新北市政府秘書處D級機關共用資通安全維護計畫

目　　錄

壹、依據及目的

本計畫依據資通安全管理法第 13 條及施行細則第 9 條訂定。

貳、適用範圍

本計畫適用範圍為新北市政府秘書處(以下簡稱本機關)。

參、核心業務及重要性

一、核心業務及重要性：

本機關之核心業務、核心資通系統及重要性如下表，並針對全部核心業務訂定營運持續計畫，定期辦理營運持續計畫演練：

序號	科室	核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間(MTPD)	復原時間目標(RTO)	復原點目標(RPO)
1	文檔科	文書法規	無	訂定及解釋本府文書法規	影響本府各機關對文書法規之依據及參考	無	無	無
2	文檔科	監印作業	無	府公文蓋印，使公文書具行政效力與公信力，具以推動執行行政作業	無法確認公文是否依規定完成決行，致使無法用印，影響行政效能	8 小時	12 小時	1 日
3	文檔科	收發文登記與處理	無	點收來文登記與處理、分文（改分文）	影響本府各機關公文時效	無	無	無

4	文檔科	公報業務	無	本府公報為每週發行之法定刊物，統一刊登本市法規、政令、公告及市政會議紀錄，刊登後視為正式公文，不另行文。	公報停辦或錯刊，將使法規無法完成法定公開、政令無法視為正式行文，直接衝擊法令效力與行政效能。	無	無	無
5	文檔科	府公報發行	無	辦理府公報編印、發行，提供公務資訊之正式發布管道。	影響市府政策、法規及重要公告資訊之發布時效與完整性，及各機關及民眾取得正式資訊。	無	無	無
6	文檔科	檔管法規	無	訂定本府檔管法規	影響本府各機關檔案管理之參考	無	無	無
7	文檔科	檔案規劃-編訂機關檔案分類及保存年限區分表	無	訂定本機關檔案分類號及保存年限，作為檔案管理工作執行之依據	影響本機關檔案管理工作執行之依據	無	無	無
8	文檔科	檔案規劃-審核所屬機關檔案分類及保存年限區分表	無	審核並層送本府所屬各機關編製之檔案分類及保存年限區分表，作為該機關檔案管理工作執行之依據	影響所屬各機關檔案管理工作執行之依據	無	無	無
9	文檔科	檔案掃瞄	無	保存檔案電子影像	影響檔案影像儲存作業	1日	1日	2日

10	文檔科	檔案檢調	無	檢取及提供借調或調用檔案	影響調還卷作業	1 日	1 日	3 日
11	文檔科	檔案移交	無	機關改組、裁撤或業務移撥時將檔案完整移交	影響接關機關參考應用相關檔案	無	無	無
12	文檔科	檔案移轉	無	機關永久保存之檔案自產生之日起屆滿 25 年者	國家檔案無法移轉至國家檔案館保存	無	無	無
13	文檔科	檔案目錄彙送	無	落實政府資訊公開，並公布於機關檔案目錄查詢網	影響供民眾查詢與申請應用	無	無	無
14	文檔科	輔導所屬機關參加金檔獎及金質獎	無	表揚推動檔案管理工作績效卓越的機關團體及檔案管理工作上表現優秀的個人（檔管人員）	機關及個人無法參獎	無	無	無
15	文檔科	檔案應用	無	提供檔案應用申請程序相關問題諮詢	影響申請程序疑義之說明	3 日	3 日	3 日
16	文檔科	新北市政府各機關檔案管理標準作業程序	無	本府各機關處理一般及機密公文依據，包括：查詢歷史紀錄、歸檔、清查與檢調作業等。	造成公文歸檔、清查或調閱作業程序非標準化。	24 小時	4 小時	1 小時

17	事務科	財產管理	無	本處財產增置、登記借用、養護、異動、減損、盤點等事項	影響本處財產使用效能及財產管理各項業務之正常運作	無	無	無
18	事務科	物品管理及採購	無	訂定及解釋本府非消耗品法規及本處物品管理及採購事項	影響本府非消耗品法規適用及本處物品管理及採購業務之正常運作	無	無	無
19	事務科	車輛管理	無	公務車管理、調派與維護，確保公務車調派運作順暢。	公務車管派系統失效，將影響各機關車輛管理，無法順利運作。	無	立即	希能立即修復
20	事務科	宿舍管理	無	訂定及解釋本府宿舍法規及本處宿舍借用、管理等事項	影響本府宿舍法規適用及本處宿舍管理各項業務之正常運作	無	無	無
21	事務科	工友管理	無	本府所屬機關工友管理法令解釋諮詢	影響本府所屬機關對工友管理法規之依據及參考	無	無	無
22	事務科	勞健保	無	辦理本處駕駛、技工、工友及臨時人員、約聘僱人員(含眷屬)加(提繳)退(停繳)保事宜及保費預借、繳費、轉正核銷、給付申請等事項。	影響人員投保及給付申請的權益。	無	立即	希能立即修復

23	行政園區管理一科	公共空間管理維護	無	維持行政大樓公共空間之整潔、秩序與環境品質	導致公共區域環境髒亂，降低辦公效率、服務品質與機關形象	48 小時	24 小時	無
24	行政園區管理一科	設備管理維護	無	維護與檢修大樓各項設備，確保日常運作順暢	設備故障停擺造成辦公環境或運作受阻，衍生安全隱患與額外修繕成本	24 小時	24 小時	48 小時
25	行政園區管理一科	行政大樓各項防災安全	無	維護消防、安檢與緊急應變機制，保障大樓人員生命安全與機關資產防護	緊急災害時無法預警或應變，造成人員傷亡、財產重大損失及機關功能停頓	2 小時	2 小時	無
26	行政園區管理二科	公共空間管理維護	無	確保大樓環境整潔與動線順暢，提供良好的洽公與辦公空間。	大樓環境品質下降或設施損壞，影響大樓整體運作與觀感。	48 小時	24 小時	無
27	行政園區管理二科	設備管理維護	無	維持機電、空調等基礎設施穩定運作，確保日常辦公環境。	設備故障導致辦公環境受影響，需額外耗費人力與時間進行維修。	24 小時	24 小時	48 小時
28	行政園區管理二科	行政大樓各項防災安全	無	確保消防與防災設施正常運作，提供安全的辦公環境。	遇突發狀況時影響應變效率，恐導致人員傷亡、重大財產損失。	2 小時	2 小時	無
29	國際科	城市外交	無	辦理姊妹友好城市及國	影響國際城市交流活動之聯繫及辦理，相	無	無	無

				外城市交流相關事宜。	關交流事項可能延後。			
30	國際科	外賓接待	無	辦理外國訪賓與駐臺使節禮貌性拜會府層長官接待事宜。	影響外賓接待及相關拜會行程安排。	無	無	無
31	國際科	國際參與及行銷	無	參與綜合性地方政府國際組織及相關會議與活動，並向國際社會推廣本市施政成果與優質政策。	影響國際組織及相關會議活動之參與，並降低本市施政成果對外交流之機會。	無	無	無
32	機要科	辦理市長題贈各界婚、喪、喜、慶之中堂、輓聯、題詞事項	無	維繫市長與各界之良好互動，樹立市府親民形象。	恐致中堂、輓聯等發送延宕，影響市民觀感與市府公關形象。	無	無	無
33	機要科	市長公共關係招待及府外宴客事宜	無	攸關市長與各界之公共關係及市府形象維繫。	導致對外聯繫中斷，影響市府跨界合作與市政推展，損及市府公關形象。	無	無	無
34	機要科	市長交辦事項處理及市長信函回覆	無	確保首長交辦之專案或緊急陳情事項得以如期完成。	延誤長官交辦重大事項及陳情回覆之時效，嚴重影響整體施政效能。	無	無	無
35	機要科	機要業務處理	無	妥適處理具機密性或重	影響機要事務之保密性與處理時效，衍生	無	無	無

				要性之行政幕僚事務。	內部行政管理風險。			
36	人事室	組織編制及任免遷調	無	辦理本處組織編制及任免遷調業務	影響本處組織編制及任免遷調業務辦理期程	無	無	無
37	人事室	差勤考核及訓練進修	無	辦理本處差勤考核及訓練進修業務	影響本處差勤考核及訓練進修業務辦理期程	無	無	無
38	人事室	待遇福利及退休撫卹	無	辦理本處待遇福利及退休撫卹業務	影響本處待遇福利及退休撫卹業務辦理期程	無	無	無
39	會計室	歲計	無	(一) 年度概算及追加(減)預算之籌編。 (二) 分配預算之彙編。	如未妥適辦理預算籌編及分配作業，將影響本處經費配置及預算執行，並可能造成各項業務無法依原訂計畫及期程推動。	24 小時	24 小時	5 日
40	會計室	會計	無	(一) 會計憑證、記帳憑證之編製、審核與保管。 (二) 財務上增進效能及減少不經濟支出之改進建議。 (三) 各項採購案之監辦。 (四) 會計月	如相關會計、財務及採購監辦作業未妥適執行，可能造成帳務處理錯誤、經費支用或採購程序不符規定，影響財務資訊正確性、預算執行及決算作業，並增加後續查核風險。	24 小時	24 小時	5 日

				報、半年報與決算報告之編製。				
41	會計室	統計	無	(一) 公務統計方案之覆核、稽、彙整。 (二) 公務統計報表之管理。	如未確實辦理統計資料覆核、彙整及報表管理，可能造成統計資料錯漏或未能如期提供，影響統計資訊之正確性、完整性及後續業務分析運用。	24 小時	24 小時	5 日
42	政風室	政風查處	無	貪瀆及不法事項之處理	影響機關廉潔、危害社會公平正義及降低行政效率。	無	無	無
43	政風室	政風預防	無	廉政宣導及推動、公職人員財產申報審查及利益衝突迴避處理	一、無法發現短漏報與隱匿財產。另未經審查會使得財產異常增加的來源無法被釐清，喪失阻絕貪腐的預警功能。 二、若未依法執行迴避，或機關的迴避機	無	無	無

					制因故失效，將產生嚴重的法律效力瑕疵與行政處罰。			
44	政風室	安全與機密維護	無	維護機關安全及防止機密資料外洩，避免民眾權益受損。	導致公務機密外洩、行政效能下降、資產損失、機關形象受損，甚至危害人員安全。	無	無	無

二、非核心業務及說明：

本機關之非核心業務及說明如下表：

序號	科室	非核心業務	資通系統	業務失效影響說明	最大可容忍中斷時間(MTPD)	復原時間目標(RTO)	復原點目標(RPO)
1	文檔科	性平業務	無	影響本機關內部性平業務之推展	48 小時	72 小時	5 日
2	文檔科	各機關申請製（換）發及繳銷印信作業	無	影響文書作業時間	48 小時	72 小時	3 日
3	文檔科	研資考評業務	無	辦理研資考評及為民服務資料彙整、提報等相關業務，提供本處業務績效及服務品質評估所需資料。	無	無	無

4	文檔科	議會相關業務	無	影響市府與議會間資訊傳遞及業務聯繫，造成議會資料提供、案件回復及相關作業延誤(如施政報告、業務報告、議會紀錄、經建考察案件)。	無	無	無
5	文檔科	施政計畫業務	無	影響本處施政計畫提報及列管案件進度追蹤，造成施政管考作業延誤。	無	無	無
6	文檔科	施政成果業務	無	影響施政成果彙整、提報進度追蹤，造成施政成果資訊更新及管考作業延誤。	無	無	無
7	文檔科	志工業務	無	影響本機關每月時數登錄	30 日	30 日	30 日
8	文檔科	公文通訊錄系統維護管理	無	影響本府各機關發文作業	24 小時	4 小時	48 小時
9	文檔科	處務會議	無	導致處內政令傳達短暫延遲、會議延期， 但各科室仍可獨立運作，衝擊範圍僅限於機關內部。	5 日	48 小時	24 小時
10	文檔科	檔案管理輔導考評	無	無	無	無	無
11	文檔科	檔案鑑定	無	影響本機關檔案清理作業之進行	48 小時	72 小時	5 日
12	文檔科	檔案銷毀業務	無	影響庫房空間釋出	無	無	無
13	事務科	新北電聯網	無	影響機關智慧電錶業務	24 小時	48 小時	3 日
14	機要科	財產管理登記(含府本部資訊設備)	無	影響科內財產帳物盤點與府本部資訊設備管理之準確性。	72 小時	5 日	7 日
15	機要科	庫存物品管理及備品採購	無	影響科內日常辦公用品、年節禮品及物資之補充，造成內部行政作業不便。	72 小時	5 日	7 日
16	機要科	人事、加班費及出差費業務	無	影響科內同仁及府本部人員之差勤核銷及權益。	48 小時	72 小時	5 日

17	機要科	研考業務及其他內部綜合行政	無	影響科內公文管考及日常行政作業之流暢度。	48 小時	72 小時	5 日
18	會計室	憑證銷毀	無	如未依規定辦理檔案銷毀作業，可能造成逾保存年限檔案未妥適清理，增加檔案管理及儲存負擔。	48 小時	72 小時	5 日

肆、資通安全政策及目標

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），並符合相關法規之要求，特制訂本政策如下，以供全體同仁共同遵循。

（一） 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

（二） 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

（三） 應強固核心資通系統之韌性，確保機關業務持續營運。

（四） 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。

（五） 針對辦理資通安全業務有功人員應進行獎勵。

（六） 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

（七） 禁止多人共用單一資通系統帳號。

二、資通安全目標

(一) 量化型目標

1. 知悉資安事件發生，未能於規定的時間完成通報、應變及復原作業次數為 0。

2. 電子郵件社交工程演練之郵件開啟率及點閱率分別低於 5%及

2%。

3. 個人電腦中毒數量每月平均 5%以下。

(二) 質化型目標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

3. 提升人員資安防護意識、有效偵測與預防外部攻擊。.

三、資通安全政策及目標之核定程序

資通安全政策由本機關資安業務主辦單位簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 本機關之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。

2. 本機關應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。

伍、資通安全推動組織

一、資通安全長

依資通安全管理法第 12 條之規定，本機關訂定副首長或適當人員為資通安全長，負責督導機關資通安全相關事項，其任務包括：

(一)資通安全管理政策及目標之核定、核轉及督導。

(二)資通安全責任之分配及協調。

(三)資通安全資源分配。

(四)資通安全防護措施之監督。

(五)資通安全事件之檢討及監督。

(六)資通安全相關規章與程序、制度文件核定。

(七)資通安全管理年度工作計畫之核定。

(八)資通安全相關工作事項督導及績效管理。

(九)其他資通安全事項之核定。

二、資通安全推動小組

(一) 組織

為推動本機關之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各業務部門主管/副主管以上之人員代表成立資通安全推動小組[1]，其任務包括：

1. 跨部門資通安全事項權責分工之協調。

2. 應採用之資通安全技術、方法及程序之協調研議。

3. 整體資通安全措施之協調研議。

4. 資通安全計畫之協調研議。

5. 其他重要資通安全事項之協調研議。

(二) 分工及職掌

本機關之資通安全推動小組依下列分工責任分組，並依資通安全長之指示負責下列事項，本機關資通安全推動小組人員名單及職掌應列冊，並適時更新之[2]：

1. 執行秘書：

負責襄助資通安全長與督導資通安全相關工作事宜，包含召集會議、決議事項追蹤管理、交辦之其他管理事項等。

2. 資通安全處理分組：

[1] 資通安全推動小組成員由機關之資通安全長召集組成，依資通安全長之指示，負責協助或與機關內之相關單位合作推動機關內部之資通安全業務，如機關未成立資通安全推動小組，相關業務則應由資通安全長責承相關資通安全權責人員辦理之。

[2] 各公務機關應製作「資通安全推動小組成員及分工表」，說明小組成員及相關職掌，格式可參附件：資通安全推動小組成員及分工表。

(1) 風險管理及法律遵循：負責資訊資產盤點風險管理作業，包含資訊資產清冊之維護、弱點與威脅調查、風險評估、風險處理計畫之擬定與進度追蹤等。並負責規劃及辦理資通安全管理適法性之識別、相關爭訟（議）案件之協調處理，並配合司法單位調查之進行，提供必要資源等。

(2) 推動及執行：負責建置資通安全管理措施、執行安全監控、程序文件修訂及管制、規劃教育訓練計畫及相關宣導事項之辦理、建立資通安全維護計畫等相關規範，推動資通安全業務，彙整實施成果等。

3. 危機應變分組：

負責執行資通安全危機應變、管理系統範圍之營運持續管理作業，包含營運衝擊分析、營運持續計畫、事件通報應變程序及相關演練活動等。

4. 稽核分組：

負責規劃與執行資通安全稽核作業，包含稽核計畫之撰寫檢查表之擬定、稽核人員之遴選、稽核發現之改善追蹤等。

陸、專職人力及經費配置

一、專職人力及資源之配置

（一）本機關依資通安全責任等級分級辦法之規定，屬資通安全責任等級 D 級，無須設置資通安全專職人員。本機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽上級機關相關專職人員或請相關學者專家或專業機關（構）提供顧問諮詢服務。

（二）本機關之首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。

（三）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。

二、經費之配置

（一）資通安全推動小組於規劃配置相關經費及資源時，應考量本機關之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[3]。

(二)各單位於規劃建置資通系統建置時，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。

(三)各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出[4]，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

(四)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。

柒、資通系統及資訊之盤點

一、資通系統及資訊盤點

本機關每年辦理資通系統及資訊資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為人員資產、資訊資產、軟體資產、實體資產、建築與保護資產、服務資產、支援服務資產等。

(一)資通系統及資訊資產項目如下：

1. 人員資產：內部人員、外部人員（含委外人員）等。
2. 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。
3. 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。
4. 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。
5. 建築與保護資產：辦公區域、資訊機房、檔案室區域、倉庫/庫房、建築保護設施等。
6. 服務資產：內外部服務、委外服務、雲端服務等。
7. 支援服務資產：相關基礎設施級其他機關內部之支援服務，

[3] 為有效建置機關之資通安全風險防護機制，公務機關應投入相當之資源，故機關之資通安全推動小組於資源規劃或編制預算時，應考量機關之責任等級、資通安全政策及目標。

[4] 各機關可填具資通安全需求申請單，格式可參附件：資通安全需求申請單。

如電力、消防等。

(二)本機關每年度應依資訊及資通系統盤點結果，製作「資通系統及資訊資產清冊」，欄位應包含：資產名稱、資產類別、擁有者、管理者、使用者、存放位置、資產說明、機密性、完整性、可用性、法律遵循性、資產價值等級、防護需求等級。

(三)本機關依前揭盤點結果，倘發現機關有下載、安裝或使用危害國家資通安全產品（含大陸、香港或澳門廠牌資通訊產品）時，應確認下列事項：

1. 自 114 年 12 月 1 日資通安全管理法修正施行後，凡下載、安裝或使用之產品，應依規定向主管機關申請專案核准使用；未經主管機關核定之產品，應即刻移除、解除安裝或停止使用。倘因使用未經核定之產品，致有影響機關資通安全之虞，本機關得依資通安全管理法第 28 條規定，對相關人員予以懲戒或懲處。

2. 機關現存之危害國家資通安全產品（含軟體、硬體及服務），應依「危害國家資通安全產品審查辦法」第 7 條規定，採取相關必要之管控措施。

(四)伺服器、網路設備、桌上型電腦、筆記型電腦等之硬體類資產，應將可供識別之資產清冊資訊以適當方式或財產標籤標示於硬體外觀（如：財產編號、財產名稱、財產別名、購買日期、年限、保管單位等），以供區別。核心資通系統及相關資產，並應加註標示。

(五)為確保使用物聯網（IoT）裝置安全，避免不當使用，遭受蓄意資料竊取、遺失或惡意程式入侵等資通安全事件發生，每年度應盤點 IoT 裝置，並針對網路印表機、門禁設備、網路攝影機、無線網路基地台/無線路由器、環控系統、網路儲存伺服器（NAS）等進行資安檢核。

(六)各單位管理之資通系統或資訊資產如有異動，應即時通知資通安全推動小組更新資產清冊。

二、機關資通安全責任等級分級

本機關因無維運自行或委外開發之資通系統，為資通安全責任等級 D 級機關。

捌、資通安全風險管理

一、本機關應每年針對資訊及資通系統資產進行風險評估。

二、執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

玖、資通安全防護及控制措施

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項，採行相關之防護及控制措施如下：

一、技術面－資通安全防護

本機關應完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級，項目如下：

(一)防毒軟體。

(二)網路防火牆。

二、認知與訓練－實施資通安全教育訓練。

三、資訊及資通系統之管理

(一) 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

(二) 資訊及資通系統之使用

1. 本機關同仁使用資訊及資通系統前應經其管理人授權。
2. 本機關同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本機關同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

4. 非本機關同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。

5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

(三) 資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。

2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。

3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

四、存取控制與加密機制管理

(一) 網路安全控管

1. 本機關之網路區域劃分如下：

(1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

(2) 非軍事區(DMZ)：放置機關對外服務伺服器之區段。

(3) 內部區域網路(Local Area Network, LAN)：機關內部單位人員及內部伺服器使用之網路區段。

2. 外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。

4. 對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。

5. 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

6. 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

7. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

8. 網域名稱系統(DNS)防護

   (1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

   (2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

   (3) DNS 伺服器應設定指向 GSN Cache DNS。(公務機關適用)

   (4) 內部主機位置查詢應指向機關內部 DNS 伺服器。

9. 無線網路防護

   (1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。

   (2) 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

   (3) 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

   (4) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二) 資通系統權限管理

1. 本機關之資通系統應設置通行碼管理，通行碼之要求需滿足：

   (1) 通行碼長度 8 碼以上。

   (2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

   (3) 使用者每 180 天應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

(三) 特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通系統之特權帳號不得共用。

3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者ID。

4. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5. 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四) 加密管理

1. 本機關之機密資訊於儲存或傳輸時應進行加密。

2. 本機關之加密保護措施應遵守下列規定：

(1) 應落實使用者更新加密裝置並備份金鑰。

(2) 應避免留存解密資訊。

(3) 一旦加密資訊具遭破解跡象，應立即更改之。

五、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

(1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

(3) 確實執行網頁惡意軟體掃描。

2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

3. 使用者不得私自使用已知或有嫌疑惡意之網站。

4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體

利用系統或軟體漏洞進行攻擊。

(二) 遠距工作之安全措施

1. 本機關資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

   (1) 提供適當通訊設備，並指定遠端存取之方式。

   (2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

   (3) 進行遠距工作時之安全監視。

   (4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三) 電子郵件安全管理

1. 本機關人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。

2. 電子郵件系統管理人應定期進行電子郵件帳號清查。

3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。

4. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

5. 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

6. 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

7. 使用者應確保電子郵件傳送時之傳遞正確性。

8. 使用者使用電子郵件時，應注意電子簽章之要求事項。

9. 本機關應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。

(四) 確保實體與環境安全措施

辦公室區域應遵守以下實體與環境安全措施：

1. 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
2. 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
3. 機密性及敏感性資訊，不使用或下班時應該上鎖。
4. 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
5. 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
6. 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。
7. 敏感或機密性資訊之備份應加密保護。

(五) 媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(六) 電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

5. 下班時應關閉電腦及螢幕電源。

6. 如發現資安問題，應主動循機關之通報程序通報。

7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

(七) 行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。

2. 機敏會議或場所不得攜帶未經許可之行動設備進入。

(八) 即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

2. 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：

(1) 用戶端應有身分識別及認證機制。

(2) 訊息於傳輸過程應有安全加密機制。

(3) 應通過經濟部工業局行動應用App基本資安檢測基準版本L2檢測項目。

(4) 伺服器端之主機設備及通訊紀錄應置於我國境內。

(5) 伺服器通訊紀錄（log）應至少保存六個月。

六、系統獲取、開發及維護

本機關無維護、自行或委外開發資通系統。

七、營運持續計畫演練

本機關無核心資通系統。

八、資通安全防護設備

1. 本機關應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本機關應訂定資通安全事件通報、應變及演練相關機制，詳新北市政府所屬各機關資通安全事件通報及應變管理程序。

壹拾壹、資通安全情資之評估及因應機制

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本機關接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、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識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情

資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

二、資通安全情資之因應措施

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四) 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理措施

(辦理委外作業者，適用本項管理)

本機關委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需

求，選任適當之受託者，並監督其資通安全維護情形。

一、選任受託者應注意事項

(一)受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

(二)受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

(三)受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

(四)受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦理該項業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

(五)前點適任性查核得在必要範圍內就下列事項查核，查核前應經當事人書面同意：

1. 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。

2. 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。

3. 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。

4. 其他與國家機密保護相關之具體項目。

二、監督受託者資通安全維護情形應注意事項

(一)安全性檢測要求：受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及核心資通系統或委託金額達新臺幣一千萬元以上者，本機關應自行或另行委託第三方進行安全性檢測。涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

(二)通報與應處機制：受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

(三)資料處理與移轉：委託關係終止或解除時，應確認受託者返

還、移交、刪除或銷毀履行委託契約而持有之資料。

(四)稽核與監督：本機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形[5]。

(五)其他資安維護措施：受託者應採取之其他資通安全相關維護措施[6]。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

本機關依資通安全責任等級分級屬 D 級，本機關之一般使用者與主管，每人每年接受 3 小時以上之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式

(一)承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

(二)本機關資通安全認知宣導及教育訓練之內容得包含：

1. 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
2. 資通安全法令規定。
3. 資通安全作業內容。
4. 資通安全技術訓練。

(三)員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

(四)資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

[5] 受託業務稽核可參考「數位發展部辦理政府機關受託者資通安全聯合稽核計畫」辦理。

[6] 公務機關與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書、保密同意書，格式可參附件：委外廠商執行人員保密切結書、保密同意書。

壹拾肆、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本機關所屬人員辦理業務涉及資通安全事項，依資通安全管理法第 18 條第 1 項及第 28 條第 1 項規定，績效優良者，應予獎勵；未依該法規定辦理者，應按其情節輕重，依相關規定予以懲戒或懲處。

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員辦理資通安全事項作業辦法、新北市政府及所屬各機關學校公務人員平時獎懲基準及本機關各相關規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

一、資通安全維護計畫之實施

為落實本安全維護計畫，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 資通安全推動小組得於視需要(例如本府系統重大變更、本機關組織改造或其他事由)執行內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

3. 辦理稽核時，資通安全推動小組應於執行稽核前 30 日，通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

4. 本機關之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。

5. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之

相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

4. 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、資通安全維護計畫之持續精進及績效管理

(一) 本機關之資通安全推動小組每年至少召開一次資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

(二) 管理審查議題應包含下列討論事項：

1. 過往管理審查議案之處理狀態。

2. 法遵事項實施情形。

3. 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

4. 資通安全維護計畫內容之適切性。

5. 資通安全績效之回饋，包括：

(1) 資通安全政策及目標之實施情形。

(2) 資通安全人力及資源之配置之實施情形。

(3) 資通安全防護及控制措施之實施情形。

(4) 內部稽核、外部稽核、演練結果。

(5) 不符合項目及矯正措施。

6. 風險評鑑結果及風險處理計畫執行進度。

7. 重大資通安全事件之處理及改善情形。

8. 利害關係人之回饋。

9. 持續改善之機會。

(三) 持續改善機制之管理審查應做成改善績效追蹤報告[7]，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本機關依據資通安全管理法第 14 條之規定，每年按上級機關指定期限，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾柒、相關法規、程序及表單

一、相關法規及參考文件

(一) 資通安全管理法

(二) 資通安全管理法施行細則

(三) 資通安全責任等級分級辦法

(四) 資通安全事件通報應變及演練辦法

(五) 資通安全維護計畫實施情形稽核辦法

(六) 資通安全情資分享辦法

(七) 公務機關所屬人員辦理資通安全事項作業辦法

(八) 危害國家資通安全產品審查辦法

(九) 國家資通安全會報設置辦法

(十) 新北市政府及所屬各機關學校公務人員平時獎懲基準

[7] 格式可參附件：改善績效追蹤報告。

(十一) 新北市政府所屬各機關資通安全事件通報及應變管理程序

二、附件表單

(一) 資通安全推動小組成員及分工表

(二) 資通安全需求申請單

(三) 資通安全維護計畫實施情形

(四) 稽核項目紀錄表

(五) 稽核委員聘任同意保密切結書

(六) 稽核結果及改善報告

(七) 改善績效追蹤報告

壹拾捌、目次

1. 通安全推動小組成員及分工表

○○○（機關名稱）資通安全推動小組成員及分工表

編號：○○

製表日期：○○○○年○○月○○日

單位職級	名稱	職掌事項	分機	備註（代理人）
EX：資訊室專員	王○○	資通安全事件通報	○○	王○○

資通安全長：○○○

註：陳核層級請機關依需求調整

2. 資通安全需求申請單

○○○（機關名稱）資通安全需求申請單

編號：○○

申請單位	○○部門	**申請日期**	○○○年○○月○○日
申請項目	■軟體 □硬體 □其他	**項目名稱**	○○防毒軟體
申請數量	1	**需用日期**	○○○年○○月○○日
申請類別	■新購 □升級	**使用設備**	■主機 □使用者電腦 □其他
安裝單位	資訊室	**安裝位置**	機房
用途說明	防毒軟體更新		
申請人	○○○	**單位主管**	○○○
資通安全推動小組	■可採購 □不可採購	說明：	
資通安全推動小組承辦人員	○○○	**資通安全長**	○○○

註：陳核層級請機關依需求調整

3. 資通安全維護計畫實施情形

○○○（機關名稱）資通安全維護計畫實施情形

編號：○○○

本機關（單位）之業務因涉及全國性民眾個人資料檔案之持有及處理，經主管機關核定後本單位之資通安全責任等級為 A 級 ，依資通安全管理法第 14 條之規定，向 鈞部（院）提出本（○○○）年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明 （下列內容為範例，請機關依自身情形填寫對應的說明，並提供證明，如計畫、程序、記錄或相關公文等）
1. 核心業務及其重要性	1. 核心業務及重要性盤點	本機關核心業務及重要性詳參資通安全維護計畫（詳附件，下同）。
2. 資通安全政策及目標之訂定	1. 資通安全政策訂定及核定	本機關已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定（詳公文附件）。
	2. 資通安全目標之訂定	本機關已訂定資通安全目標，詳參資通安全維護計畫。
	3. 資通安全政策及目標宣導	本機關為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	4. 資通安全	本機關已定期召開資通安全管

	政策及目標定期檢視	理審查會議中檢討資通安全政策及目標之適切性 （詳會議記錄） 。
3. 設置資通安全推動組織	1. 設定資通安全長	本機關已指定○○長為資通安全長，其職掌詳參資通安全維護計畫。
	2. 設置資通安全推動小組	本機關已設置資通安全推動小組，其組織、分工及職掌詳參資通安全維護計畫。
4. 專職人力及經費之配置	1. 專職人員配置	本機關依規定配置資通安全專職人員四人以上，並具備資通安全專業證照及資通安全職能評量證書各四張以上。另因其業務內容將涉及機密性資料，故已進行相關安全評估。
	2. 經費之配置	本機關今年視需求已合理分配資安經費，資安經費佔資訊經費之○○%。
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	1. 資訊及資通系統之盤點	本機關已於今年○月盤點本機關之資訊、資通系統，建立資產目錄。
	2. 機關資通安全責任等級分級	本機關依資通安全責任等級分級辦法，為資通安全責任等級A級機關。
6. 資通安全風險評估	1. 資通安全風險評估	本機關已於今年○月完成本機關之資訊、資通系統及相關資產之風險分析評估及處理。

	2. 資通安全風險之因應	本機關已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	1. 管理面	本機關已依安全維護計畫辦理，詳附件資料。
	2. 技術面	本機關已依安全維護計畫辦理，詳附件資料。
	3. 認知與訓練	本機關已依安全維護計畫辦理，詳附件資料。
	4. 存取控制與加密機制管理	本機關已依安全維護計畫辦理，詳附件資料。
	5. 作業與通訊安全管理	本機關已依安全維護計畫辦理，詳附件資料。
	6. 資通系統獲取、開發及維護	本機關已依安全維護計畫辦理，詳附件資料。
	7. 實體與環境安全管理程序	本機關已依安全維護計畫辦理，詳附件資料。
	8. 人員安全管理	本機關已依安全維護計畫辦理，詳附件資料。

8. 資通安全事件通報、應變及演練相關機制	1. 訂定資通安全事件通報、應變及演練相關機制	本機關已依規定訂定資通安全事件通報應變程序。(詳附件)
	2. 資通安全事件通報、應變及演練	本機關已依規定進行資通安全事件通報。 本機關已依規定於今年○、○月辦理社交工程演練，並於○月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	1. 資通安全情資之分類評估	本機關接受情資後，已進行分類評估。
	2. 資通安全情資之因應措施	本機關已接受情資之分類，採取對應之因應措施。
10. 資通系統或服務委外辦理之管理措施	1. 選任受託者應注意事項	本機關資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	2. 監督受託者資通安全維護情形應注意事項(建議可參考本年度受託者聯合稽核計畫之查檢表	本機關已依規定監督受託者資通安全維護情形，客製化資通系統開發者 ，已要求其出具安全性檢測證明....(請機關依實際情形列出)。

	修正)	
11.資通安全教育訓練	1. 資通安全教育訓練要求	本機關人員已依規定進行資通安全教育訓練。
	2. 辦理資通安全教育訓練	本機關已於今年○月辦理資通安全教育訓練。
12.公務機關所屬人員辦理業務涉及資通安全事項之考核機制	1. 訂定考核機制並進行考核	本機關已建立考核機制，並已依規定進行平時及年終考核。
13.資通安全維護計畫及實施情形之持續精進及績效管理機制	1. 資通安全維護計畫之實施	本機關已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。
	2. 資通安全維護計畫實施情形之稽核機制	本機關已依規定辦理內部稽核。
	3. 資通安全維護計畫之持續精進及績效管理	本機關已依規定辦理內部召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

其他說明	

單位主管：陳○○ 資通安全長：陳○○

註：陳核層級請機關依需求調整

4. 稽核項目紀錄表

○○○（ 機關名稱）稽核項目紀錄表

稽核日期：○○○年○○月○○日

稽核範圍：全機關

項次	稽核項目	符合	部分符合	不符合	不適用	稽核發現
1	EX：是否盤點全機關業務，並進行營運衝擊分析，以識別核心及非核心業務，且盤點對應之資通系統？					
2						
3						
4						
5						

註：陳核層級請機關依需求調整

第二方稽核之稽核項目檢核表，請參考數位發展部資通安全署官網，年度資通安全稽核計畫附件

5. 稽核委員聘任同意暨保密切結書

○○○(機關名稱）○○○（計畫名稱）

稽核委員聘任同意暨保密切結書

本人＿＿＿＿＿＿（以下簡稱甲方）為協助○○○（以下簡稱乙方）執行「○○○」(以下簡稱本計畫)，接受乙方之邀請，擔任○○○年資安稽核團隊之稽核委員，特立書同意事項如下：

1. 甲方應遵守國家機密保護法、個人資料保護法、著作權法及其他相關法令之規定，並對因執行本計畫或因執行本計畫之機會所知悉之機密資訊負有保密義務；且上開各義務不因甲方與乙方，就本年度擔任稽核委員相關事宜之法律關係解除、終止或完成而失其效力。

2. 甲方就因執行本計畫或因執行本計畫之機會，所知悉或接觸之乙方、受稽機關或其他第三人之機密資訊，除因執行本計畫所必須，且事先經乙方書面同意者，或法律另有明文規定外，不得有下列行為：

    1. 全部或一部重製或留存上開機密資訊；

    2. 以任何方式向任何第三人揭露上開機密資訊之全部或一部；

    3. 以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；

    4. 以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；

    5. 揭露、公開或使用上開機密資訊之全部或一部。

3. 甲方因執行本計畫所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬乙方所有。

4. 甲方與受稽機關有下列情形之一者，就與該受稽機關之稽核相關事宜，應主動迴避，或事先以書面告知乙方，以確認是否得免予迴避：

    1. 甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人，與受稽機關間，有財產上或非財產上利益之利害關係者；

2. 甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬，與受稽機關或其負責人間現有或於過去兩年間曾有僱傭、承攬、委任、代理或其他類似之關係者；

3. 甲方或其現任職或於過去兩年內曾任職之機關，於民國○○○年至本次稽核期間，曾為受稽機關進行與受稽事項相關之顧問輔導者。

5. 前條所稱財產上利益，係指動產、不動產、現金、有價證券、債權、其他財產上權利、具有經濟價值或得以金錢交易取得之利益；所稱非財產上利益，係指有利於甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人於受稽機關或其關聯機關之任用、陞遷、調動及其他人事措施。

6. 有其他情形足認甲方有不能公正執行職務之虞，經受稽機關敘明理由，並由乙方作成迴避決定者，甲方應迴避之。

7. 甲方有第四條各款情形之一，而未自行迴避，亦未事先以書面告知乙方相關情事，並經乙方書面同意免予迴避者，乙方得終止本契約，甲方應返還已收取之報酬，如乙方，因此認有必要對受稽核機關重為全部或一部稽核，或受有其他不利益時，甲方並應賠償乙方因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

8. 甲方如違反第二條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致乙方、受稽機關，遭受任何不利益，或受第三人法律上請求或訴追者，甲方應賠償乙方、受稽機關，因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

9. 甲方應公正執行職務，並應避免使人誤認推薦特定廠商、產品或服務；且處理稽核相關事務或出席會議，應親自為之。

此　致

○○○（機關名稱）

受稽機關
立同意書人
姓　　名：　　（簽章）
身分證字號：

中　華　民　國○○○年○○月○○日

6. 稽核結果及改善報告

○○○（機關名稱）稽核結果及改善報告

稽核範圍	全機關			
稽核日期	○○○ 年 ○○ 月 ○○ 日			
審查日期	○○○ 年 ○○ 月 ○○ 日			
改善措施				
編號	**稽核缺失或待改善稽核項目**	**改善措施**	**改善期程規劃**	**相關證明資料**
1				
2				
3				
4				
5				
6				
7				
8				

單位主管：陳○○ 資通安全長：陳○○

註：陳核層級請機關依需求調整

7. **改善績效追蹤報告**

○○○（機關名稱）改善績效追蹤報告

編號：○○

製表日期：○○○○

稽核發現			
稽核日期	○○○ 年 10 月 20 日 08 時	受稽核單位	○○○
稽核區域	■ 電腦機房 委外業務之監督措施 自動備份系統之安全措施		
缺失或待改善項目與內容	待改善項目：電腦機房所設置之預備電源設備老舊。 缺失項目：委外廠商未定期保養相關設備。		
影響範圍評估	將影響電腦機房之運作及相關非核心系統之線上服務之提供。		
發生原因分析	未落實監督委外廠商管理之責任。		
改善措施成效追蹤			
改善措施		**預計成效**	**執行情況**
管理面	定期進行委外廠商承辦人員之教育訓練，已落實對委外廠商之監督責任。	要求委外廠商每季進行保養，並提供相關保養紀錄。	已與委外廠商接洽。

技術面			
人力面			
資源面	更新相關電腦機房設備，並確保備份設備及機制運作效果。	電腦機房電源設備更新，並採用不斷電系統，於停電時可維持 12 小時運作。	已進行採購作業。
作業程序			
其他			

績效管考			
改善措施確認	■合格／完成 □待追蹤（追蹤期限：_年_月_日） □不合格（說明：_）		
經費需求或編列執行金額	○○○萬元。	經費執行情形	已進行相關電腦機房設備更新採購，共執行○○萬元。
預定完成日期	○○○ 年 11 月 20 日	實際完成日期	○○○ 年 11 月 20 日

完成進度或情形說明	定期檢視委外廠商之監督維護責任。		
改善成效考核			
後續成效追蹤			
資通安全推動小組	○○○	資通安全長[1]	○○○

註：陳核層級請機關依需求調整

1 特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。