|  |  |  |  |
| --- | --- | --- | --- |
| **實施項目** | **實施內容** | **辦理情形** | **審核意見** |
| 1.核心業務及其重要性 | 1.1核心業務及重要性盤點？註：有關核心業務及核心資通系統之定義，請參考資通安全管理法施行細則第7條 | 110年盤點機關核心業務計項 項 未盤點機關核心業務，原因為： 補充說明(選填)： |  |
| 2.資通安全政策及目標之訂定 | 2.1資通安全政策訂定及核定？註：資安政策參考範例如下1.符合法令與法規要求2.落實資通安全教育訓練，以提高員工之資訊安全意識3.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 | (單選)本機關資通安全政策為：  本機關資通安全政策訂定於文件內(編號、名稱及章節)： 未訂定，原因為： 補充說明(選填)： |  |
| 2.2 資通安全目標之訂定？註：資通安全目標參考範例如下1.同仁皆達到資安時數2.同仁社交工程點閱及開啟連結率符合要求。 | (單選)本機關資通安全目標為： 本機關資通安全目標訂定於文件內(編號、名稱及章節)： 未訂定，原因為： 補充說明(選填)： |
| 2.3 資通安全政策及目標宣導？註：宣導方式包含：函知各單位、會議宣導、網站公告、教育訓練、辦理測驗等。 | (單選)已向同仁宣導，方式為： 未宣導，原因為： 補充說明(選填)： |
| 2.4 資通安全政策及目標定期檢視註：1.會議如管審會、月會、季報、年度會議等2.核定主管請依【姓名+職稱】方式填寫，如王小明副局長 | (單選)本機關110年資安政策及目標檢視方式為：於會議中檢視，會議名稱為：  (如管審會、月會、季報、年度會議等) 簽陳主管核定，核定主管為： (姓名+職稱，如王小明副局長)未檢視，原因為： 補充說明(選填)： |
| 3.設置資通安全推動組織 | 3.1設定資通安全長 註：資通安全長管請依【姓名+職稱】方式填寫，如王小明副局長 | (單選) 本機關110年資通安全長為 (姓名+職稱，如王小明副局長) 未設資通安全長(未符法遵)，原因為： 補充說明(選填)： |  |
| 3.2 設置或加入資通安全推動小組 | (單選)本機關參與之資安推動組織如下： 自行簽辦設置，110年計開會  次，本機關資安長親自出席 次。 參與其他機關推動組織，主政機關為  ，110年計開會 次，本機關資安長親自出席次。 無設置且無參加(其他)機關資安推動組織，原因為： 補充說明(選填)： |
| 4.專責人力及經費之配置 | 4.1專職(責)人員配置註：總員額包含正職、約聘、約僱、約用等人員 | 本機關總預算員額計  人，資訊人員計  人， 無須配置資安專職人員，本機關資安相關業務承辦人數為： 補充說明(選填)： |  |
| 4.2 經費之配置 | 詳本機關[附表2-經費配置](https://spm.nat.gov.tw/ManageMPIS110/MPIS110FundingEdit.aspx?ReplyedOID=2.16.886.111.90011.100021&AuditedOID=2.16.886.111.90011.100021&AuditedYear=2021)補充說明(選填)： |  |
| 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 | 5.1 資訊及資通系統之盤點 | 詳本機關 [附表3-資通系統資產清冊](https://spm.nat.gov.tw/ManageMPIS110/MPIS110InfoSysReply.aspx?ReplyedOID=2.16.886.111.90011.100021&AuditedOID=2.16.886.111.90011.100021&AuditedYear=2021)補充說明(選填)： |  |
| 6.資通安全風險評估 | 6.1 資通安全風險評估及因應？註：風險評估結果範例：人員共用帳號、點選未經識別或不受信任的連結...。 風險之因應範例：提升人員資安意識、敘明於機關資安政策並宣導，以降低風險。 | (單選) 本機關資安風險評估結果為：  ，因應措施為 評估結果及因應措施載明於文件內(編號、名稱及章節)：  無進行風險評估及因應，原因為： 補充說明(選填)： |  |
| 7.資通安全防護及控制措施 | 7.1 資通安全防護及控制措施註：若機關無資通系統防護及控制措施規定之文件，但仍訂有相關規定，或配合上級機關規定辦理，請將機關之相關規定內容敘明於補充說明中(範例：本機關之資通系統防護及控制措施規定配合OO市政府OO局之規定辦理、本機關之資通系統防護及控制措施包含：…) |  本機關之資通安全防護及控制措施(含存取控制與加密機制管理、作業及通訊安全管理、系統開發及維護機制、防毒軟體、網路防火牆等)規定於  文件(編號、名稱及章節) 本機關無資通安全防護及控制措施相關規定文件，原因為： 補充說明(選填)：註：若機關無資通系統防護及控制措施規定之文件，但仍訂有相關規定，或配合上級機關規定辦理，請將機關之相關規定內容敘明於補充說明中(範例：本機關之資通系統防護及控制措施規定配合OO市政府OO局之規定辦理、本機關之資通系統防護及控制措施包含：…) |  |
| 8.資通安全事件通報、應變及演練相關機制 | 8.1 訂定資通安全事件通報、應變及演練相關機制？註：不一定要機關自行訂定，可採用上級機關訂定之資安事件通報機制。 | (單選) 本機關資通安全事件通報、應變及演練相關機制規定於 文件中。 本機關遵守上級(其他)機關所訂定之資通安全事件通報、應變及演練相關機制，訂定機關為  機關無相關機制(未符法遵)，原因為： 補充說明(選填)： |  |
| 8.2 資通安全事件通報、應變及演練 | 1.資安事件通報：(單選)本機關110年計通報資安事件 件，符合相關時限規定。本機關110年計通報資安事件 件，有 件事件不符合時限規定，原因為：  無資安事件補充說明(選填)：2.110年社交工程演練：(單選)計 位同仁點閱(點閱率 %)， 位同仁開啟內容連結(開啟連結率 %)未辦理，原因為： 補充說明(選填)：註：若不只進行一次演練，請填寫最近一次演練結果，並將其他次演練結果敘明於補充說明(選填)中。3.110年通報應變演練(單選)符合相關時限規定有不符合時限規定情形： 未辦理，原因為： 補充說明(選填)： |
| 9.資通安全情資之評估及因應機制 | 9.1資通安全情資之評估及因應措施？註：資安情資來源如上級機關、技服中心、ISAC等… | (單選) 本機關資安情資來源有：  ，已進行情資評估及因應措施，情資分類評估機制及因應措施載明於  文件(編號、名稱及章節)本機關資安情資來源有：  ，但無資安情資之評估及因應措施相關文件，原因為：  本機關未知悉任何資安情資來源，且無資安情資之評估及因應措施相關文件，原因為： 補充說明(選填)： |  |
| 10.資通系統或服務委外辦理之管理 | 10.1選任受託者應注意事項 | (單選) 本機關無資通系統或服務委外 本機關資通系統或服務委外，選任受託者應注意事項(如要求ISMS導入、安全性檢測、稽核其執行等、資安事件通報等)已納入並明確標註於採購招標文件中。 本機關有資通系統或服務委外，但未訂定選任受託者應注意事項，原因為： 補充說明(選填)： |  |
| 10.2監督受託者資通安全維護情形應注意事項 | (單選)1.訂定規範或文件：本機關監督受託者資通安全維護情形應注意事項已訂定於 文件(編號、名稱及章節)內。本機關無資通系統或服務委外未訂定監督受託者資通安全維護情形應注意事項，原因為： 補充說明(選填)：註：第1題如點選「本機關無資通系統或服務委外」，第2項問題鎖住不能填寫。2.110年本機關計份契約：全部契約皆已納入前述規定。其中 份契約已納入前述規定，其餘未納入之原因為： 全部契約皆未納入相關規定，原因為： 補充說明(選填)： |
| 10.3是否辦理委外廠商查核？ | (單選)本機關無資通系統或服務委外本機關110年委外資通系統、服務廠商共計 家，110年自行辦理委外廠商查核，計查核 家，受查核廠商為 ，查核方式為 (例如實地查核、書面查核等)；110年聯合其他機關(包含 等機關)辦理委外廠商聯合查核，計查核 家委外廠商，受查核廠商為 ，查核方式為 。註：如查核廠商多於一家，請用頓號區隔，例如：A公司、B公司110年未進行委外廠商查核，原因為： 補充說明(選填)： |  |
| 11.資通安全教育訓練 | 11.1機關人員接受資通安全教育訓練情形 | 詳本機關應辦事項-資通安全教育訓練。補充說明(選填)： |  |
| 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 | 12.1訂定考核機制並進行考核 | (單選)110年本機關資通安全考核獎懲情形：記獎 人、懲 人。110年本機關資通安全考核獎懲情形：無獎懲110年本機關無進行相關考核，原因為： 補充說明(選填)： |  |
| 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 | 13.1資通安全維護計畫實施情形之稽核機制 | (單選) 本機關已訂定資安內部稽核機制。 本機關無資安內部稽核機制，原因為： 補充說明(選填)： |  |
| 13.2資通安全維護計畫之持續精進及績效管理 | 本機關定期每  個月檢視及追蹤內部稽核改善執行情形本機關不定期檢視及追蹤內部稽核改善執行情形，方法為 未追蹤，原因為： 補充說明(選填)： |
| 13.3檢視並審核所屬/所監督/所管機關(構)資通安全維護計畫實施情形[所屬機關查詢](https://spm.nat.gov.tw/ManageMPIS110/MPIS110UnitListExtSubList) | 1.本機關所屬/所監督公務機關，共有 個，其110年資通安全維護計畫實施情形被檢視及審核情形：無所屬/所監督公務機關本機關110年已檢視並審核個所屬/所監督公務機關之實施情形。未檢視及審核，原因為： 2.本機關所管特定非公務機關，共有 個CI提供者、 個公營事業、 個財團法人，其110年資通安全維護計畫實施情形：(1) 要求提報情形無所管特定非公務機關。已要求全部所管特定非公務機關提報。已要求 個CI提供者、 個公營事業、 個財團法人提報實施情形，未全部要求提報之原因為：未要求所管特定非公務機關提報實施情形，原因為： (2) 檢視及審核情形無所管特定非公務機關。本機關110年已檢視並審核 個CI提供者、 個公營事業、 個財團法人之實施情形。未檢視及審核所管特定非公務機關實施情形，原因為： 補充說明(選填)： |
| 13.4對所屬/所監督/所管機關(構)訂定稽核計畫 | (單選)1.本機關對所屬/所監督/所管機關(構)訂定稽核計畫已訂定於文件(編號、名稱及章節)內，執行情形載明於 文件(編號、名稱及章節)，並透過 (後續追蹤管考機制)定期檢核執行情形。註：如無所屬機關/監督/所管機關(即2、3都填無) 其第1項問題鎖住不用填寫2.所屬/所監督公務機關之稽核計畫：無所屬/所監督公務機關本機關稽核規劃納入 個公務機關，每年稽核 個，預於 年內完成全部機關稽核。稽核小組包含 個單位，共 人。每次稽核成員規劃：(人數及組成規則)。尚未訂定對所屬/所監督公務機關之稽核計畫，原因為： 3.所管特定非公務機關之稽核計畫：無所管特定非公務機關本機關稽核規劃納入 個特定非公務機關，每年稽核 個，預於 年內完成全部機關稽核。稽核小組包含個 單位，共 人。每次稽核成員規劃： (人數及組成規則)。尚未訂定對所管特定非公務機關之稽核計畫，原因為： 補充說明(選填)：註：如對所屬/所監督/所管之部分機關非由本機關(構)辦理稽核作業，請補充說明，範例：計OO個公務機關非由本機關辦理稽核，其中OO個採分層稽核、OO個採橫向稽核、OO個採其他方式(OO)稽核；計OO個特定非公務機關非由本機關辦理稽核，其中OO個採分層稽核、OO個採橫向稽核、OO個採其他方式(OO)稽核。 |
| 13.5對所屬/所監督/所管機關(構)辦理資通安全維護計畫實施情形之稽核 | (單選)1.對所屬/所監督公務機關之稽核無所屬/所監督公務機關本機關110年已辦理 個所屬/所監督公務機關之稽核作業，計有 項改善建議，預計於 年 月前完成改善。未稽核所屬/所監督公務機關，原因為： 補充說明(選填)：2.對所管特定非公務機關之稽核(1) CI提供者之稽核無所管CI提供者。本機關110年已辦理 個所管CI提供者之稽核作業，計有 項改善建議，預計於 年 月前完成改善。未稽核所管CI提供者，原因為： (2) 對公營事業之稽核無所管公營事業。本機關110年已辦理 個所管公營事業之稽核作業，計有 項改善建議，預計於 年 月前完成改善。未稽核所管公營事業，原因為： (3) 對財團法人之稽核無所管財團法人。本機關110年已辦理 個所管財團法人之稽核作業，計有 項改善建議，預計於 年 月前完成改善。未稽核所管財團法人，原因為： 補充說明(選填)：註：若不只進行一次對所屬/所監督/所管稽核，請填寫最近一次稽核結果，並將其他次稽核結果敘明於補充說明(選填)中。 |  |