識時，資料資產之價值評估以機密性為主要考量，另軟、硬體資產之價值評估主要考量以可用性及完整性為主。

(四) 資訊資產標示及編號

1. 已列入機密等級分類之資訊資產或系統所輸出資料，應明確標示其機密等級，避免其機密性遭破壞。

2. 資料及文件類資訊資產項中，資料所存在之儲存媒體須於明顯處標示可識別之資訊，例如標示與媒體清單相符合的編號，並於媒體清單清楚敘明該媒體內。

3. 硬體類資訊資產應標示本所資產編號，該編號須與設備清單相符合，設備清單須清楚敘明歸屬系統。

4. 資訊資產編號代碼編碼方式詳如「資訊安全管理制度-實施程序書-資訊資產編號代號編碼原則表(表單編號: DL-ISMS-05_04)」如圖 4 所示，共 13 碼：第 1~2 碼為組織代號；第 3~7 碼資產分類代號；第 8~10 碼為資產年號代號；11~13 碼為流水編號代號。

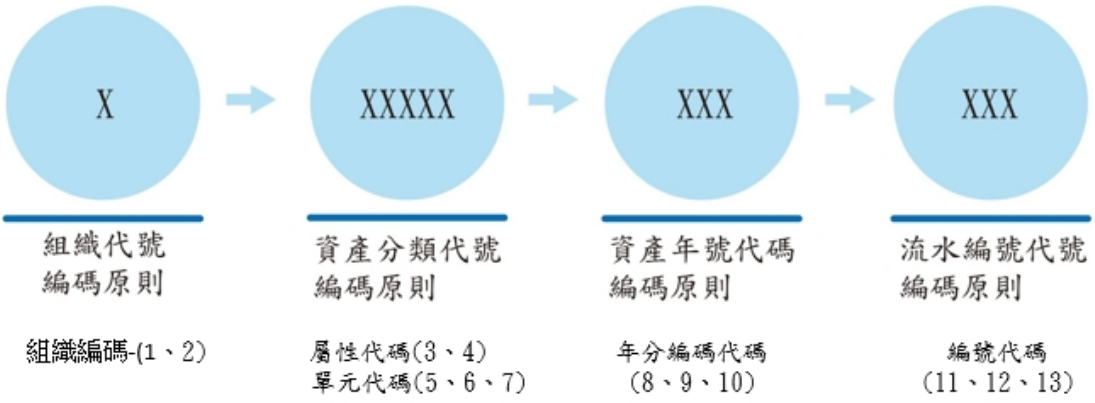

圖 4、資訊資產編號代號編碼原則表

5. 例如觀光課於 109 年購買了第一台全所共用伺服器，編號如下：

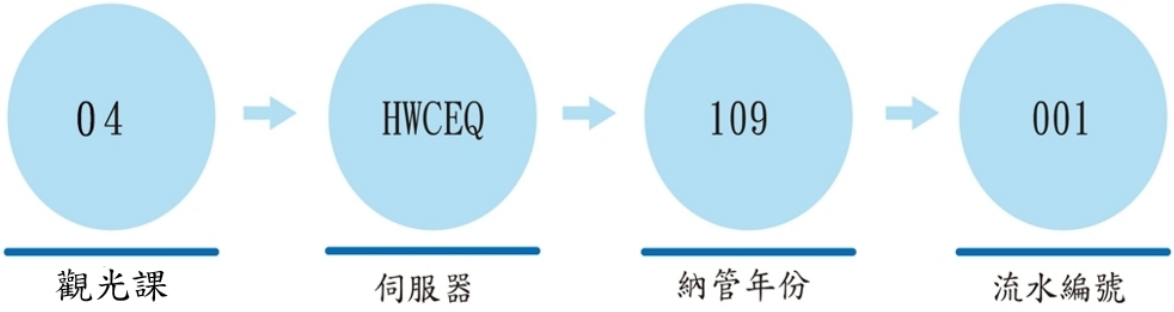

圖 5、資訊資產編號代號編碼原則範例

(五) 資訊資產管理作業

1. 內部資料機密等級以上文件應由負責人妥為保管，避免遺失、毀損，不得擅自攜出、影印及借閱。如契約合約、套裝軟體所附之授權書、使用權證明書等，應指派專人保管。
2. 單位業務機密等級以上文件得禁止使用傳真設備傳送，避免明文資料外洩。如有必要使用傳真系統傳送資訊時，應先以電話確認接收人員到位後始得傳輸。
3. 業務機密等級以上資訊資產應於傳輸與儲存過程加密保護，以防止未經授權的竄改、破壞。如使用電子郵件傳送，需加密處理。
4. 單位業務機密等級以上資料庫檔案應執行權限控管與備份機制。

5. 有關文件、紀錄、相關電子檔控管原則及方式，應依據本程序書「陸、處理步驟第三節、訂定與審視文件與紀錄管制作業」辦理。
6. 有關人員之控管原則及方式，由應依據本程序書「陸、處理步驟第二節、訂定與審視資訊安全組織管制作業」負責辦理。
7. 每年應至少進行一次資訊資產清冊覆核，更新及確保資訊資產清冊的正確性及完整性。
8. 當發生下列狀況時，應實施不定期的覆核，以更新及確保資訊資產清冊之正確性及完整性：
   (1) 有新增、變更或移除資訊資產
   (2) 資訊系統有重大異動
   (3) 作業環境改變
   (4) 單位變革

(六) 資訊資產安全風險評鑑

1. 脆弱點/威脅選擇
   (1) 參照國際標準 ISO/IEC 27005 脆弱點/威脅範例資料與 ISO 31000 風險評鑑標準及各資訊系統可能面臨的脆弱點/威脅，依各資訊資產類別列出一般可能面對的脆弱點/威脅因子，彙整成如「資訊安全管理制度-實施程序書-資訊資產脆弱點/威脅資料表(表單編號: DL-ISMS-05_05)」以做為後續風險評鑑之依據。
   (2) 「資訊安全管理制度-實施程序書-資訊資產脆弱點/威脅資料表(表單編號: DL-ISMS-05_05)」根據不同資訊資產類別定義，分別羅列四類說明如下

   甲、 第一類：為資訊(Information；IM)類屬性，資訊資產脆弱點/威脅選項。

乙、 第二類：軟體 (Software; SW)類屬性，資訊資產脆弱點/威脅選項。

丙、 第三類：硬體 (Hardware; HW)類屬性，資訊資產脆弱點/威脅選項。

丁、 第四類：人員(Staff；ST)/ 服務(Service；SE)類屬性，資訊資產脆弱點/威脅選項。

(3) 依各資訊資產之分類，查照「資訊安全管理制度-實施程序書-資訊資產脆弱點/威脅資料表(表單編號: DL-ISMS-05_05)」為每一項資訊資產選擇所需評估的事件(脆弱點/威脅)類別。

(4) 脆弱點/威脅選擇，依據每一項資訊資產特性，針對機密性－Confidentiality(C)；完整性－Integrity(I)及可用性－Availability(A)等評估價單一值數值高低，以高分項目為基礎依序選擇。

(5) 如機密性－Confidentiality(C)；完整性－Integrity(I)及可用性－Availability(A)等評估價值分數相同，則脆弱點/威脅選擇時，應同列為基礎選項。

(6) 每一項資訊資產脆弱點/威脅選擇，不一定要將資訊資產脆弱點/威脅資料表全部納入選項，可依據資訊資產特性至少選擇一項以上脆弱點/威脅項目。

2. 事件衝擊及發生機率的評估

(1) 為每一項資訊資產所選擇之脆弱點/威脅項目，根據「資訊安全管理制度-實施程序書-事件衝擊及發生機率評估表(表單編號: DL-ISMS-05_06)」，評估脆弱點/威脅事件衝擊程度等級及發生機率可能性等級。

(2) 事件衝擊程度的評估項目，可區分為「業務財務衝擊」、「法

律法規遵循」、「組織聲譽損害」及「個人資料外洩」等四種。

(3) 每種事件衝擊程度的評估等級分為『極高(等級值為 5)』->『高(等級值為 4)』->『中(等級值為 3)』->『低(等級值為 2) ->『極低(等級值為 1)』等五項衝擊評估標準，各自評估後取最高等級為事件衝擊程度評估等級。

事件衝擊程度的評估等級 = MAX(「業務財務衝擊」、「法律法規遵循」、「組織聲譽損害」、「個人資料外洩」)

(4) 事件發生機率可能性的評估等級分為『極高(等級值為 5)』->『高(等級值為 4)』->『中(等級值為 3)』->『低(等級值為 2) ->『極低(等級值為 1)』等五項可能性評估標準。

3. 風險值的計算

(1) 風險值的計算由資訊『資產價值等級值(最高 5 分)』、『事件衝擊程度等級值(最高 5 分)』及『發生機率可能性等級值(最高 5 分)』三個因子構成，以下為其計算方式，風險值的範圍為 1～125。

風險評鑑值＝資訊資產價值等級＊事件衝擊程度等級值＊發生機率可能性等級值

範例：資產價值等級值為 4，事件衝擊程度等級值為 3，發生機率可能性等級值為 3，計算出風險值為 36。

4. 風險評鑑彙整及風險排序

(1) 將上述評估資料彙整後產生「資訊安全管理制度-實施程序書-資訊資產風險評鑑表(表單編號: DL-ISMS-05_07)」。

(2) 每年至少定期更新與維護一次「資訊安全管理制度-實施程序書-資訊資產風險評鑑表(表單編號: DL-ISMS-05_07)」。

(3) 依據風險評估的結果由高而低排列出風險值統計表的次序

並建立「資訊安全管理制度-實施程序書-資訊資產風險值統計表暨資訊安全風險分布圖(表單編號：DL-ISMS-05_08)」，並透過資訊資產風險值統計表繪製出資訊安全風險分布圖。

(4) 可接受風險值的決定

甲、依據「資訊安全管理制度-實施程序書-資訊資產風險值統計表暨資訊安全風險分布圖(表單編號：DL-ISMS-05_08)」由資訊安全長召集資訊安全管理委員，召開資訊安全管理委員會，研討可接受風險值。

乙、於召開資訊安全管理委員會前，先由文件管理小組依本所狀況沿用前次之可接受風險值或依本所組織現況暫定可接受風險值。

丙、可接受風險值決定方式，可以是固定方式，亦可以是浮動方式或是彈性方式。

丁、固定方式：不管本所組織現況、資源情況及人力支援等，採用特定方法論(如 80/20 法則『或稱柏拉圖法則 Pareto Principle』等)決定可接受風險值。

戊、浮動方式：全權考量本所組織現況、資源情況及人力支援等狀態，每年定義可接受風險值。

(七) 資訊資產風險處理、監控與審查

1. 風險改善狀況的後續追蹤

(1) 依據「資訊安全管理制度-實施程序書-資訊資產風險值統計表暨資訊安全風險分布圖(表單編號: DL-ISMS-05_08)」由資訊安全管理委員會，研討確認可接受風險值後，針對風險值超過可接受風險值之資訊資產風險值，審視「資訊安全管

理制度-實施程序書-資訊資產既有防護措施表(表單編號: DL-ISMS-05_09)」對所面臨的脆弱點/威脅與是否有足夠對策與控制可使用。

(2) 對於現行風險值之實施結果，對照「資訊安全管理制度-實施程序書-資訊資產既有防護措施表(表單編號: DL-ISMS-05_09) 」藉以找尋有效之控制措施，依據「資訊安全管理制度-實施程序書-資訊資產既有防護措施識別表(表單編號: DL-ISMS-05_10) 」，據以調整『發生機率可能性等級值』，進而重新調整「資訊安全管理制度-實施程序書-資訊資產重新調整之風險評鑑表(表單編號: DL-ISMS-05_11)」。

(3) 重新調整之風險值計算方式

甲、風險值的計算仍由資訊『資產價值等級值(最高 5 分)』、『事件衝擊程度等級值(最高 5 分)』及『發生機率可能性等級值(最高 5 分)』三個因子構成，惟『發生機率可能性等級值』需先依據「資訊安全管理制度-實施程序書-資訊資產既有防護措施識別表(表單編號: DL-ISMS-05_10) 」識別其可能降低值後，使用已降低值之『發生機率可能性等級值』計算出結果，以下為其計算方式，風險值的範圍為 1～125。

乙、***重新調整風險評鑑值＝資訊資產價值等級＊事件衝擊程度等級值＊(發生機率可能性等級值-可降低級值)*** 。

丙、範例：資產價值等級值為 4，事件衝擊程度等級值為 3，(發生機率可能性等級值為 3-降 1 級值)，計算出重新調整之風險值為 24。

(4) 經重新調整後之「資訊安全管理制度-實施程序書-資訊資產重新調整之風險評鑑表(表單編號: DL-ISMS-05_11)」仍超出可接受風險值，且既有控制措施，不足以控制風險，則思考本所組織現況、資源情況及人力支援等狀態，建立適當之控管措施，產出「資訊安全管理制度-實施程序書-資訊資產風險因應計畫表(表單編號: DL-ISMS-05_12) 」。

(5) 超過可接受風險值之各資訊資產風險管理人於資訊資產風險因應計畫表中填寫有效之因應對策與對應控制項目，並說明風險控管措施之執行辦法及確認風險管理負責單位與風險管理負責人員等，有效有效性評量機制與風險改善完成時間及風險處理之優先性(依據「資訊安全管理制度-實施程序書-業務衝擊分析表（Business Impact Analysis：BIA、表單編號: DL-ISMS-05_12) 」之『失效模式因子評估中所評定之搶救順序等級』結果，進行優先序搶救作業) 。

(6) 執行資訊資產風險因應計畫表中之因應對策後，應預測計算殘餘風險值。

(7) 殘餘風險值預測計算方式，仍以『資產價值等級值(最高 5 分)』、『衝擊程度等級值(最高 5 分)』及『可能性等級值(最高 5 分)』三因子構成，惟『資產價值等級值及衝擊程度等級值』降低可能性較低，故多數資訊資產風險因應計畫表中之因應對策執行，以降低脆弱點/威脅之可能性為主(非絕對) 。

(8) 當殘餘風險值仍超過可接受風險值時，則須填寫殘餘風險值說明。

(9) 在完成殘餘風險值說明後，殘餘風險值仍超過可接受風險值

時，應再思考後續處理作業方式，並填寫實際完成時程，並經評量確認可行之防護後，是否將此因應對策與對應控制項目納入既有防護措施，如有未納入既有防護措施者，應說明未納入既有防護措施者原因。

2. 控制措施的實施必須建立相對應的指標或紀錄，以反映出控制措施實施的狀況及成效，以便於管理階層及相關人員做定期或不定期審視。
3. 為保持組織/各項風險評鑑方法之有效性與適用性，管理審查會議得定期檢討可接受風險值與威脅及弱點評估表之項目，以期確保組織/各組資訊資產均處於最佳保護之下，提供持續不中斷的業務。
4. 每年應至少執行一次資訊安全安全風險評鑑。
5. 當有新增系統、系統有重大異動或作業環境改變時，應執行不定期之風險評估。
6. 當關鍵業務或活動改變或變更時造成資訊系服務異動時所進行的風險評鑑，應修訂於「資訊安全管理制度-實施程序書-資訊資產風險評鑑表(表單編號: DL-ISMS-05_07)」。
7. 另如有涉及風險管理控制措施的新增，亦應修訂於「資訊安全管理制度-實施程序書-資訊資產風險評鑑表(表單編號: DL-ISMS-05_07)」、「資訊安全管理制度-實施程序書-資訊資產既有防護措施表(表單編號: DL-ISMS-05_09) 」及「資訊安全管理制度-實施程序書-資訊資產風險因應計畫表(表單編號: DL-ISMS-05_12) 」。

六、訂定資訊安全管理制度目標及有效性量測

(一) 依據全景分析，將相關風險，選擇其重要關注項目列入「資訊安全管理制度-實施程序書-目標清單(表單編號: DL-ISMS-06_01) 」定期量測。

(二) 每年應依據資訊安全政策及風險評鑑結果訂定資訊安全管理制度目標，並填寫「資訊安全管理制度-實施程序書-目標清單(表單編號: DL-ISMS-06_01) 」。

(三) 每季應對「資訊安全管理制度-實施程序書-目標清單(表單編號: DL-ISMS-06_01) 」的各項目標進行量測，並填寫「資訊安全管理制度-實施程序書-有效性量測表(表單編號: DL-ISMS-06_02) 」以確認目標達成情形。

(四) 實施定期實施量測與監督時，所獲得資訊安全管理制度改善活動之相關資料，並將相關活動作業提請資訊安全管理委員會審視確認，必要時由資訊安全長召集相關資訊安全委員與資訊安全各小組召開會議檢討確認方針。

(五) 配合本所資訊安全管理制度內部稽核作業，定期稽核資訊安全管理制度是否有效地實施和維持，並持續符合標準要求與內部規定。

(六) 確保本所訂定之資訊安全管理制度目標達成，需經量測與監督所獲取之改善資料，找出未達成目標原因，以作為矯正與預防之參考。

七、 審視風險評鑑管理架構與調整適用性聲明

(一) 審視風險評鑑管理架構

「資訊安全管理制度-實施程序書-風險評鑑作業(表單編號: DL-ISMS-07_01) 」，係彙整本實施程序書「陸、處理步驟之四、界定本所組織全景及利害關係者需求與期望及五、建立資訊資產分類分級管理作業」相關風險評估過程，確保資訊安全風險評鑑中高階風險(關鍵/核心業

務與核心系統)均能有效評估，藉由高階風險評估，確認細部風險(資產)之機密性、完整性及可用性與法律遵循程度，詳如「陸、處理步驟之八、資訊安全管理實施」。

(二) 調整適用性聲明

依據風險評鑑及風險防護規劃結果訂定「資訊安全管理制度-實施程序書-適用性聲明書（Statement of applicability，SOA）(表單編號:DL-ISMS-04_05)」,且每年度適時修訂,以符合本所資訊安全作業適用性。

八、 實體及環境安全管理

保護本所電腦、辦公室及行動辦公作業與週邊設備，降低環境之威脅及未經授權存取系統之機會，以達成實體及環境安全控管的目的。

(一) 電腦機櫃管理

1. 資訊資產裝載與拆離之安全管制如下：
   (1) 電腦設備、資料或軟體，未經授權不得裝載機櫃內。
   (2) 電腦設備拆離機櫃與裝載應予記錄，且設定裝載期限，並檢查裝載之電腦設備。
2. 往來利害關係人(供應商)如需開啟電腦機櫃作業，須由本所人員陪同或監督。
3. 實體環境要求
   (1) 電源供應
   甲、應建置預備電源或使用不斷電系統,應定期檢查、測試。
   乙、應考量不斷電系統失效後之緊急應變處理措施。
   (2) 電纜安全
   甲、電力及通信電纜線應予保護，防止損壞或資料被竊取。
   乙、使用明確可識別的電纜線與設備標示，減少處理錯誤。

4. 資訊設備使用管制

(1) 行動裝置管制

甲、應安裝防毒軟體並啟動連線時即時主動更新，以保持病毒碼為最新狀態。

乙、不得安裝與業務無關的軟體（包含非法軟體與來路不明之軟體）。

丙、與外部其他電腦（或攜帶型儲存設備）交換資料時，必須先經過掃毒。

(2) 可攜式儲存媒體

甲、檢查確定無電腦病毒等足以妨害系統因素後始得使用。

乙、嚴禁將機密資訊儲存至可攜式儲存媒體，如有特殊業務需求，應經單位主管同意並採取加密防護。

丙、可攜式儲存媒體用畢後，應立即清空機密資訊。

丁、與個人業務相關的機密資訊儲存於可攜式儲存媒體時應加密處理，不得以明文直接儲存，避免遺失或遭竊。

(3) 設備安置地點之保護

甲、設備應安置在適當地點並予以保護，以防止遺失、損害、竊盜或未經授權存取設備之機會。

乙、應評估火災、水災、灰塵、震動、電力供應等可能之風險及防護。

丙、人員未上班或無人看管時，機房門應予閉鎖。

丁、機櫃內嚴禁存放易燃物品及未經核准之其他物品。

(4) 設備安全管制

甲、應妥善維護資訊設備，以確保設備之完整性及可用性。

乙、設備維護只能由授權之維護人員執行，並留存紀錄。

丙、設備需送修時，應採取適當之控制措施。(例如：將內部敏感性之資料清除)。

丁、新設備上線前應先進行測試。

戊、設備維護作業，應填寫「資訊安全管理制度-實施程序書-維護紀錄表(表單編號: DL-ISMS-08_01)」。

(5) 外部設備之安全管制

甲、設備置放在外部時，應考量資訊安全管理之要求及符合相關授權之程序，以維持與本所內部設備之安全水準。

乙、未採取安全措施(如個人電腦防毒)，不應在外部使用。

(6) 周邊設備安全管制

甲、應明確界定那些週邊設備須列為安全管制之對象，並視所保護資產之價值，建置相關安全機制。

乙、支援資訊作業之相關設施如影印機、傳真機等，應安置在適當之地點，以降低未經授權人員進入管制區之風險，減少敏感性資訊遭破解或洩漏的機會。

丙、合適溫度定為 8℃（冬季）～40℃（夏季）之間超過 40℃開啟風扇進行扇熱作業。合適溼度定為 40%~75%之間，超過 75%開啟除濕機，進行除濕作業。

丁、設備異常時應立即處理，並將問題描述與處理情形，並填寫「資訊安全管理制度-實施程序書-維護紀錄表(表單編號: DL-ISMS-08_01)」。

(二) 辦公室暨行動辦公管理

1.使用桌面應實施淨空政策，減少文件或資料之遺失或遭竊。

2.機密等級「敏感」以上資訊，不使用或下班時應予上鎖。

3.個人電腦及電腦終端機不再使用時，應登出、鎖定螢幕或以其他控制措施保護。

4.列印機密等級「敏感」以上資訊，應立即取走。

5.文件及外接式儲存媒體在不使用時，應存放於桌櫃內，如屬機密性及敏感性資訊，應上鎖或置於有防護功能之設備內。

6.個人資訊設備管理

(1) 個人電腦使用要求

甲、本所同仁於提供服務所需之個人電腦桌上型(筆記型)電腦，應滿足下列控制措施以確保設備之安全。

I. 電腦開機時須輸入密碼(或者使用生物特徵辨識)確認後，始可登入系統。

II. 電腦應設定螢幕保護裝置，等候時間不得超過 15 分鐘，逾時將以密碼保護。

乙、本所同仁於公務之個人(筆記型)電腦，若需處理敏感或個人資料得採下列控制措施以確保設備安全：

I. 使用加密的硬體或軟體設備，以保護所保有之敏感或個人資料。

II. 電腦使用者密碼，必須符合複雜性密碼原則。

III. 暫時離開座位時應將畫面鎖定。

IV. 得使用電腦鎖：抽離時上鎖、插回後輸入密碼解鎖。

(2) 可攜式儲存媒體使用要求

甲、隨身碟、數位錄音筆、數位相機與記憶卡等儲存媒體，於使用完畢後清空儲存的資料，以避免民眾資料外洩。

乙、盡量避免可攜式硬碟或可攜式燒錄器之使用，若須將資料備份於可攜式硬碟中，應對個資敏感資料進行加密。

丙、無線網卡，使用前得先經過本所同意，並以連結本所開放的無線網路區域(需輸入驗證碼)為原則，以避免敏感資料於無安全性的無線網路區域傳輸過程中遭受竊取，如有傳輸必要時需先將敏感資料加密後始得傳輸。

丁、可攜式儲存媒體的維修與再利用前，須進行資料清除。

戊、可攜式儲存媒體的銷毀，原則上以實體銷毀為主。

(3) 個人資訊設備操作

甲、軟體使用

I. 作業程式之漏洞修補必須常保持最新的修補狀態，以避免遭受到系統漏洞的惡意攻擊。

II. 防毒軟體必須常保持最新版本，以避免遭受到病毒或木馬等惡意程式的攻擊。

III. 人員應使用合法版權或 Freeware 軟體，避免交換使用或下載來路不明之軟體、資料。

乙、資料傳輸

含有個資的資料傳輸應使用適當方法(如使用 7z、ZIP 或 RAR 壓縮並加上密碼)加以保護後始得傳輸，加密檔案與解密的密碼應分別使用不同途徑進行資料之交付。

丙、電腦內資料之保存

相關的文件或資料應妥善保存於電腦中，必要時得使用加密機制保護資料。

丁、個人資訊設備之查核

應定期或不定期使用「資訊安全管理制度-實施程序書-個人資訊設備查核表(表單編號: DL-ISMS-08_02」抽查個人資訊設備之符合性。

九、 存取控制

保護本所資、通訊系統與網路作業，降低來自網路之威脅及未經授權存取系統之機會，以達成資、通訊系統與網路控管的目的。

(一) 網路存取管制

1. 網路區隔與強制路由存取路徑管控

(1) 為管制網路存取，於系統對外存取應設置防火牆或代理伺服器，強制區隔安全防護網段，並限制網際網路的存取方式。

(2) 主機服務系統與使用者端採用 VLAN 隔離網段或採用各自獨立之網路集線交換器(SWITCH HUB)，確保伺服器安全。

(3) 網路服務連結申請經核准後，申請人應注意使用期間之必要性，遇有系統續用、變更、停用或使用屆期時，應主動申請網路服務續用、變更或刪除。對於限期之網路服務連結申請單應採列管措施，逾期則關閉網路服務，不另行通知；對於職務異動或服務內容變動者，應主動提出申請變更，查有非必要對其開放之網路服務時，應通知後取消該網路服務。

2. 無線網路存取

為防護本所資訊安全管理制度實施範圍的安全，採用密碼認證通過後使得使用無線區域網路。

3. 外部存取

(1) 本所同仁如因業務特殊需求，需於防火牆對外開放特殊服務（如遠端登入或檔案傳輸等），在不影響本所網路安全條件下（如採用 VPN tunnel、SSH 技術），得提出「資訊安全管

理制度-實施程序書-系統服務連結申請表(表單編號:DL-ISMS-09_01)」經核可後設定防火牆權限開放。

(2) 非本所同仁或本所協力供應商，於外部存取服務如非有迫切的作業需求，應盡量避免常時性的開放，僅於必要時以電話聯繫確認後作暫時性開放，使用結束後即予以關閉。

(3) 提供外部存取服務時，須考慮外部作業的安全性，至少應確保相關資訊於遠端的存取、處理及儲存的機密性與安全性。

(二) 系統作業存取控制

1. 帳號管理

(1) 帳號名稱不應帶有足以辨識使用者權限的資訊。

(2) 系統管理人員自擔任該角色時起自動具備管理者帳號權限，無須提出申請。(包含主機、資料庫及應用系統)。

(3) 本所同仁到/離(調)退職或職務異動時，如需申請帳號權限，提出申請，辦理離(調)退職時，應填寫「資訊安全管理制度-實施程序書-帳號申請(刪除)單 (表單編號:DL-ISMS-09_02)」，由主任秘書室協助建立，或依系統性質，由各業務負責單位直接建立。

(4) 系統只允許必要帳號存在，非必要帳號應刪除，特別是客用(guest)與匿名(anonymous)帳號一定要取消其登入之權限。

(5) 非主任秘書室人員，需使用系統特殊權限時，須經本所資訊安全長同意。

(6) 系統軟、硬體維護廠商承接本所維護案時，得填寫「資訊安全管理制度-實施程序書-帳號申請(刪除)單 (表單編號:DL-ISMS-09_02)」申請帳號，該帳號不得具有系統特許權限，專案結束時，亦由專案承辦人員填寫「資訊安全管理制

度-實施程序書-帳號申請(刪除)單 (表單編號: DL-ISMS-09_02)」帳號刪除。

(7) 使用者填寫的「資訊安全管理制度-實施程序書-帳號申請(刪除)單 (表單編號: DL-ISMS-09_02)」為機敏性資料，管理人員須妥善保管。

(8) 配賦使用者帳號或特殊帳號權限時，應賦予最小作業權限。

(9) 系統的特殊權限（如 administrator、root、資料庫管理者等系統軟體管理者帳號之權限）應僅授權予必要之維護人員。

(10) 主任秘書室每年應請各系統業務管理單位清查使用者帳號，並填寫「資訊安全管理制度-實施程序書-帳號清查紀錄表(表單編號: DL-ISMS-09_03)」，確保使用者帳號資料之正確性與使用必要性，辦理帳號取消、停用或權限調整，清查結果送資訊安全管理小組存查。

2. 系統保全與使用者身分鑑別

本所提供之資訊服務應採帳號或個人憑證認證身分，始提供端末使用者登入，禁止竊取使用他人帳號，如經查獲，由資訊安全管理小組提交資訊安全管理委員會裁決。若為本所委託之維護廠商，除要求維護廠商依合約要求辦理，並更換維護人員。倘因此危害本所資訊安全情事，將依相關法律規範，提請訴訟。

3. 自動離線的保護

本所建置之資訊系統應設定自動離線或桌面鎖定保護(包括系統畫面須有登入者帳號、時間等訊息)，非本所建置系統，依建制單位設定使用，如有需要，由各系統業務單位提出，由本所主任秘書室協助與系統建置單位資訊單位溝通。

4. 連線作業時間的限制

本所建置之資訊系統因業務需要，不限定連線作業時間，應由相關使用單位及業務單位負責人，統一申請，由主任秘書室彙整後，提交資訊安全管理小組進行初步審查，再提交資訊安全管理委員會確認審查，審查解果確認後，再依此程序回復申請單位。

(三) 其他存取控制事項

1. 資、通訊系統之存取控制須遵循本所業務持續運作及資訊安全需求之相關授權標準核可，方可存取本所相關資、通訊系統服務。
2. 資、通訊系統之存取控制須合乎本所業務持續運作需求，並依工作性質與職務授予。
3. 資、通訊系統管理人員依使用者之差異設計職務群組(課室)，以利權限之控管。
4. 使用者須善盡保護個人通行碼之責任，不得將個人登入之身分識別與登入網路之帳號、密碼交付他人使用。
5. 帳號及存取權由各資、通訊系統管理人，每年定期清查使用者之權限，確保資訊系統未遭非法或不當使用，並依情況停用或刪除重覆或閒置的使用者識別碼。
6. 使用者於作業完成後，或需離開工作場所時，應即登出系統或離開作業畫面，並進入加密螢幕保護程式後，再離開工作場所。
7. 應用系統存取權限設定應基於使用者業務需求授與權限。
8. 本所公務用之行動式電腦設備、平板電腦及智慧型行動裝置等應適當使用、保管及處理，防止未經授權取用、破壞及資料遺失。
9. 個人之行動式電腦設備、平板電腦及智慧型行動裝置等，未經許可，禁止存取本所資、通訊系統與銜接本所內部網路節點。

十、 系統獲取、開發及維護管理

保護本所有效管理系統與軟體開發、變更維護等作業，並提供自行維護

系統之資訊系統業管人員或委外維護的承包廠商進行資訊系統軟體變更維護，降低開發成本、改善開發時程及提昇系統品質

(一) 資訊系統安全要求

1. 資訊系統作業環境要求

(1) 宜分隔開發、測試及作業設施，以降低對作業系統未經授權存取或變更的風險。

(2) 輸入系統之資料，應在事前檢查，以確保資料之完整性。

(3) 系統內部之作業，應建立驗證資料正確性之作業程序，避免因系統處理錯誤或是人為因素而使資料遭受破壞。

(4) 系統資料輸出宜經確認，以確保儲存於系統內之資訊，與列印報表內容一致性。

2. 程式碼安全要求

程式碼比對檢查（code review）

(1) 資訊系統程式碼比對檢查（code review）的範圍，至少應包括使用者帳號、資訊系統稽核日誌(Audit log)（資訊系統負責人得視日誌的重要性選擇審查範圍）及機關標示為機密等級以上資料之存取與處理之程式。

(2) 資訊系統委外開發/維護時，於委外合約中應要求資訊系統開發/維護廠商就範圍內之程式碼進行審查並留下紀錄。

(3) 資訊系統上線前，資訊系統負責人應檢查資訊系統開發/維護廠商之程式碼審查紀錄，視需要以抽查方式進行一部分程式碼審查，確定檢查結果沒問題，始可辦理上線申請。

(4) 對於已上線之資訊系統，於程式碼變動時，依前述規定辦理程式碼審查工作。

(二) 資訊系統開發程序

資訊系統開發專案應依循軟體發展的模型架構，進行系統分析、系統設計、程式撰寫、單元測試、系統整合與測試及系統安裝建置等相關步驟，逐步發展，並留下資訊系統發展各階段相關文件。

1. 系統安全需求規劃

(1) 當原定功能需求、設計方式或工作產品有所變動，由業務單位或系統業管人員填寫「資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號: DL-ISMS-10_01)」提出申請，必要時，得檢附會議紀錄、簽、函、電子郵件或合約書。

(2) 新發展的資訊系統，或是現有系統功能之強化，應在系統規劃之需求階段，即將安全需求納入系統功能。

甲、除系統自動執行的安控措施，亦可考量人工執行安控措施;在採購套裝軟體時,亦應進行相同的安全需求分析。

乙、系統的安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，對機關可能帶來的傷害程度。

丙、作業系統更新前應評估其對應用系統造成的影響，或安全問題，變更後檢查與測試在作業系統上之核心系統是否正常運作。

2. 應用系統之安全

(1) 宜分隔開發、測試、及作業設施，以降低對作業系統未經授權存取或變更的風險。

(2) 系統開發應針對容量與資源預作規劃和準備，以確保有足夠的容量和資源，以符合系統所需的環境。

(3) 輸入系統之資料，應在事前檢查，以確保資料之完整性。

(4) 系統內部之作業，應建立驗證資料正確性之作業程序，避免因系統處理錯誤或是人為因素而使資料遭受破壞。

(5) 應於系統開發階段，透過風險評鑑方式，判斷應用系統是否需使用密碼技術，以鑑別與保護訊息的完整性。

(6) 系統資料輸出宜經確認，以確保儲存於系統內之資訊，與列印報表內容一致性。

3. 開發環境之安全管理

(1) 資訊系統開發應於專屬之開發環境中進行，並與線上服務中之業務資訊系統隔離。

(2) 對應用系統原始程式之存取，廠商應建立嚴格的安全管理。

(3) 廠商於資訊系統開發過程中，所須其他廠商產出之相關軟體套件於採用前應確認其安全性無虞。

(4) 應避免使用真實資料進行測試，使用之前宜移除或修改敏感資料內容，使其無法辨認。

(5) 套裝軟體不宜做修改，如有修改之必要，應事先做好風險評估，並經單位主管核可。

4. 系統變更及維護環境之安全

(1) 系統變更前須進行測試，測試內容至少應包含程式的功能符合性、資訊安全保護能力，並填寫「資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號：DL-ISMS-10_01)」(如為利害關係人/供應商維護資訊系統，本單可由廠商適當之文件(如表單、執行紀錄或測試報告書)取代。

(2) 測試應在專屬環境進行，禁止在業務系統上進行測試，測試項目宜包括可用性、安全性、效果的測試，以及使用者便利

性；對於因緊急維護狀況所變更之程式，應於事後將執行內容書面化以利追蹤及查核。

(3) 資訊系統管理人員依申請單進行需求變更，視需求完成測試後，正式上線前須先行填製「資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號：DL-ISMS-10_01)」，奉准後方可上線執行。

(4) 原始碼建構管理

甲、資訊系統委外開發/維護廠商於開發完成遞交原始碼或物件程式碼，應配合本所之軟體版本控制系統(如：SVN Server)進行控管，對本機關委託進行維護之資訊系統軟體程式碼的版次及內容需填寫「資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號：DL-ISMS-10_01)」，進行妥善的管控。

乙、自行開發維護之資訊系統，開發單位應管理程式原始碼的版次、內容及變更，每次應用系統程式變更時應將相關程式碼納入控管，確保程式碼安全，避免誤用或竄改。

(5) 金鑰管理

資訊系統/服務如採用憑證金鑰的加密技術者，應對金鑰採取適當的保護措施；伺服器上之金鑰如為檔案形式存在，則應對伺服器之金鑰檔案存取權限作適當保護，並作適當的備份保管（例如：將伺服器金鑰備份燒錄光碟後以機密文件歸檔保管），如係以韌體形式存在於電腦系統時，則僅需保護其實體存取之安全。

5. 資訊系統資料之安全

本所於導入新的技術或資訊系統時應對個人資料進行下列保護

(1) 資訊系統之測試

資訊系統負責人應對測試資料提供下列保護措施：

甲、避免提供涉及個人隱私之真實資料進行測試。

乙、若無法避免於測試環境使用真實資料進行測試工作，需經授權後始能進行。惟資訊系統負責人應監督系統開發維護廠商在完成測試後，立即要求清除測試資料。

丙、使用真實資料進行測試工作之前宜移除或修改敏感資料內容，使其無法辨認後，始得進行相關測試。

丁、真實資料之複製情形應予以紀錄，以備日後稽核之用。

(2) 資訊系統之個資安全要求

資訊系統獲取於開發時應確保下列個資安全要求被滿足：

甲、依照其存取權限應提供不同之程式畫面，如資料輸入人員僅能檢視與其權限相符之欄位，審核人員或權責主管可以檢視該案件當事人之所有欄位。

乙、查詢或列印含有個人資料之欄位時，應由系統自行保留稽核軌跡並由權責主管或稽核人員定期審查其適切性。

丙、系統應定期產生稽核報表，由稽核人員施行資料安全稽核機制以確保個人資料之安全。

丁、查詢含有個人資料之欄位應採用遮蔽之技術，避免詳細之個人資料遭受不當人士抄錄或以其他方式進行保存，若因業務需要需完全檢視其個人資料，應透過權責單位主管之帳號執行，並於需求結束後應立即登出此帳號含有個人資料之資訊系統檔案應須確保資料之安全。

十一、 人員安全管理暨教育訓練

規範本所全體同仁及利害關係人/供應商之安全管理及教育訓練，減少人員因資訊安全認知不足所引發之資安事件。

(一) 同仁遴用之安全評估

1. 本所全體同仁之工作職責須使用資訊資產者，應予以適當安全評估並以書面方式清楚定義，並簽屬「資訊安全管理制度-實施程序書-資訊安全保密通知書(表單編號: DL-ISMS-11_01)」。
2. 到職時應遵守本所相關管理規範，並克盡保密之責。
3. 本所全體同仁及利害關係人/供應商，於業務上所獲知之資訊，非經本所業管單位主管授權不得對外透露。
4. 利害關係人/供應商執行/駐點人員均須簽署「資訊安全管理制度-實施程序書-利害關係人/供應商執行人員保密同意書(表單編號: DL-ISMS-11_02)」，應與合約共同保存於檔案室，並由檔案室負責統一保管。如利害關係人/供應商人員有異動或臨時作業時，應另簽署「資訊安全管理制度-實施程序書-利害關係人/供應商執行人員保密同意書(表單編號: DL-ISMS-11_02)」，並交由業務負責單位負責保管。

(二) 機密維護之責任

1. 本所全體同仁及利害關係人/供應商使用本所資訊資產者，應依相關法令、法規之規定落實機密維護責任。
2. 約聘僱條件或契約有所變更時(尤其是離職或是約聘僱契約終止時)，應重新檢討機密維護責任約定是否妥適，以利下次約聘僱時能適當調整其契約。
3. 各單位主管，應負責督導所屬同仁依據本所資訊安全制度相關規範執行資訊作業安全，防範不法及不當行為。

4. 違反本所資訊安全實施程序書要求者，應依「公務機關所屬人員資通安全事項獎懲辦法」處置相關違紀人員。
5. 各單位合約中須訂定利害關係人/供應商人員違反本所資訊安全之要求處理規定，並擬定於委外合約中。
6. 本所新進用與無經驗的同仁，授權於敏感性資訊系統執行存取作業時，應由各課室主管指派專人輔導。
7. 本所全體同仁禁止使用違反智慧財產權相關的資訊資產。其違反者，應負相關的法律責任。
8. 各單位擁有最高權限之系統管理員、可存取機密等級「敏感」以上資訊資產者，或配賦特別存取權限之同仁，須專人列冊並加強控管。

(三) 同仁個人資料蒐集、處理及利用要求

1. 人事單位發給面試通知時僅能保留求職者之姓名、連絡電話及電子郵件地址。
2. 求職者於面試前應閱讀面試個人資料上之相關告知內容，同意後始得繼續填寫並作為後續面試之依據。
3. 本所所蒐集之求職者資料僅作為面試或任用後轉為人事管理使用。未取得任用之求職者資料，依告知之使用期間進行個人資料之使用，結束後依本所銷毀時程統一進行銷毀。

(四) 資訊安全教育訓練

1. 為提升本所全體同仁之資訊安全意識與知識，每年編列資訊教育訓練經費，規劃資安教育訓練課程，或派員接受外單位辦理之專業資安課程，以提升同仁之資訊安全知識及警覺意識，降低人為錯誤、故意或誤用資訊之風險。
2. 針對不同層級同仁，進行適當的資訊安全教育訓練，其內容包括：

(1) 本所資訊安全政策

(2) 資訊安全法令規範

(3) 資訊安全作業管理程序

(4) 安全責任

(5) 資訊系統之安全防範或安全資料交換

(6) 個人資料、機密性或敏感性資料之保管

(7) 資訊資產、個人資料檔案與資訊安全管理制度正確使用方法

(8) 緊急應變處理程序

(9) 其它資訊安全相關議題

3. 規劃資訊安全教育訓練，於課後實施學習評量，評估訓練成效。
4. 接受外單位訓練之同仁受訓完成後，得視業務需要，辦理宣導說明會，以加強同仁資訊安全知識，促其遵守資訊安全規定。
5. 辦理資訊安全教育訓練，應保存教育訓練之相關紀錄，作查核用。
6. 在同意及授權使用單位存取系統前，應教導使用單位登入系統的程序，以及如何正確操作及使用軟體。

(五) 職務終止或變更

1. 同仁於離調職、合約或協議終止時，應歸還其所擁有的本所資產。
2. 同仁對資訊資產的存取權限，於離調職前、合約或協議終止前，或職務異動時，其權限均應予以移除或調整。
3. 同仁離調職或職務異動時，依據人事室離職作業程序辦理職務交接，主任秘書室承辦人應即取消其相關權限，並查核其所領用之資訊資產是否完成移交或繳回，防止人為舞弊或設備損失。

(六) 本所資訊安全訓練如與利害關係人有關時，則依利害關係人相關法規要求之時數辦理。

十二、 資訊設備軟、硬體管理

(一) 資訊系統管理

1. 系統軟體安裝管理

(1) 系統中啟動的應用服務，如非必要，不得以 Admin、Administrator、sa 或 root 權限的帳號來執行，降低應用系統被入侵的風險。

(2) 安裝軟體前應確認有合法授權後始得安裝。

(3) 使用自由軟體時，應注意軟體須由相關官網下載，勿自非官網下載(如 Windows 內建之壓縮軟體)，如有安全性版本更新，應隨時更新安全性，確保軟體無漏洞之虞。

(4) 自由軟體應注意其授權狀態，確保使用為合法使用。

(5) 系統負責人員於安裝系統軟體或應用軟體時，應僅針對必要使用之部分進行安裝，主機系統則應僅啟動必要之服務。

(6) 新建置或安裝之軟體，安裝完成後應即更新廠商預設密碼。

(7) 系統公用程式需進行安全管控，其機制為：

甲、應嚴格限制及控制電腦公用程式之使用。

乙、設定使用者通行碼以保護系統公用程式。

丙、將系統公用程式與應用系統分離。

丁、移除非必要的公用程式及系統軟體。

(8) 系統管理使用之服務安全

甲、網路管理服務(SNMP): 為了 SNMP 服務的安全性，不得使用預設的 SNMP 群組，應設定本所自有的群組，

包含各網路設備、UPS、主機設備均應進行適當的設定。

乙、時間同步服務(NTP): 為使各網路、主機設備記錄的有效性與關聯比較需求，系統裝有校時程式軟體，設定時間同步服務，設備的時間同步服務應盡可能指向同一時間來源，如設備限制，將依設備提供之校時服務為主。

(9) 管理者的責任

甲、管理人員負責建立及維護本所系統使用者帳號，並記錄系統異常狀況及相關維護書面資料。

乙、管理人員未經權責主管人員許可，不得閱覽、增加、刪除或修改其他使用者上傳之私人檔案。當發現有可疑之網路安全情事（如惡意程式、病毒或特洛依木馬等），得使用適當的工具追蹤檢查相關檔案，採取必要處理措施，事後再行知會該檔案擁有者。如確定為感染病毒，為避免病毒擴散，得逕行掃毒、隔離或刪除檔案再行知會該檔案擁有者。

丙、管理人員登入系統時應保留所有登出入系統紀錄，不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成追蹤查詢之困擾，為確保此紀錄，可適時考慮建立適當保存紀錄之服務。

丁、管理人員應定期檢查及停止或撤銷閒置不用的帳號，並不得將其重新配賦給其他的使用者。此外，必須確認不得有非必要的帳號存在（如 guest、anonymous…等）。

戊、每位使用者僅得核發一個使用者帳號，如有特殊情形（如系統測試、免費軟體下載等用途），經申請單位主管核定，始得建立匿名或多人共享的帳號。

己、本所專屬客用服務帳號(service)，依需求建立，不再此要求範圍內管制。

2. 作業安全管理

(1) 各系統軟體與應用軟體的修補程式應處於最新的狀態，如因本所委託或自行開發之系統限制除外。

(2) 資產使用與管理，應依機密分級採取適當之控制措施。

(3) 資產機密性分為三級，說明如下：

分級	說明
高 不可公開	■現行法令法規或內部作業要求，認定該資料屬機密者。 ■對應風險評鑑機密等級「極高」。
中 敏感資料	■資料內若有洩漏，會影響組織聲譽，民眾權益，或造成有形或無形的損害。 ■對應風險評鑑機密等級「高」或「中」。
普通 可公開	■資料內容為一般性資料，但須遵守相關發布流程。 ■若流傳至組織以外，不會對組織造成有形或無形傷害 ■對應風險評鑑機密等級「低」或「極低」。

(4) 進行本程序書「陸、處理步驟七、審視風險評鑑管理架構與調整適用性聲明」中進行細部風險評鑑(資產價值評估時)，須考量資產資產機密性，確保資產評估。

(5) 資訊設備應以標籤標示於設備明顯處，並載明財產編號、保管人員、廠牌、型號等資訊。

(6) 高級（不可公開）資料，應依相關規定辦理；中級（敏感資料），應以黃色標籤標示於資料夾明顯處，或使用黃色資料夾；普通（可公開）資料，無需特定標示。

3. 電腦病毒及惡意軟體之防範

(1) 病毒防護軟體由系統管理者進行規劃評估與建置。

(2) 人員應使用合法具版權軟體，避免交換使用或上網下載來路

不明之軟體或資料。

(3) 與外部交換資料時，使用資料前應啟動病毒防護軟體偵測。

(4) 人員應注意病毒防護資訊，隨時下載病毒碼更新，並定期下載修補系統漏洞。

(5) 操作電腦系統如發現病毒時應立即清除或隔離，無法清除或隔離時依本程序書「陸、處理步驟十五、資訊安全事件管理」內容進行通報。

4. 金鑰管理

資訊系統/服務如採用憑證金鑰的加密技術者，應對金鑰採取適當的保護措施；伺服器上之金鑰如為檔案形式存在，則應對伺服器之金鑰檔案存取權限作適當保護，並作適當的備份保管，如係以韌體形式存在於電腦系統時，則僅需保護其實體存取之安全。

(二) 資訊系統之使用管理

1. 本所暨所屬各機關人員依其職掌或公務需要使用資訊系統(包括資訊設備及資訊軟體)。

2. 本程序書所稱識別碼及密碼使用人，係指使用本所電腦系統識別碼及密碼(以下簡稱識別碼及密碼)查詢特定電腦資料之本所現職市長、主任秘書、職員及經本所核准使用識別碼及密碼查詢資料之其他人員。

3. 識別碼及密碼之申請，應填寫「資訊安全管理制度-實施程序書-帳號申請(刪除)單 (表單編號: DL-ISMS-09_02)」，如為臨時大量需求由本所主任秘書室協助統一建立，使用人應親自使用識別碼及密碼查詢資料。非經核准使用之人員，不得擅自利用他人之識別碼及密碼查詢資料。

4. 本所以外之人員因業務所需，必須委託經核准使用識別碼及密碼

之人員查詢、列印資料，應先填載「資訊安全管理制度-實施程序書-帳號申請(刪除)單 (表單編號: DL-ISMS-09_02)」，並經首長或其授權人核准後，送交受委託查詢人員查詢之。特定資料之查詢、列印，法令另有規定者，依其規定辦理。

5. 個人使用之識別碼及密碼訂定，應依據「行政院國家資通安全會報技術服務中心」所訂定之「政府組態基準(Government Configuration Baseline，簡稱 GCB)」密碼原則規定。識別碼及密碼使用人，應嚴密保管其識別碼及密碼，不得張貼於明顯處所。如有保管不週情事，應由識別碼及密碼使用人負完全之責任。
6. 識別碼及密碼使用人僅得為公務之需要查詢資料，如有查詢自然人個人資料部分，依個人資料保護法相關查詢資料及相關使用規範，不得擅自為公務以外之利用。
7. 區域網路應設置於各機關辦公室內，不得設置於辦公室以外。
8. 主任秘書室除進行資訊系統之故障排除或維護外，未經首長或其授權人員核准，不得逕行查核同仁使用之資訊系統。惟因網路遭不當使用、濫用或破壞，而嚴重影響資訊系統之運作效能者，得為緊急之處理，並於處理完成後，報告首長或其授權人員，以保障資訊業務之順行。

(三) 資訊系統之備援與回復

1. 資訊系統應依其重要性，擬定系統備援、資料備份或回復策略，載明於系統文件，並確實執行。
2. 備份策略應考量類型（全備份、異動備份、歷史檔）、時機、週期、標的（資料程式、作業系統及相關設定）、媒體、存放代數、保存期限、異地儲存、磁碟重整時機、代理人員、操作手冊、成本及安全等。

3. 回復策略應考量備援系統之建置、系統回復及重建之程序及文件， 回復演練時機等。
4. 災變發生時，資訊單位主管應立即掌握災變對資訊作業之影響，指揮執行回復作業，向首長呈報，並視情況與警察、消防、醫院等單位聯絡，作適當之處理。
5. 資訊機房系統應定期執行系統、資料及紀錄之備份，備份工作由系統管理人員統籌規劃執行。
6. 使用虛擬服務系統，以快照方式進行備份者，至少每日進行一次同地快照備份，如儲存機制允許，宜進行異地快照備份。
7. 資訊系統檔案與稽核軌跡紀錄至少應每季執行一次完整備份，備份資料需保存最近一次之備份資料。
8. 備份前應填寫「資訊安全管理制度-實施程序書-資訊系統備份作業紀錄表(表單編號: DL-ISMS-12_01)」統一由系統管理人員設定後辦理定期備份。
9. 每年進行一次備份資料之測試，以驗證備份之有效性，並填列「資訊安全管理制度-實施程序書-資訊系統備份測試查核表(表單編號: DL-ISMS-12_02)」。
10. 資訊機房系統辦理備份資料還原，應填寫「資訊安全管理制度-實施程序書-維護紀錄表(表單編號: DL-ISMS-08_01)」。
11. 系統作業過程中所產生之暫存檔案，應審慎處理是否具機敏與個人資料，於刪除前應須確認檔案，已依據相關法規要求處理。

(四) 資訊系統之個資安全要求

1. 依照其存取權限應提供不同之程式畫面，如資料輸入人員僅能檢視與其權限相符之欄位，審核人員或權責主管可以檢視該案件當事人之所有欄位。

2. 查詢或列印含有個人資料之欄位時，應由系統自行保留其稽核軌跡並由權責主管或稽核人員定期審查其適切性。
3. 系統應定期產生稽核報表，由稽核人員施行資料安全稽核機制以確保個人資料之安全。
4. 查詢含有個人資料之欄位應採用遮蔽之技術，避免詳細之個人資料遭受不當人士抄錄或以其他方式進行保存，若因業務需要需完全檢視其個人資料，應透過權責單位主管之帳號執行，並於需求結束後應立即登出此帳號。
5. 列印含有個人資料欄位之文件時，應採用浮水印之技術以鑑別執行人員及相關個資安全性要求，其內容得包含下列內容：
   (1) 資料提供之公務機關或非公務機關名稱。
   (2) 載明使用資料之"機關名稱"或者為"當事人"。
   (3) 得以鑑別列印執行人員之文字或編號。
   (4) 列印之日期與時間及使用期限。
   (5) 敘明使用此份個人資料之限制或範圍。
6. 含有個人資料之資訊系統檔案應確保離開公司環境後無法開啟，以維護其資料之安全。
7. 保存與備份
   (1) 相關紙本資料不可置於開放之區域，應置於可上鎖之抽屜、公文櫃或具有防火防潮之設備中，鑰匙應由專人進行保管，透過系統進行設備權限之核准應定期清查其授予人員是否與現況相符。
   (2) 個人資料檔案得視需求置於外部資料倉儲或保險櫃中，應建立保存之清單，並定期由查核人員抽核清單內容是否與保存地點之內容是否相符。

(3) 以電子方式保存之個人資料檔案應透過帳號權限控管方式，限定可以讀取或使用之人員，每年應適時進行個人資料檔案之備份且備份之檔案應採用加密技術予以保護。

8. 進行資料複製或輸出時

(1) 進行資料複製或輸出時，應注意是否需完整提供相關個人資訊，應加以遮蔽部分個人資料後再行複製或輸出，若因遮蔽導致違反適法性之資料除外。

(2) 複製或輸出後應立即取回相關資料，相關廢棄之紙張不可再重複使用。

9. 透過電子方式進行傳遞時

(1) 透過傳真進行時，於接獲傳真後應即取走其個人資料檔案。另於傳真給外部單位或當事人時應確認對方是否已收到。

(2) 原則上不以電子郵件傳遞此類個人資料，但若有立即提供之需求，應於交換前先進行加密，再透過電子郵件進行傳遞。傳遞時應注意密碼與加密之檔案應透過不同方式進行交付。

10. 個人資料檔案之刪除與銷毀，應參照本所「陸、處理步驟三 、訂定與審視文件與紀錄管制作業」辦理。

(五) 網路服務的安全

為管理本所網路服務的安全性，應由兩方面來進行管控，一是在系統防火牆僅開放必要之服務設定，其他非必要的服務一律阻絕；二是在伺服器本身僅開放其提供之服務，其他非必要的服務均予以關閉，以達到網路服務的安全。

1. 聯通測試服務(Ping)及路由查詢服務(Trace Route): 本所得提供同仁於端末設備執行 Ping 及 Traceroute 服務，以檢測網路是否聯通。

2. 微軟檔案分享服務(NetBUEI): 個人終端設備禁止採用微軟檔案分享服務，伺服器依需要設定，提供服務。

(六) 行動裝置管理

1. 應安裝防毒軟體，並啟動連線時即時主動更新，以保持病毒碼為最新狀態。
2. 不得安裝與業務無關的軟體(包含非法軟體與來路不明之軟體)。
3. 與外部其他電腦（或攜帶型儲存設備）交換資料時，必須先經過掃毒。

(七) 可攜式儲存媒體

1. 使用可攜式媒體前，須檢查確定無電腦病毒等妨害系統運作因素後，始得使用。
2. 使用可攜式媒體前，應防止執行可攜式媒體中之自動執行檔。
3. 未經主管許可，不得以照相機、攝影機、具照相或攝影功能之PDA 或手機等，進行拍攝。
4. 可攜式儲存媒體用畢後，應立即清空機密資訊。
5. 如有個人業務相關的機密資訊儲存至可攜式儲存媒體時，應予以加密處理，不得以明文方式直接儲存於媒體中，避免遺失或遭竊。

(八) 系統安全稽核

2. 稽核監控與事件紀錄管理

(1) 網路與安全監控

應設置網管系統對網路進行監控，並應定期檢視相關紀錄以達到監控的目標。

(2) 主機登出入稽核

甲、系統管理人員登出入主機系統時應保留所有登出入系

統紀錄，不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成追蹤查詢之困擾。

乙、為保護稽核日誌的獨立完整性，應將資訊系統的相關稽核日誌，包含 syslog、message、eventlog 等集中管制，並定期檢視。

(3) 取證對象，從電腦系統、儲存媒體、電子文件檔案，至網路上傳輸的封包等，取證步驟說明如下：

甲、事前準備

鑑識前應依據遭入侵或內部壞設備進行盤點作業，確認鑑識範圍。

乙、蒐集資料

依據事前準備所確認之鑑識範圍，蒐集相關執行紀錄及數位軌跡資料。

丙、測試

依據所得數位軌跡資料，進行軌跡測試及還原相關原始作業資訊。

丁、分析

將還原原始資料進行分析比對作業，找出關鍵訊息，確認數位資料原始作業程序。

戊、報告

依照此數位原始作業程序製作數位證據之關鍵報告。

3. 系統弱點掃瞄

為強化資訊系統的安全，降低系統軟體已被揭露的漏洞或是應用軟體留下的後門，甚或是不當引入的木馬程式對本所造成安全的

危機，應不定期進行系統弱點掃瞄。

(1) 弱點掃瞄的方法與策略

弱點掃瞄由本所或經授權人員執行

甲、 在內部對所有主機及網路設備進行檢測

I. 此種掃描方式不需透過防火牆，因此可以檢查出所有弱點掃描工具可辨識的安全弱點。

II. 掃瞄結果應與前次比對，以判定漏洞修補之有效性。

乙、從 Internet 對暴露在外的主機及網路設備進行檢測：

此種掃描方式因必須透過防火牆，其範圍與外部惡意攻擊者所能接觸到的範圍一樣，可以真實檢測出目前實際暴露在 Internet 可能被利用的弱點。

(2) 弱點掃瞄的後續處理

甲、弱點掃瞄結果初步分析

弱點掃描報表應按風險高低分類，並針對不同的區域進行風險加權考量，做為漏洞修補優先順序重要參考依據。

乙、漏洞修補評估

I. 辦理漏洞修補前，應與各相關系統負責人討論初步掃描分析結果，評估漏洞修補之影響範圍、修補方法，施作時程等，並完成掃瞄報告與修補建議。

II. 修補的建議方式可為更新 patch、關閉服務、更新軟體版本、限制服務提供目標...等方法，評估過程亦應確認弱點是否為誤判，必要時得以人工檢視進行。

丙、系統漏洞修補

針對高風險弱點項目，應個別擬定預訂修補期限，並責

成相關人員於限期內完成修補工作。

丁、修補成效分析

對於掃瞄分析的結果、修補的結果、修補的時效性、各次弱點的分佈及關連性做整個弱點管理的成效分析，以確認整個弱點修補的有效性。

(九) 其他

1. 各單位應善盡保管之責，未經核准不得私自拆裝，若因私自異動導致電腦系統損毀者，應負賠償責任並依法究辦。
2. 電腦設備、資料或軟體之轉移，均應列帳管理並善盡保管之責。
3. 設備及媒體報廢或改為其他用途時，應檢查其內容是否包含敏感性資訊及個資資料，或者是合法之軟體，務必確認其內容已被適當的處理（格式化、刪除內容或實體銷毀），方可移交或報廢。
4. 嚴禁安裝非法軟體、未授權與來路不明之軟體；另非本所擁有之軟體或未經合法授權之軟體不得使用。
5. 因離職或其他原因移交電腦軟體，或個人不再使用且無人需要之套裝電腦軟體，應辦理變更、異動登記。
6. 系統軟體如需變更或升級，應評估其影響層面後才可以進行，以免因非預期之錯誤，影響作業之正常進行。
7. 可攜式電腦、可攜式媒體及智慧型行動裝置，應適度管制使用範圍與連線作業。

十三、 委外服務安全及供應商管理

(一) 執行委外管理

1. 安全需求規劃

(1) 依據資通安全管理法，所涉及資訊服務之利害關係人/供應

商，於合約及標案中均應要求該利害關係人/供應商，具備良善之資訊安全管理制度獲通過 TAF 認證授權之第三方驗證，並取得 CNS 27001 驗證。

(2) 資訊系統於建置、調整及停用前，應納入安全需求，辦理資訊安全與規格需求分析，確保相關資訊系統之安全要求。

(3) 有關軟、硬體設備之資訊安全需求，特別是架構網路與系統安全所採用之安全系統，應考量是否採購通過資訊安全產品標準驗證之產品，例如：ICSA Labs (http://www.icsalabs.com/)、Common Criteria，以保障整體系統之安全。相關軟、硬體設備之安全需求規劃與驗收，應於需求規格書、合約書或驗收相關文件中以文字清楚描述。

(4) 有關應用系統之資訊安全需求應逐一考量輸入資料之確認、內部處理之控制、訊息鑑別、輸出資料之確認等控制點，必要時，應採用通行碼、加密、數位簽章等方法，確保資訊之機密性、鑑別性、完整性及不可否認性。

(5) 資訊設備應視實際需求簽訂維護契約，以維護設備可用性。若簽訂維護契約者，應納入服務水準協定（SLA，如：服務日期、到場時限、修復時限、服務流程、服務指標等）。

(6) 廠商執行設備安裝維護作業時，除應獲得系統相關人員授權外，須由專人陪同與適當監督，並依據不同設備，要求廠商提供維護紀錄副本或填寫維護紀錄，由專人妥善保管。

2. 容量規劃及檢查

(1) 系統於建置或調整前，應辦理容量規劃，預估未來需求，以確保資訊系統之處理能量與儲存空間。該規劃得以委外方式辦理，惟應審查其適切性。

(2) 有關現有系統容量(包括硬體，儲存媒體及網路頻寬)平均使用率超過80%時，可由資訊人員邀集相關人員重新評估容量需求，並進行容量擴充規劃。

3. 委外合約

所有委外合約均需符合「行政院所屬各機關資訊業務委外服務作業參考原則」，並應標註以下保密及安全需求條款：

(1) 廠商專案人員於執行專案期間所知悉之機關秘密或任何不公開之文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片等訊息，均應保密，不得洩漏。廠商專案人員應簽署保密切結書，對於工作期間所知悉、持有有關之資料、程式、檔案、媒體或電磁紀錄等內容，應遵守相關法令及契約之規定，如「個人資料保護法」、「國家機密保護法」等，善盡保密之責，凡未經機關書面同意或授權，不得以任何形式對外洩漏或交付他人。如有違反應負民事及刑事責任，廠商並負連帶責任，具切結人離職後亦同。

(2) 乙方(廠商)應遵守甲方(本所)所訂之個人資料安全管理事項。

(3) 乙方受甲方委託所蒐集之個人資料其保存期間應至本契約結束為止，契約結束後乙方應視合約要求，調整完成個人資料之轉移及刪除。

(4) 乙方受甲方委託進行個人資料之蒐集、處理或利用者，於個人資料保護法適用範圍內，視同委託機關，應遵循相關法令規定。

(5) 乙方未經甲方同意不得將個人資料複製或交付第三者。

(6) 乙方所維護之個人資料檔案若發生個資安全事故，應立即聯繫甲方承辦單位進行損害之防堵，並於事後提出檢討報告。

(7) 因乙方疏失致發生個資安全事故導致當事人權益受損，應由乙方逕行通知當事人，並負擔一切賠償責任及賠償甲方之損失，賠償金額不受本合約金額限制。

(8) 甲方若需針對合約標的之資料保護情形進行查核監督，乙方不得以任何理由進行拒絕。

(9) 乙方須與其執行本契約服務工作之人員簽訂保密協議，以保護遵守上述保密義務並送交甲方備查。

(10) 乙方及其執行本契約服務工作之人員，應遵守個人資料保護法及相關法令法規之要求，若有違規之情事甲方保留所有追訴之權利。

(11) 委外專案終止責任的溝通，宜包括持續的安全要求、法律責任及依當時包含於機密性協議內的責任，以及在結束委外作業後持續一段期間的僱用條款與條件，為確保於僱用終止後仍然有效的責任與職務，宜於委外合約內訂定。例如：業務秘密、個人資料之保密期限，不受專案工作完成（結案）及乙方不同工作地點及時間之限制。乙方持有或獲知業務相關資料、個人資料，不得洩漏或轉讓於第三者。

(12) 應依據資通安全管理法施行細則要求，第 4 條全部項目，達成相關資通安全服務委外資安管理。

4. 資訊技術服務契約要求

(1) 本要求涵蓋所有 IT 技術支援服務專案，包含：弱點掃瞄、滲透測試、社交工程模擬測試、SOC 監控…等。

(2) 乙方(廠商)應定期對於甲方(本所)委託之資訊資產進行清查與評鑑，並透過風險管理對資訊資產進行適當之控管。

(3) 乙方所維護之資訊資產若發生資訊安全事件，應立即連繫甲

方承辦單位進行損害之防堵，並於事後提出檢討報告。

(4) 甲方若需針對合約標的之資訊資產保護情形進行查核，乙方不得以任何原因進行拒絕。

5. 資訊系統開發與維護安全程序

資訊系統開發與維護計畫，並應於契約內容及在建議徵求書中視業務需要增加以下內容：

(1) 應完成資訊系統開發各階段文件，如系統分析文件、系統設計文件、系統維護手冊、使用者操作手冊、測試報告...等(資訊系統維護計畫視需要之文件類別提出)。

(2) 資訊系統開發與維護過程中，承包廠商應按合約規定召開內部會議，另應定期向承辦單位彙報專案進度與遭遇問題，報告內容應包含專案會議記錄、專案度量與分析...等說明。

(3) 資訊系統開發專案投標廠商應於建議書中，提出資訊系統開發之安全規劃，包含資訊的機密性與完整性保護，內容至少包含資訊於儲存、傳輸、交換、複製時之加密、不可否認...等安全防護機制，以及對於資訊系統管理人員、使用者之認證、授權...等管理機制，並應針對資訊系統之作業紀錄管控與稽核機制進行規劃。

(4) 廠商應於專案管理計畫書中，提出專案開發設備及人員作業環境之實體面與系統面之安全防護措施及管理機制，說明如何防護開發環境之資訊安全。

(5) 資訊系統於規劃、建置或使用階段，宜評估是否已採行適當之矯正處理功能，包含輸入資料的檢核、程式內部處理的管制、訊息的完整性與輸出資料的檢核等功能是否滿足作業安全所需，以避免造成例如輸入資料誤植或資料隱碼攻擊(SQL

Injection)所導致系統資料異常或未授權存取資料外洩事件。

(6) 廠商於專案執行過程中，對於開發與維護的系統需求與程式碼，至少應進行軟體開發之需求管理、問題單管理、程式碼建構管理。另交付之程式碼應通過測試，並於系統交付時一併提交測試紀錄及程式相關文件。

(7) 測試完成之程式於上線前需填寫本所「資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號: DL-ISMS-10_01)」於核准後方可上線。

(8) 針對版本管制應配本所之軟體版本控制系統(SVN Server)進行控管及填寫本所「資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號: DL-ISMS-10_01)」。

6. 資訊安全驗收程序

所有委託廠商開發的資訊系統在驗收前需通過下列審查並留下審查紀錄。

(1) 測試報告的審查。

(2) 程式碼檢查，可以內部進行或委託第三方進行，檢查的範圍至少包含功能面的符合性、不當或惡意程式、後門、輸出入欄位資訊符合性檢核設計等。

(3) 於測試主機執行測試，透過弱點或入侵偵測工具檢驗。

(4) 合約所訂相關資訊安全控制項目。

(5) 於開發過程應填寫「資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號: DL-ISMS-10_01)」，提供本所驗收審視，確保開發過程委託開發廠商安全。

7. 第三方服務的管理

(1) 簽署正式協議之機關與廠商委派人員提供服務，或因應政府

法規或行政命令採用第三方提供的服務，應對第三方提供的服務進行適當的管理。無正式協議之外部單位，不得使用其所提供的服務(公共服務除外) 。

(2) 對於使用第三方服務，應進行以下之管理作業：

甲、協議提供的服務內容安全性審查。

乙、服務執行人員的資格審查。

丙、服務執行人員的保密切結書。

丁、執行成效的審查，得經由會議紀錄、彙整資料審查或現場實地訪查。

戊、第三方提供之服務如須變更時，應正式函文通知並經雙方同意後始得進行變更。

己、未驗收但已上線之資訊系統與設備專案，預計造成網路服務中斷時，應訂定相關變更之管控要求；如為自行上線系統將由上線單位撰寫應變計畫。

8. 保密需求

(1) 利害關係人/供應商需於簽約書內文明訂保密切結條款及規範，專案內規畫人員需填寫「資訊安全管理制度-實施程序書-利害關係人/供應商執行人員保密同意書(表單編號: DL-ISMS-11_02)」如有駐點人員，需增加填寫「資訊安全管理制度-實施程序書-利害關係人/供應商執行人員保密同意書(表單編號: DL-ISMS-11_02)」。

(2) 利害關係人/供應商需於簽約書內文明訂保密切結條款及規範需填寫「資訊安全管理制度-實施程序書-利害關係人/供應商保密切結書(表單編號:DL-ISMS-13_01)」。

9. 職內訓練

應對利害關係人/供應商執行計畫人員，實施資訊安全教育訓練，並要求遵循資訊安全管理規定。

10. 利害關係人/供應商人員離職及變更

合約中應明訂利害關係人/供應商參與人員離職及變更等相關規定。

(二) 系統委外開發與維護之服務交付管理

1. 系統開發與維護委外辦理時，應與資訊系統開發/維護廠商簽訂適當的資訊安全協定，賦予相關安全管理責任，並納入契約條款。
2. 系統開發與維護委外辦理期間，應定期對資訊系統開發/維護廠商所提供之服務、報告及紀錄等進行監控與審查。
3. 管理契約條款與專案內容的變更，應針對變更項目進行評估，確保符合相關資訊安全管理制度與法律規定、業務需求之期望。

(三) 各項業務委外之第三方監督，應納入合約中管理並包含下列事項：

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間，本所應定期確認受託者執行之狀況，並將確認結果記錄之。
2. 委外之第三方應依「個人資料保護法施行細則第十二條第二項界定個人資料之範圍」採取之措施。
3. 有複委託者，其約定之受託者。
4. 委外之第三方或其受僱人違反個人資料保護法或其他法規命令時，應向本所通知之事項及採行之補救措施。
5. 本所如對委外之第三方有保留指示者，其保留指示之事項。
6. 委外之第三方僅得於本所指示之範圍內，蒐集、處理或利用個人資料；委外之第三方如認為，本所之指示有違反個人資料保護法或其他法規命令者，應立即通知本所。

7. 委託關係終止或解除時，個人資料載體之返還，及委外之第三方履行委託契約以儲存方式而持有之個人資料之刪除。
8. 委外之第三方業者與本所終止合作或契約，其業務終止後所需處理之個人資料屬本所所有部分，本所視需要派員全程督導處理過程，於處理後取得其所有與本所委託之個人資料檔案清冊、處理方式、以及處理記錄。如該受委託者有複委託單位亦同。
9. 如本所業務終止涉及委外第三方業者，應通知第三方業者立即停止該項個資業務活動（蒐集、處理、利用及國際傳輸等），並依個資資料轉移作業及個資資料銷毀作業，要求第三方業者辦理，本所視需要派員全程督導處理過程，於處理後取得其所有與本所委託之個人資料檔案清冊、處理方式、以及處理記錄。如該受委託者有複委託單位亦同。
10. 如有涉及當事人權益之事項應要求第三方業者以適當之方式通知當事人，並留存相關紀錄或證明交付本所存查。

(四) 委外業務未驗收上線之設備管理

未驗收但已上線之資訊系統與設備專案，預計造成網路服務中斷時，應訂定相關變更之管控要求。

(五) 其他

1. 資、通訊系統服務委外，應考量成本、人力、管理、安全、不停頓需求、備援需求、資料傳輸需求、系統、資料存取及個資保護安全需求及服務水準等方面。
2. 委外服務合約除包含各課室及其所屬單位提出之資訊安全需求外，應明定遵循法律要求並清楚界定本所與承包商之權責義務。
3. 所有承包商與本所簽署之合約，須適當載明相關保固服務與因資訊安全事件造成本所損失之罰責(包含因承包商人員作業疏失所

造成之損失），以確保服務品質之要求。

4. 所有承包商使用本所管理之金鑰及憑證須加強管制。

5. 本所應適時針對各項不同委外服務之供應商進行適當之稽核作業，作為本所委外服務依據。

十四、 業務持續運作管理

確保本所之關鍵業務流程活動作業中斷時，能在最短時間內復原，並提供正常服務。

(一) 業務持續管理

1. 業務衝擊分析及業務持續策略

(1) 為保障資訊系統的持續運作，除資訊系統運作策略外，另須包含發電機、不斷電系統（UPS）、電腦、網路設備、辦公設施、運作人力及其他計畫等運作所需的週邊環境。

(2) 進行填寫「資訊安全管理制度-實施程序書-業務衝擊分析表（Business Impact Analysis：BIA)（表單編號：DL-ISMS-14_01)」時，主要需考量的因子為可以忍受的最大服務中斷時間（Maximum Tolerable Downtime：MTD）及資料回復點（Recovery Point Objective：RPO）。

(3) 鑒於本所作業特性，對於資料及時復原的需求較低，系統及時回復需求較高，因此 MTD 幾乎與系統回復時間(Recovery Time Objective：RTO）相等，後續將以 RTO 取代 MTD 作說明。本所 RTO 的時間包含從災難發生至系統回復點，針對本所重要業務進行衝擊分析，並填寫「資訊安全管理制度-實施程序書-業務衝擊分析表（Business Impact Analysis：BIA)(表單編號: DL-ISMS-14_01)」:

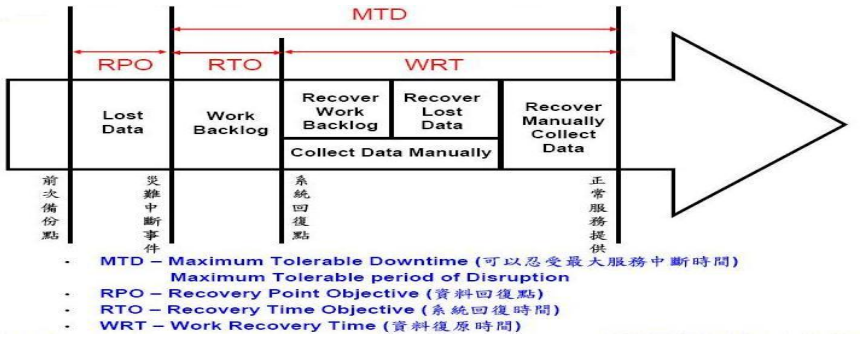

圖 6、業務衝擊分析圖

2. 業務衝擊分析依據「資訊安全管理制度-實施程序書-業務衝擊風險鑑別原則(表單編號：DL-ISMS-14_02)」來加以判定。

3. 處理原則

(1) 須建立業務持續運作計畫暨緊急應變及災害演練計畫作業以確保本所負責之重要業務能持續運作。

(2) 業務持續運作計畫暨緊急應變及災害演練計畫作業之撰寫應考量下列重點：

甲、目的及範圍。

乙、界定重要的業務作業程序，並訂定其優先順序。

丙、評估各種災害對本所業務可能的衝擊。

丁、維持本所業務持續運作之人員責任界定，以及緊急應變相關措施之安排。

戊、建立本所業務持續運作之作業程序及流程，並以書面或其他電子方式記載。

己、遵循作業程序直到復原及恢復工作完成。

庚、執行緊急應變措施及作業流程，進行同仁教育及訓練。

辛、定期演練緊急應變措施須。

壬、定期更新緊急應變措施。

(3) 演練及調整

甲、定期災害演練，為確保計畫的有效性，並使相關同仁確實瞭解計畫的最新狀態。

乙、依據業務持續運作計畫，使用「資訊安全管理制度-實施程序書-XX 年度營運持續災害復原演練範本(表單編號：DL-ISMS-14_03)」訂定每年年度業務持續災害復原演練計畫，依演練項目，每年至少進行 1 次災害復原演練，使緊急應變措施維持在有效及最新的狀態。

(4) 業務持續運作計畫之審核及發行

甲、資訊安全管理小組應每年制定及審核年度業務持續災害復原演練計畫，並經資訊安全長核准通過後發行。

乙、應確保業務持續運作計畫之可用性，使得相關人員在緊急狀況發生時，都能取得該計畫並且依計畫執行。

丙、應確保業務持續運作計畫之完整性，確保各相關人員所持有之計畫為最新版本。

丁、應妥善辦理教育訓練，使得相關同仁在緊急事件發生時能夠按照計畫辦理。

(5) 業務持續運作計畫之重新檢視及評估

甲、資訊安全管理小組定期檢視及評估業務持續運作計畫。

乙、當環境發生重要變動時，資訊安全管理小組須重新檢視及評估業務持續運作計畫。

丙、計畫變更時應通知所有相關同仁，以確保相關同仁均已知其責任及持有最新版之業務持續運作計畫。

(二) 業務持續計畫內容解說

1. 業務持續計畫啟動

當資訊安全事件發生時，由資安長決定是否啟動業務持續計畫。

2. 業務持續計畫執行程序

(1) 確認緊急集合地點及聯絡清單

甲、當本所發生重大災難事件，災難事件結束後，人員應儘速回報並進行復原工作，優先集結地點及聯絡資訊為

I. 地點：斗六市公所主任秘書室

II. 地址：640 雲林縣斗六市府文路 38 號

III. 電話總機：(05)533 2000

乙、無法於上述地點集結時，改於斗六廳集結，由資訊安全處理小組組長負責依「資訊安全管理制度-實施程序書-推行小組成員暨利害關係人名冊(表單編號：DL-ISMS-02_01)」緊急聯繫相關人員進行後續處理。

(2) 設備與環境之資源

甲、辦公環境

I. 終端電腦作業環境

II. 終端印表機

III. 網路作業環境

IV. 電話

V. 傳真

乙、關鍵活動業務資訊系統服務

I. 關鍵活動業務系統伺服器

II. 網路連結設備

III. 關鍵活動業務系統與網路服務

IV. 網路與安全監控服務

丙、資料與日誌

資訊與紀錄為業務是否能持續的重點，應定期備份

丁、業務持續作業的後勤支援

I. 電腦軟、硬體及網路設備的購置

II. 辦公及電話通訊設施的購置

III. 異地辦公環境及設備、文件的搬遷

IV. 人員狀態的確認及工作分派

V. 設備維護採購及人事、差旅經費的取得

VI. 系統回復所需的環境與設備

VII. 技術支援的取得

(3) 資訊安全組織各成員依據下列模擬情境，以關鍵活動業務或服務為主軸，或可採多項模擬情境整合方式，建立年度災害復原演練計畫應變演練模擬情境與劇本「資訊安全管理制度-實施程序書-XXX 年度營運持續災害復原演練範本(表單編號：DL-ISMS-14_03)」，進行相關應變及處理。

(4) 關鍵活動業務或服務評估檢討

甲、當關鍵活動業務或服務重大事故的危機解除，作業單位人員皆安全後，將災害應變處置復原過程相關完整的紀錄，撰寫評估檢討報告，由文件管理小組建檔管制，以利爾後查考使用。

乙、評估災害損失項目，包括

I. 關鍵活動業務或服務是否可持續作業或有延誤狀況，如作業影響、備援作業啟動…等。

II. 關鍵活動業務或服務所使用之電腦設備損失情況，

如電腦主機、工作站、網路設備、備份...等。

III. 關鍵活動業務或服務之資訊系統或資料回復所需時間評估。

丙、評估檢討報告的內容應包括：

I. 重大事故的描述及日期、時間

II. 重大事故的程度

III. 復原的方案選擇

IV. 事件原因分析

V. 稽核軌跡

VI. 相關證據資料

VII. 矯正預防措施

3. 異地備援(或備份)緊急建置

(1) 如發生重大災難事件，無法於本地進行系統回復作業時，由資訊安全處理小組尋找適當場所，經資訊安全長授權資訊安全管理代表執行，建置異地備援機制，由現有備份媒體進行關鍵活動業務或服務之資訊系統回復作業後，於異地提供緊急作業服務。

(2) 如異地備援因受限人力、財力、物力等主觀因素或環境空間等客觀因素，不易達成，則以異地備份機制取代，將本地端備份資料，另行拷貝一份逕送一地備份機房存放，一旦本地端發生重大災難後，仍可由異地端將原備份資料取回存至關鍵活動業務或服務之資訊系統內，進行運作。

(3) 異地備援(或備份)環境與設備需求

甲、(備用)電力系統

乙、終端電腦作業環境

丙、終端印表機

丁、網路作業環境

戊、電話

(4) 關鍵活動業務或服務之資訊系統服務需求

甲、關鍵活動業務或服務系統伺服器

乙、網路連結設備

丙、重要業務系統與網路服務

丁、網路與安全監控服務

(三) 災害復原演練

1. 業務持續計畫須定期測試，如屬實際發生之災害，應依據上項所訂定進行緊急應變作業；若未曾發生之災害，則自行視需要不定期對全部或部份的業務持續，模擬情境方案計畫執行演練測試或擬定 3 年度災害復原演練計畫應變演練模擬情境與劇本，並於 3 年期限內分項完成，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。
2. 演練項目、步驟及查核表詳如「資訊安全管理制度-實施程序書-XXX 年度營運持續災害復原演練範本(表單編號：DL-ISMS-14_03)」中，並依年度災害復原演練計畫應變演練模擬情境與劇本進行演練。
3. 業務持續計畫測試前須填報測試計畫，經核可後進行。
4. 每年應針對本計畫之可行性與有效性至少進行結構化測試（Structural walk-through），以確定本計畫的有效性，所產生之業務持續計畫測試報告應列為內部稽核之重點項目，測試報告應

包括以下內容：

(1) 業務功能說明

(2) 模擬測試環境

(3) 模擬測試過程

5. 資訊安全管理小組應不定期辦理教育訓練，並依據程序書「陸、處理步驟十一、人員安全管理暨教育訓練」要求辦理。

6. 業務持續計畫之重新檢視

(1) 主任秘書室除每年定期檢視外，於下列重大事件發生後也應對業務持續計畫進行重新檢視與維護：

甲、新的業務業務策略

乙、採購新的設備，或是更新作業系統

丙、使用新的問題偵測及控制技術

丁、使用新的環境控制技術

戊、組織上的調整變動

己、契約當事者或是供應商的調整變動

庚、實務作業的變更

(2) 有關本計畫各項業務持續演練之過程與決議，應保留相關紀錄「資訊安全管理制度-實施程序書-OOO 年度業務持續演練之災害復原演練報告範本(表單編號：DL-ISMS-14_04)」，並列為內部稽核之重點項目。

十五、 資訊安全事件管理

確保本所加強資訊安全事件發生時之應變能力及避免資訊安全事件失去控制，成為影響組織業務持續運作的危機：

(一) 當重大天然災害(如地震、海嘯及及風災等)及人為災難(惡意攻擊、

網路中斷及系統不明中斷等)影響本所關鍵業務之相關資訊安全之事件，除依「陸、處理步驟十四、業務持續運作管理」進行復原外，應將相關訊息傳遞管理階層，藉以管控及指導因應。

(二) 如遭中斷之業務作業與各利害關係人要求相關(如提供利害關係人服務之資訊系統或具識別個人之個資外洩等)，應通知相關利害關係人並依其相關要求進行處置。

(三) 資安事件分類與影響分級

1. 資安事件類別分為三類

(1) 內部資安事件：如惡意破壞毀損、作業不慎、未依規定操作。

(2) 外力入侵事件：如病毒感染、駭客攻擊（或非法入侵）。

(3) 天然災害或重大突發事件：如颱風、水災、地震、火災、爆炸、核子事故、重大建築災害等。

2. 資安事件影響等級分為四級

(1) 4 級事件

符合下列任一情形者，屬 4 級事件

甲、國家機密資料遭洩漏（機密性衝擊）。

乙、國家重要資訊基礎建設系統或資料遭竄改（完整性衝擊）。

丙、國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作（可用性衝擊）。

(2) 3 級事件

符合下列任一情形者，屬 3 級事件

甲、密級或敏感公務資料遭洩漏（機密性衝擊）。

乙、核心業務系統或資料遭嚴重竄改（完整性衝擊）。

丙、核心業務運作遭影響或系統停頓，無法於可容忍中斷時

間內回復正常運作（可用性衝擊）。

(3) 2 級事件

符合下列任一情形者，屬 2 級事件

甲、非屬密級或敏感之核心業務資料遭洩漏(機密性衝擊)。

乙、核心業務系統或資料遭輕微竄改（完整性衝擊）。

丙、核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作（可用性衝擊）。

(4) 1 級事件

符合下列任一情形者，屬 1 級事件

甲、非核心業務資料遭洩漏（機密性衝擊）。

乙、非核心業務系統或資料遭竄改（完整性衝擊）。

丙、非核心業務運作遭影響或短暫停頓（可用性衝擊）。

(四) 資安事件通報作業處理程序

1. 各單位同仁發現資訊系統或服務運作不合常態，或發現可疑安全弱點或威脅時，應向資訊安全處理小組反映請求協助。
2. 資訊安全處理小組發現或接獲通知資訊系統運作不合常態時，應先判斷是否屬於資安事件。
3. 資訊安全處理小組於確認發生資安事件時，經研判影響程度屬於內部資安事件之 1 級（含）以下者，即自行處理復原。屬於 2 級（含）以上重大災害，資訊安全處理小組應立即（最遲不得超過三十分鐘）填報「資訊安全管理制度-實施程序書-資訊安全事件通報單(表單編號：DL-ISMS-15_01)」並依據事故狀況，評估相關可能因素，藉由適當管道，尋求解決方案。
4. 本所資訊安全處理小組於確認發生資安事件或接獲所屬機關發

生資安事件之通報後，經研判影響程度屬於 2 級（含）以上重大災害，且影響層面深廣、受損程度嚴重時，應將事件發生之事實、可能影響之範圍、損失評估、判斷支援申請、採取之應變措施等事項，立即（最遲不得超過三十分鐘）填具「資訊安全管理制度-實施程序書-資訊安全事件通報單(表單編號：DL-ISMS-15_01)」，並透過上網、行動電話、傳真或電子郵件等方式，通報至「國家資訊安全應變中心」及其隸屬之分組召集單位。

5. 各機關之資安事件，若危及人員生命或設備遭到破壞等涉及民、刑事案件時，應即時通報檢調單位請求處理。如引發重大災害時，應向災害防救體系提報，請求支援處理。

(五) 資安事件應變作業處理程序

1. 狀況判斷

(1) 各機關就資安事件之徵兆，查明事件狀況、安全等級區分、判定可能影響範圍、評估可能損失、判斷是否需要支援申請等作業項目逐一檢討與處置；並保留被入侵或破壞等證據（如網頁置換等）。

(2) 透過系統弱點（病毒）資料庫、上網站、技術支援單位（或廠商）等方式，查詢獲得解決方案（如下載漏洞修補程式、解毒程式等）；或依既定之緊急應變計畫，實施災害緊急應變搶修處置（如保護、救援、回復運轉等），並持續性主動積極之監控與追蹤管制。

(3) 視損害程度啟動備援計畫等應變措施。

(4) 如屬新生（以往未發生過）無法解決之危害事件，應迅速向本所資訊安全處理小組反映，請求提供相關技術支援。

(5) 執行其他災害應變及防止事件擴大之措施。

2. 應變作業優先順序如後：

(1) 資訊網路：GSN VPN 網路、機關內部網路等。

(2) 一般行政：公文電子交換系統、公文系統、差勤系統、薪資系統等。

(3) 網路服務：防火牆、DNS 、網站伺服器、電子郵件伺服器、防毒主機等。

3. 分類應變作業處理程序

(1) 內部資安事件：儘速查明事件影響狀況、受損程度等，啟用備份資料、程式或備援計畫相關措施，以儘速回復正常運作。

(2) 外力入侵事件

甲、病毒感染事件：病毒入侵後，應先拔除網路線隔離病毒，避免疫情擴散，並隨時掌握電腦病毒感染最新動態；同時儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。

乙、駭客攻擊（或非法入侵）事件

I. 發現（或）被入侵時，立即隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並迅速啟動備援系統或程序。

II. 如入侵者已被嚴密監控但不危害內部（含 DMZ 區）網路安全下，可考慮讓入侵者作有條件的連接，適度允許其繼續動作，以利追查入侵者 IP 位置；並利用稽核檔案或系統指令、聯合 ISP 公司等方式，追蹤入侵者行蹤。惟一旦入侵者危害到內部(含 DMZ 區)

網路安全，則立即切斷入侵者之實體連線。

III. 正式紀錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考，並向主管機關或檢警單位反映。

(3) 天然災害或重大突發事件

甲、如遇颱風、水災、地震等天然災害或火災、爆炸、核子事故、重大建築災害等重大意外事件，應迅速攜帶重要資料及程式等離開現場，或儲存於防火保險櫃等設施內，以利災後系統重置復原。

乙、如遇通訊網路系統骨幹中斷事件，應立即查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶修作業。

4. 分級處理程序

(1) 3 級：機房人員應儘速通知相關系統負責人及主管處理該事件，立即採取緊急處置（如關閉電源、搬離重要資料等），並連絡維護廠商或相關技術支援單位（如技服中心）協助。

(2) 2 級：系統負責人應儘可能備份目前系統所有資料及狀態，找尋其它可行替代運作方案，並邀集主管、維護廠商或相關人員處理該事件及研判問題所在。

(3) 1 級：系統負責人應先復原該系統，並邀集廠商或相關人員研判問題所在，以確定系統異常原因。

(4) 上述各項災害，若系統負責人懷疑損害會因網路或系統開機而持續擴大，應立即中斷網路連線或關機。

5. 資安事件應變作業處理流程圖如下

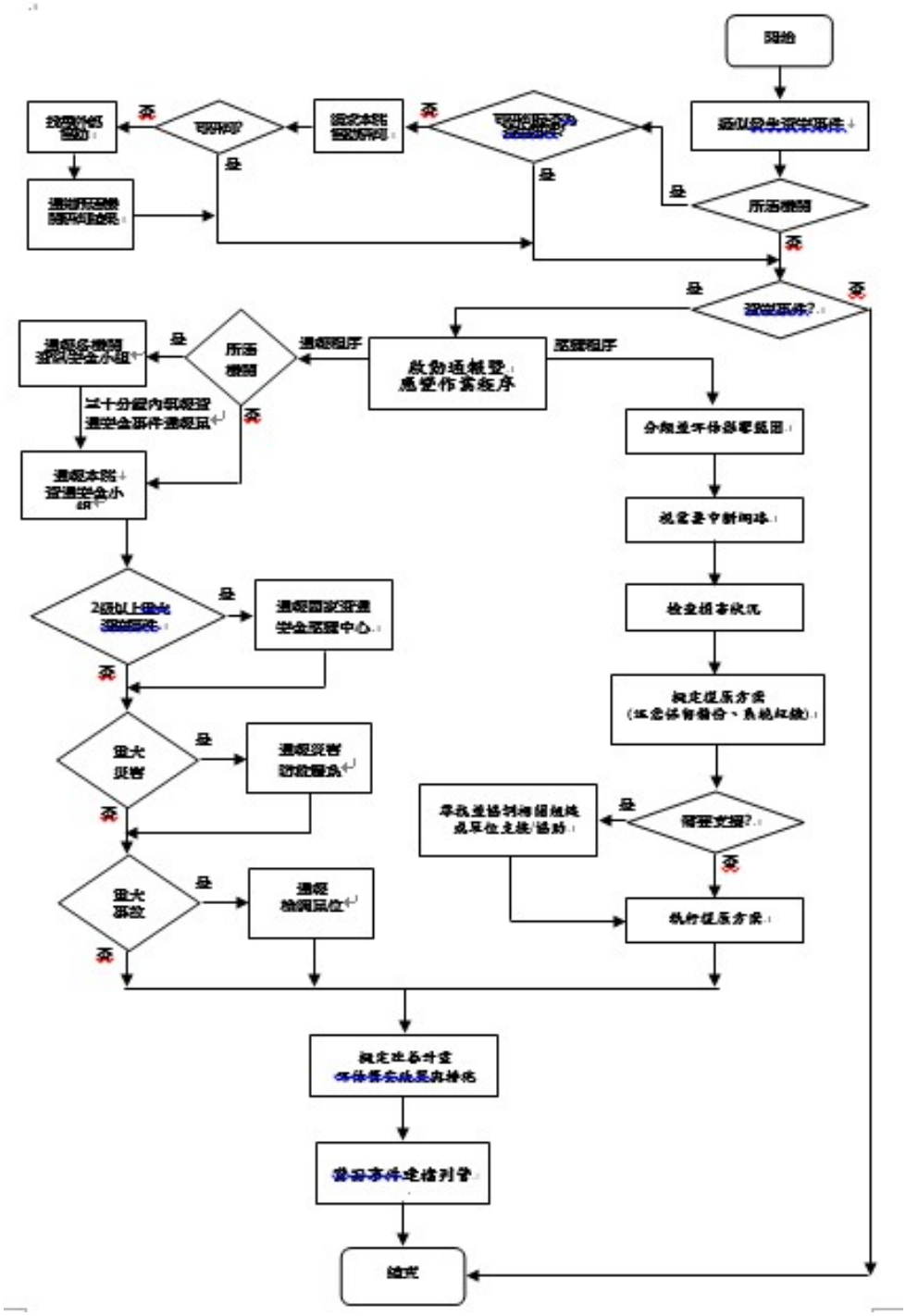

圖 7、資安事件應變作業處理流程圖

(六) 復原追蹤鑑識

1. 受損機關執行災後復原工作，首先檢驗資訊安全環境及硬體設備是否可以正常運作，並執行環境重建、系統復原及掃描作業，其步驟包含軟硬體設備重新取得建置、重置作業系統及應用系統，

以及運轉測試等；並俟運作正常後即進行安全備份檔案下載、資料回復、資料重置等相關事宜。

2. 當危機解除後，受損機關應將災害應變處置復原過程之完整紀錄（如事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料），予以建檔管制，以利爾後查考使用。

3. 受損機關如有需要，應保留事件發生之線索，經洽本所資安小組同意後，向技術服務中心或檢警單位申請追蹤鑑識、偵查支援，藉研析稽核紀錄或入侵活動偵測等相關資料，以釐清事件發生的原因與責任；並找出防護系統之漏洞，尋求補強保護方法，避免事件再度發生。

4. 資安事件或造成運作中斷之事件，由各機關發言人統一對外發言。

十六、 法律遵循與內部規範管理

確保本所，符合並遵循政府之法律、法規與本所內部資訊安全需求相關之義務，並定期蒐集資訊安全相關法規，針對本所工作範圍，界定適用之法規，登錄於「資訊安全管理制度-實施程序書-法規一覽表(表單編號：DL-ISMS-16_01)」，如有最新資訊安全法規與其他要求之適用性與版本變更狀況，並應即時變更。

(一) 瞭解最新之資訊，檢查並更新與本所門各項作業相關之法規，同時依該規定之要求評估符合性，若有不符合狀況時，應依「陸、處理步驟十八、矯正與改善」辦理。

(二) 本所依據所界定組織全景與利害關係人要求事項，遵循相關政府法令法規要求，如有最新資訊安全法規與其他要求之適用性與版本變更狀況，應即時變更。

(三) 針對本所內部作業要求，自行訂定規範，亦須根據內部作業要求適

時更新，確保內部規範管理作業。

(四) 智慧財產權(IPR)。

(五) 個人資料保護。

(六) 建立資料安全稽核機制及保全必要之使用紀錄、軌跡資料及證據，以為後續舉證(證明)確保善良管理人之責。

(七) 核對技術遵循性。

(八) 對系統稽核工具使用須加以管制，以防止任何可能之濫用或危害，若狀況許可時，應考慮將稽核紀錄存放於其他主機上，避免系統管理人員誤用或蓄意破壞。

(九) 遵守資通安全管理法及相關子法

十七、 資訊安全稽核作業

確保本所，規範資訊安全管理制度稽核之執行方式，以驗證本所資訊安全相關活動執行是否符合資訊安全管理制度之要求：

(一) 本所資訊安全管理制度每年實施一次資訊安全內部稽核，由資訊安全稽核小組規劃執行。

(二) 辦理內部稽核前，應於稽核計畫中審慎規劃稽核活動中運作系統與稽核工具保護措施，俟稽核計畫核定後方可著手稽核。

(三) 內部稽核的結果及協助執行稽核之設備（工具）須適當保護措施。

(四) 內部稽核過程須量測風險管理措施的有效性，並發掘潛在性的風險，以利進行預防措施，防止資訊安全危機事件的發生。

(五) 資訊安全稽核種類

1. 外部稽核
2. 內部稽核

3. 上級機關稽核

(六) 內部稽核員資格要求

1. 稽核工作執行人員由管理代表遴選符合安全管理系統內部稽核員資格要求之人員擔任。
2. 曾完整見習一次(含)以上之內部稽核活動。
3. 資訊安全內部稽核員要求(至少需符合一項)：
   (1) 應完成 ISO/CNS 27001 至少 6 小時以上之專業訓練。
   (2) 取得 ISO 27001 LA(主導稽核員)資格。
   (3) 曾參加資訊安全教育訓練及稽核訓練課程者。
4. 委託專業顧問公司協助執行內部稽核工作，委託顧問應取得ISO27001LA(主導稽核員)資格。

(七) 稽核程序

1. 責任
   (1) 受稽單位
      甲、指派人員接受稽核。
      乙、提供稽核團隊所需之相關文件與紀錄。
      丙、針對稽核缺失提出矯正措施。
   (2) 資訊安全工作小組
      協調、提供稽核作業所需之各項資源。
   (3) 資訊安全稽核小組
      甲、擬訂稽核計劃。
      乙、執行稽核計劃。
      丙、撰寫資訊安全稽核報告。
      丁、針對稽核結果提出建議改善方案。

戊、追蹤改善方案之執行成果。

己、配合辦理其他單位對本所之外部稽核。

(4) 稽核領隊

甲、規劃該次稽核之「資訊安全管理制度-實施程序書-稽核計畫(表單編號：DL-ISMS-17_01)」。

乙、指派稽核員、組成稽核團隊。

丙、彙整並提出稽核報告。

丁、主持稽核啓始及結束會議。

(5) 資訊安全稽核小組組長

甲、指派資訊安全稽核小組領隊並核可稽核員名單。

乙、主持稽核團隊準備會議、稽核結果會議。

丙、審核資訊安全稽核報告。

(6) 資訊安全推行小組

督導稽核作業之規劃與執行。

2. 稽核作業說明

(1) 稽核週期

甲、每年定期執行資訊安全稽核作業。

乙、資訊安全稽核小組組長得視需要不定期指派專人、委由外部專家或配合外單位，執行資訊安全稽核作業。

(2) 組成稽核團隊

甲、稽核領隊由資訊安全稽核小組組長指派；稽核員由稽核領隊指派。

乙、稽核員之指派及稽核分工應考量其獨立性，稽核員不得對所負責之業務執行稽核。

丙、稽核人員資格要求如下：

依據本程序書本節「(六)內部稽核員資格要求」。

(3) 稽核計畫

甲、「資訊安全管理制度-實施程序書-稽核計畫(表單編號：DL-ISMS-17_01)」內容應包括：目的、範圍、稽核項目、稽核團隊、稽核時程、稽核程序及「資訊安全管理制度-實施程序書-內部稽核表(表單編號：DL-ISMS-17_02)」 等，並應經資訊安全推行小組召集人核准。

乙、資訊安全稽核小組組長應召開並主持稽核團隊準備會議，確認計畫內容及其它相關稽核事項。

丙、執行定期稽核作業，應於稽核前 5 個工作日通知受稽核單位，以利受稽核單位準備稽核事宜。

(4) 稽核執行

甲、稽核團隊應先召開稽核啟始會議，由稽核團隊介紹成員與分工，並說明稽核範圍、時程及雙方配合事項等。

乙、稽核員執行稽核作業時，應以抽樣之方式收集足夠之客觀證據，並應保存適當之稽核紀錄。

丙、稽核員應根據稽核事實與發現，填寫「資訊安全管理制度-實施程序書-內部稽核表(表單編號：DL-ISMS-17_02)」。稽核過程中「資訊安全管理制度-實施程序書-內部稽核表(表單編號：DL-ISMS-17_02)」之稽核項目若須增修，需經稽核領隊同意。

丁、受稽核單位應據實答復稽核員所提問題，並提供適當之相關文件及紀錄，以為資訊安全管理制度執行之證明。

戊、稽核過程中若有存取系統之需求，應由受稽核單位人員進行操作，並留下系統存取紀錄。

己、稽核過程中之系統存取與操作，應事先評估稽核作業之風險，並不得影響系統正常運作。

庚、稽核過程中若使用系統稽核工具，應遵循以下規範：

I. 系統稽核工具之存取應由專人於授權範圍內操作，並保留存取與操作紀錄。

II. 系統稽核工具及稽核證據應予以妥善保護，以避免非經授權存取或竄改。

(5) 稽核報告

甲、稽核作業結束後，稽核小組組長應召開稽核結果會議，針對稽核事實與發現予以彙整，作成「資訊安全管理制度-實施程序書-稽核報告(表單編號：DL-ISMS-17_03)」。

乙、「資訊安全管理制度-實施程序書-稽核報告(表單編號：DL-ISMS-17_03)」完成後，稽核團隊應召開稽核結束會議，由稽核領隊報告稽核結果及發現，並對疑義進行澄清。

丙、稽核結束會議後，受稽核單位代表應於稽核報告簽名，完成此次稽核活動。

丁、受稽核單位收到稽核報告後，應依規定填寫「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」，並管制稽核發現事項之矯正情況，如受機單位已完成矯正措施，經單位主管核定後，回復資訊安全稽核小組。

(6) 矯正措施

依本程序書「陸、處理步驟十八、矯正與改善」辦理。

(八) 委外服務廠商稽核

1. 委外稽核時機

(1) 依據本所各項資訊安全委外服務合約要求事項。

(2) 於委外服務過程中發現委外服務廠商，常有未符合本所資訊安全政策要求。

2. 稽核作業步驟

(1) 擬定委外稽核計畫，稽核計畫內容依據委外服務合約建立「資訊安全管理制度-實施程序書-資訊安全管理制度委外服務廠商稽核計畫(表單編號：DL-ISMS-17_05)」，並於稽核前 1 個月將「資訊安全管理制度-實施程序書-資訊安全管理制度委外服務廠商稽核計畫(表單編號：DL-ISMS-17_05)」寄達委外服務廠商。

(2) 內部稽核小組於稽核前 1 週再通知受稽委外服務廠商依據委外合約要求及本所委外稽核計畫「資訊安全管理制度-實施程序書-資訊安全管理制度委外服務廠商稽核計畫(表單編號：DL-ISMS-17_05)」配合稽核作業。

(3) 稽核實施之後，將稽核發現事實詳細紀錄，內部稽核小組應彙整各稽核員填寫之稽核報告完成「資訊安全管理制度-實施程序書-資訊安全管理制度委外服務廠商稽核報告(表單編號：DL-ISMS-17_06)」，除送交資訊安全管理委員會審查，並由資訊安全管理小組負責保管備查外，並將本分稽核報告函送受稽核委外服務廠商，針對不符合本所資訊安全事項，進行改正。

(4) 要求受稽核委外服務廠商針對不符合本所資訊安全不符合事項改正結果函送本所，作為本所後續委外服務招標參考。

(5) 如受稽核委外服務廠商已通過 ISO/CNS 27001 或 ISO27701 等國際或國內資訊及個資安全標準，可以要求該公司年度外部稽核報告函送本所參考，本所審視稽核報告內容情況，原則不再進行委外服務廠商稽核作業，如有例外情況才需要進行委外服務廠商稽核。

(九) 委託稽核

1. 內部稽核作業委託稽核

(1) 委託稽核時機

甲、本所稽核人力不足人時。

乙、本所稽核專業知識及經驗不足時。

(2) 委託稽核步驟

甲、事前由本所文件管理小組與內部稽核小組與委託稽核顧問公司研討本所稽核期程與稽核範圍。

乙、由委託稽核顧問公司製作稽核計畫函送本所後，依稽核計畫內容及期程，由本所內部稽核小組，陳文本所資訊安全長核准後，通告本所相關人員(資訊安全委員會、資訊安全處理小組等成員)準備稽核(包括稽核會議之出席人員與會議簡報及稽核場所布置等)事宜。

丙、稽核前 1 週本所內部稽核小組，應確認受稽核人員差勤管制(如非必要之差勤，須要求本所各單位管制差勤) 。

丁、稽核過程中，由文件管理小組依據委託稽核顧問公司要求，提供本所資訊安全管理制度相關文件及相關作業受稽核人員進行稽核，文件管理小組另安排陪稽人員，擔

任本所與委託稽核顧問公司溝通橋梁，確保稽核順遂。

戊、本所內部稽核小組，視情況擇派數名觀察員，提升本所內部稽核小組稽核能力與稽核員資格取得。

己、稽核後，由委託稽核顧問公司，製作稽核報告函送本所後，另協調時間到本所，依據本所「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」，提供發現事項矯正措施建議。

2. 委外服務廠商稽核作業委託稽核

(1) 委託稽核時機

甲、本所稽核人力不足人時。

乙、本所稽核專業知識及經驗不足時。

(2) 委託稽核步驟

相關稽核步驟參照本作業說明書「陸、處理原則；三、委外服務廠商稽核；(二)委外稽核作業步驟」。

十八、 矯正與改善

確保本所資訊安全管理制度稽核有效性，作為後續矯正措施活動進行的依據。

(一) 缺失及不符合事項定義說明

1. 缺失：係指公務機關之主管機關(如本所上級主管機關或行政院資通安全處)進行之稽核所發現事項，通常稱為缺失事項。
2. 不符合事項：依據 ISO/CNS27001 標準，進行資訊安全稽核發現事項中不符合項目，述明如下：

(1) 改善機會(Opportunity For Improvement)

甲、組織中其他的流程能因此受益的優良實務。

乙、改善資訊安全管理制度有效性之建議措施。

(2) 觀察事項(Observation)

甲、發現系統/程序有潛在不恰當的情形。

乙、具有潛在資訊安全損失的風險。

丙、提供評審員在後續評審中的參考。

(3) 次要缺失(Minor nonconformity)

甲、單獨違反系統/程序要求事件，且不會引起顯著資訊安全損失的風險。

(4) 主要缺失(Major nonconformity)

甲、系統某程序完全沒有執行， 或同一程序有多個次要缺失使得該程序無法有效執行。

乙、違犯系統/程序要求事件，且會引起顯著資訊安全損失的風險。

丙、存在明顯立即資訊安全損失的風險。

丁、重大資訊安全風險並未被鑑別及檢討改善。

戊、不符合法規(如資通安全管理法、個人資料保護法) 。

己、前一次次要缺失未作改善。

(二) 矯正措施時機的鑑別

遇下列情形時，即應啓動矯正措施：

1. 資訊安全管理制度目標之有效性無法達成。
2. 風險管理控制措施無效。
3. 內部/外部稽核不符合事項。
4. 上級機關進行稽核時發現之缺失時。
5. 發生業務持續計畫中未考慮之重大災難事件。

6. 2 級（含）以上資訊安全事件發生時。

(三) 矯正措施步驟

1. 本所同仁實施資訊安全管理制度，發現有如前所述，影響資訊安全管理制度有效性的事件發生或有可能發生時，應對資訊安全管理制度管理審查委員提出建議，由資訊安全處理小組鑑別是否啓動矯正預防程序。
2. 發現事項中，如有不符合事項中之主要缺失(Major nonconformity)、次要缺失(Minor nonconformity)及上級機關發現事項(缺失項目)均須同時填寫「資訊安全管理制度-實施程序書-矯正措施單(表單編號：DL-ISMS-18_01)」及「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」進行矯正措施管制，如僅不符合事項中之觀察事項(Observation)及改善機會(Opportunity For Improvement)，只需填寫「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」管制矯正所發現事項。
3. 資訊安全處理小組應將需啓動矯正預防程序之項目，填寫於「資訊安全管理制度-實施程序書-矯正措施單(表單編號：DL-ISMS-18_01)」及「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」，並簽報資訊安全處理代表。
4. 負責矯正預防的單位應針對需進行矯正預防的事件進行下列事宜，並將結果記載於「資訊安全管理制度-實施程序書-矯正措施單(表單編號：DL-ISMS-18_01)」及「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」。改善完畢後之「資訊安全管理制度-實施程序書-矯正措施單(表單編號：

DL-ISMS-18_01)」及「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」正本需交由資訊安全管理小組歸檔，另資訊安全稽核小組製作一份送本所主任秘書室一份副本備查。

5. 鑑別出須矯正措施之事件

(1) 分析原因，並記載於「資訊安全管理制度-實施程序書-矯正措施單(表單編號：DL-ISMS-18_01)」及「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」。

(2) 評估可以防止同樣事件再度發生的方法，可分短期方案和長期方案。

(3) 決定採取的矯正措施方案與矯正時程。

(4) 資訊安全處理小組評估矯正措施事件的後續影響，及其他單位或系統是否有類似事件存在，或潛在發生的可能性。

(5) 存在類似事件，或潛在發生的可能性的單位，及執行矯正措施方案的單位在執行矯正措施方案時，如需取得實施矯正措施所需資源時，需提報資訊安全管理代表。

(6) 資訊安全處理小組將複查結果記載於「資訊安全管理制度-實施程序書-矯正措施單(表單編號：DL-ISMS-18_01)」及「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」，並彙整收集矯正改善查核證據，交由文件管理小組存查。

(四) 追蹤查核

1. 資訊安全稽核小組至少每季一次，依據預定完成日期，追蹤查核尚未結案的「資訊安全管理制度-實施程序書-矯正措施摘要表(表

單編號：DL-ISMS-17_04)」狀態，由各項目負責人於每月底提交相關資料予文件管理小組集中管控。

2. 結案的「資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)」簽報資訊安全管理代表後交由文件管理小組歸檔。

(五) 有效性確認

1. 矯正措施執行單位應先自行確認實施結果的有效性。
2. 資訊安全稽核小組複查矯正措施時，應一併確認矯正方案及矯正措施方案的有效性。
3. 訊安全稽核小組應將年度矯正措施的實施結果，於資訊安全管理委員會審查報告，必要時召開會議。

(六) 其他

1. 針對內部稽核結果所列不符合事項，採取矯正措施，以消除不符合之原因；並納入風險評鑑採取預防措施，防止其再次發生。
2. 在績效標準可達成之情況下，仍無法有效達成所擬定之績效標準，須填寫矯正措施處理單進行管理追踪，必要時依其嚴重性給予各單位或人員相關強化措施，例如：再教育訓練等。
3. 矯正與預防措施之狀況須經資訊安全管理審查委員審視確認，如有必要提請資訊安全長召開資訊安全管理審查會並於會議中提報研討與因應作為。

十九、 管理考核

(一) 文件管制

所有資訊安全管理制度相關文件與紀錄均需管制，並依本程序書「陸、處理步驟三、訂定與審視文件與紀錄管制作業」辦理。

(二) 有效性量測

資訊安全管理小組透過資訊機房相關紀錄及資訊安全相關監控記錄與分析報告，定期彙整、審查及評估量測，確認是否達成預期目標，及是否必須修訂資訊安全管理制度目標或風險處理計畫以改善。

(三) 管理階層審查

資訊安全管理制度的執行結果，由資訊安全管理審查委員，至少每年實施一次審視管制，確保資訊安全管理制度的適用性和有效性，同時評估改進資訊安全管理制度的機會，如有必要由資訊安全長召集相關同仁進行資訊安全管理委員會議，召開會相關準備說明如下：

1. 召開管理審查會議，會議前應由資訊安全管理小組發出開會通知單，邀請本所資訊安全組織各成員參加開會。
2. 管理審查會議出席者除本所資訊安全組織成員之外，得要求系統相關人員及視需求邀請專家列席。
3. 管理審查討論之內容應包含如下：
   (1) 過往管理審查之議案的處理狀況。
   (2) 與資訊安全管理制度有關之內部及外部議題的變更。
   (3) 資訊安全績效之回饋，包括下列趨勢：
      A. 不符合項目及矯正措施。
      B. 監督及量測結果。
      C. 稽核結果。
      D. 資訊安全目標之達成。
   (4) 關注方之回饋。
   (5) 風險評鑑結果及風險處理計畫之狀態。
   (6) 持續改善之機會。

4. 管理審查會議依據管理審查討論之內容，應指引出下列主題相關之結論，並留有會議紀錄單，以利後續之改善追蹤。

5. 會議決議事項，交由資訊安全組織架構各小組配合執行及追蹤。

柒、 程序書之修訂及公告

本程序書應由資訊安全管理小組每年定期或因本所組織變革、業務、法令或環境等因素之更迭，適當修訂，並依需求適時通知利害關係人。

捌、 作業表單

一、資訊安全管理制度-實施程序書-推行小組成員暨利害關係人名冊(表單編號: DL-ISMS-02_01)

二、資訊安全管理制度-實施程序書-資訊安全文件一覽表(表單編號: DL-ISMS-03_01)

三、資訊安全管理制度-實施程序書-文件新增變更廢止核准單(表單編號: DL-ISMS-03_02)

四、資訊安全管理制度-實施程序書-管制文件借閱申請登記表(表單編號: DL-ISMS-03_03)

五、資訊安全管理制度-實施程序書-資訊安全外來文件一覽表(表單編號: DL-ISMS-03_04)

六、資訊安全管理制度-實施程序書-個人資料權利行使申請表(表單編號: DL-ISMS-03_05)

七、資訊安全管理制度-實施程序書-組織全景風險評鑑表(表單編號: DL-ISMS-04_01)

八、資訊安全管理制度-實施程序書-組織全景風險鑑別未符合可能衝擊情境分析(表單編號: DL-ISMS-04_02)

九、資訊安全管理制度-實施程序書-安全等級評估表(表單編號:

DL-ISMS-04_03)

十、資訊安全管理制度-實施程序書-資訊系統清冊(表單編號: DL-ISMS-04_04)

十一、 資訊安全管理制度-實施程序書-適用性聲明書（Statement of applicability，SOA）(表單編號: DL-ISMS-04_05)

十二、 資訊安全管理制度-實施程序書-資訊資產分類說明(表單編號: DL-ISMS-05_01)

十三、 資訊安全管理制度-實施程序書-資訊資產清冊(表單編號: DL-ISMS-05_02)

十四、 資訊安全管理制度-實施程序書-資訊資產價值評估標準表(表單編號: DL-ISMS-05_03)

十五、 資訊安全管理制度-實施程序書-資訊資產編號代號編碼原則表(表單編號: DL-ISMS-05_04)

十六、 資訊安全管理制度-實施程序書-資訊資產脆弱點/威脅資料表(表單編號: DL-ISMS-05_05)

十七、 資訊安全管理制度-實施程序書-事件衝擊及發生機率評估表(表單編號: DL-ISMS-05_06)

十八、 資訊安全管理制度-實施程序書-資訊資產風險評鑑表(表單編號: DL-ISMS-05_07)

十九、 資訊安全管理制度-實施程序書-資訊資產風險值統計表暨資訊安全風險分布圖(表單編號: DL-ISMS-05_08)

二十、 資訊安全管理制度-實施程序書-資訊資產既有防護措施表(表單編號: DL-ISMS-05_09)

二十一、資訊安全管理制度-實施程序書-資訊資產既有防護措施識別表(表單編號: DL-ISMS-05_10)

二十二、資訊安全管理制度-實施程序書-資訊資產重新調整之風險評鑑表(表單編號: DL-ISMS-05_11)

二十三、資訊安全管理制度-實施程序書-資訊資產風險因應計畫表(表單編號: DL-ISMS-05_12)

二十四、資訊安全管理制度-實施程序書-目標清單(表單編號: DL-ISMS-06_01)

二十五、資訊安全管理制度-實施程序書-有效性量測表(表單編號: DL-ISMS-06_02)

二十六、資訊安全管理制度-實施程序書-風險評鑑作業(表單編號: DL-ISMS-07_01)

二十七、資訊安全管理制度-實施程序書-維護紀錄表(表單編號: DL-ISMS-08_01)

二十八、資訊安全管理制度-實施程序書-個人資訊設備查核表(表單編號: DL-ISMS-08_02

二十九、資訊安全管理制度-實施程序書-系統服務連結申請表(表單編號: DL-ISMS-09_01)

三十、 資訊安全管理制度-實施程序書-帳號清查紀錄表(表單編號: DL-ISMS-09_02) 資

三十一、訊安全管理制度-實施程序書-帳號清查紀錄表(表單編號: DL-ISMS-09_03

三十二、資訊安全管理制度-實施程序書-應用系統開發/維護申請單(表單編號: DL-ISMS-10_01)

三十三、資訊安全管理制度-實施程序書-資訊安全保密通知書(表單編號: DL-ISMS-11_01)

三十四、資訊安全管理制度-實施程序書-利害關係人/供應商執行人員保密同

意書(表單編號: DL-ISMS-11_02)

三十五、資訊安全管理制度-實施程序書-資訊系統備份作業紀錄表(表單編號: DL-ISMS-12_01)

三十六、資訊安全管理制度-實施程序書-資訊系統備份測試查核表(表單編號: DL-ISMS-12_02)

三十七、資訊安全管理制度-實施程序書-網路服務相關資訊設備及使用 IP 對照表(表單編號: DL-ISMS-12_03)

三十八、資訊安全管理制度-實施程序書-利害關係人/供應商保密切結書(表單編號: DL-ISMS-13_01)

三十九、資訊安全管理制度-實施程序書-業務衝擊分析表（Business Impact Analysis：BIA)(表單編號: DL-ISMS-14_01)

四十、 資訊安全管理制度-實施程序書-業務衝擊風險鑑別原則(表單編號：DL-ISMS-14_02)

四十一、資訊安全管理制度-實施程序書-XXX 年度營運持續災害復原演練範本(表單編號：DL-ISMS-14_03)

四十二、資訊安全管理制度-實施程序書-OOO 年度業務持續演練之災害復原演練報告範本(表單編號：DL-ISMS-14_04)

四十三、資訊安全管理制度-實施程序書-資訊安全事件通報單(表單編號：DL-ISMS-15_01)

四十四、資訊安全管理制度-實施程序書-法規一覽表(表單編號：DL-ISMS-16_01)

四十五、資訊安全管理制度-實施程序書-稽核計畫(表單編號：DL-ISMS-17_01)

四十六、資訊安全管理制度-實施程序書-內部稽核表(表單編號：DL-ISMS-17_02)

四十七、資訊安全管理制度-實施程序書-稽核報告(表單編號：DL-ISMS-17_03)

四十八、資訊安全管理制度-實施程序書-矯正措施摘要表(表單編號：DL-ISMS-17_04)

四十九、資訊安全管理制度-實施程序書-資訊安全管理制度委外服務廠商稽核計畫(表單編號：DL-ISMS-17_05)

五十、 資訊安全管理制度-實施程序書-資訊安全管理制度委外服務廠商稽核報告(表單編號：DL-ISMS-17_06)

五十一、資訊安全管理制度-實施程序書-矯正措施單(表單編號DL-ISMS-18_01)