衛生福利部暨所屬機關

資通安全與隱私保護政策

機　密　等　級：公開
文　件　編　號：CC-IS-01-001
版　　次：V 2.0
制（修）訂日期：112 年 11 月 14 日

文件階層	文件編號	頁數	制修訂單位
一階文件	CC-IS-01-001	9	衛生福利部資通安全管理暨個資保護小組

制 修 訂 紀 錄

版次	制（修）訂日期	修訂頁次	修訂者	制（修）訂內容摘要
V 1.0	96/02/08		黃○○	初版
V 1.1	99/06/11		黃○○	因應本中心、SC 及 HCA 資安制度之整合，調整機密等級、文件編號及相關內容
V1.2	99/9/10	1,2,3	黃○○	修訂貳、二之文字內容。
V1.3	102/07/23		黃○○	1. 因應組織改造，變更組織名稱為「衛生福利部」、「資訊中心」變更為「資訊處」。 2. 修訂「電腦處理個人資料保護法」為「個人資料保護法」
V1.4	103/10/9		黃○○	3. 修訂 ISO27001 與國家資通安全發展方案名稱 4. 刪除目標改以表單呈現 5. 修訂資訊安全責任
V1.5	107/5/18		林○○	配合文件名稱修訂，調整相關文件之內文引用文件名稱。
V2.0	112/11/14		王○○	依本部暨所屬機關資通安全政策修訂，並導入隱私保護，新增相關內容。

機密等級：公開

制訂單位	文　件　名　稱	文件編號	版　次
衛生福利部資通安全管理暨個資保護小組	衛生福利部暨所屬機關資通安全與隱私保護政策	CC-IS-01-001	V2.0

目　　錄

機密等級：公開

制訂單位	文　件　名　稱	文件編號	版　次
衛生福利部資通安全管理暨個資保護小組	衛生福利部暨所屬機關資通安全與隱私保護政策	CC-IS-01-001	V2.0

壹、 依據

本政策係依據資通安全與隱私保護相關法令法規及國際標準，考量衛生福利部（以下簡稱本部）暨所屬機關業務需求，訂定資通安全與隱私保護政策及相關規範，以建立資通安全與隱私保護管理機制，強化資通安全與隱私防護，提昇資通安全與隱私保護之水準。

貳、 目的

為推動資通安全與隱私保護管理，建立安全及可信賴之資通環境，確保資通訊系統、資通設備及網路等重要資訊資產之機密性、完整性及可用性，並為致力於個人資料之保護，維持業務持續運作，保障民眾權益，特訂定本政策。

參、 資通安全與隱私保護管理指標

依據資通安全與隱私保護管理量測指標（如附件一）辦理。

肆、 適用範圍

本部暨所屬機關資訊作業環境及所涉個人資料蒐集、處理與利用之所有活動。

伍、 權責

一、 本部暨所屬各機關之所有員工及提供本部服務之機關（構）皆應共同遵守相關資通安全與隱私保護規範。

二、 本部暨所屬各機關之單位主管對於本資通安全與隱私保護政策之施行，應負監督與管理之責。

陸、 資通安全與隱私保護目標

一、 保護本部暨所屬各機關之資訊，防止未經授權之存取，避免惡意破壞，確保資通安全。

二、 維持本部暨所屬各機關資訊業務持續運作，以持續提供全民衛生醫療及社會福利相關服務。

三、 建立本部暨所屬各機關資通安全與隱私保護管理系統，避免人為作業疏失，加強同仁資通安全與隱私保護意識，以提昇本部暨所屬各機關衛生醫療及社會福利業務之資訊服務品質與安全。

四、 確保本部暨所屬各機關因公務使用之個人資料，依個人資料保護法

規定保障隱私，並依法使用，確保個人資料安全，並落實本部資通安全與隱私保護政策。

柒、 資通安全與隱私保護責任

一、 本部暨所屬各機關之所有員工應遵循資通安全與隱私保護相關法令法規，確定各項作業之資通安全與隱私保護需求，並採行適當及充足之資通安全與隱私保護措施，確保資訊蒐集、處理、傳送、儲存及流通，與個人資料蒐集、處理及利用之安全。

二、 本部暨所屬各機關之高階主管應積極參與資通安全與隱私保護管理活動，提供對資通安全與隱私保護之支持及承諾。

三、 本部暨所屬各機關應定期提供全體同仁資通安全與隱私保護訓練課程，提昇人員資通安全與隱私保護認知。

四、 本部暨所屬各機關皆須遵守資通安全事件通報及應變辦法及機關通報機制，通報所發現之資通安全事件或個資外洩事件。

五、 個人資料之蒐集、處理及利用必須符合目的限制原則及資料最少蒐集原則，並採取適切之保護措施。

六、 尊重當事人權利，於當事人提出個資之查閱、複製、更正、刪除等之申請時，於合理、合法的時間內，完成對應處理。

七、 本部暨所屬各機關、提供服務之機關（構）及其人員，應遵守本政策，若發生任何違反本政策之行為，將依相關規定處理。

捌、 審查

本政策應至少每年評估一次，以反映政府法令、技術及本部暨所屬各機關之業務等最新發展現況，並予以適當修訂。

玖、 實施方式

(一) 本政策經本部資通安全長（或經部長授權之人員）核准，始得公布並通知本部暨所屬各機關，修正亦同。

(二) 本部暨所屬各機關可自訂較本政策更為嚴密之管制措施，惟不得違反本政策要求。

附件一、資通安全與隱私保護管理量測指標（本部暨所屬各機關分別統計）

領域	量測指標項目	量測方式	目標值	量測來源	量測頻率	量測執行單位
資通安全事件	資通安全事件通報應變作業時效達成率	達成率=〔（符合通報時限且符合損害控制或復原作業時限之資通安全事件數）/（全部資通安全事件數）〕×100%	100%	國家資通安全通報應變網站	年	資訊單位
		說明： 資通安全事件含個資外洩事件。 資通安全事件依據資通安全事件通報及應變辦法： 1.公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。 2.公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜： （1）第一級或第二級資通安全事件，於知悉該事件後七十二小時內。 （2）第三級或第四級資通安全事件，於知悉該事件後三十六小時內。				
應用系統	重要資通系統帳號權限清查次數	重要資通系統帳號權限清查次數之計算方式：X 註：X 為帳號權限清查次數	≥2	帳號權限清查紀錄表	年	應用系統承辦單位
		說明： 1.各系統應獨立計算。重要系統係指資通系統防護需求等級為中或高者。 2.帳號種類包含公用資料夾、應用系統、資料庫與伺服器。				
	核心資通系	核心資通系統之最高權限帳密應定期封存之計算方式：X 註：X 為最高權限帳密封存次數	≥1	最高權限	年	應用系統承辦

領域	量測指標項目	量測方式	目標值	量測來源	量測頻率	量測執行單位
	統之最高權限帳密應定期封存	說明： 1.各系統應獨立計算。 2.帳號種類包含應用系統、資料庫與伺服器。		帳號帳密清單		單位
	核心資通系統正式上線後因系統錯誤而導致需申請資料或程式變更次數	核心資通系統正式上線後因系統錯誤而導致需申請資料或程式變更次數統計：X 註：X 為應用系統正式上線後因系統錯誤而導致需申請資料或程式變更次數	≤6	系統工作報告/維護單	年	應用系統承辦單位
		說明： 1.各系統應獨立計算。 2.因人為操作錯誤或因系統尚未完成修復而重複發生之事件，不列入次數統計。				
	核心資通系統之可用率	核心資通系統之可用率計算方式如下： $\frac{(24小時\times365天-X)}{(24小時\times365天)}\times100\%$ 註：X 為應用系統中斷服務時數	≥99%	系統工作報告/維護單	年	應用系統承辦單位
		說明： 1.各系統應獨立計算。重要應用系統係指資訊系統安全等級為高者。 2.中斷服務時數的計算，應於從斷線事件發生時即開始記錄。規劃中之系統停機、維護或過版而導致之中斷不列入中斷服務時數計算。				

領域	量測指標項目	量測方式	目標值	量測來源	量測頻率	量測執行單位
弱點管理	弱點掃描未修補比率	弱點掃描未修補比率計算方式為： $\frac{(X-Y)}{Z}\times 100\%$ 註：X 為未修補高/中風險弱點數量；Y 為可接受之高/中風險弱點數量；Z 為本次弱點掃描全部高/中風險弱點總數；高風險弱點、中風險弱點應各自計算。	高風險 0% 中風險 <=20 %	弱點處理報告單	年	應用系統承辦單位 、 資訊單位
		說明： 1.應用系統承辦單位針對因故無法進行修補之高風險弱點，須提出相對應之補償性控制措施，並於弱點掃描追蹤紀錄中予以適當之說明，以降低其風險至可接受範圍。 2.每次弱點掃描之結果，經修補後，其所剩餘高風險弱點數量，扣除可接受之高風險弱點數量，不得超過該次掃描作業全部弱點數量之 0%。 3.每次弱點掃描之結果，經修補後，其所剩餘中風險弱點數量，扣除可接受之中風險弱點數量，不得超過該次掃描作業中風險弱點數量之 20%。				
網路與機電服務	基礎網路服務可用率	基礎網路服務可用率計算方式為： $\frac{(24小時\times 365天-X)}{(24小時\times 365天)}\times 100\%$ 註：X 為網路服務中斷時數	≥99%	電腦機房操作日誌	年	資訊單位
		說明： 1.網路服務中斷時數應從斷線事件發生時即開始記錄，請執行人員從嚴計算。規劃中之維護而導致之中斷不在計算範圍中。 2.全年可容許網路服務中斷的時間為 87.6 小時，每季可容許服務中斷的時間為 21.9 小時。				

領域	量測指標項目	量測方式	目標值	量測來源	量測頻率	量測執行單位
	機電服務可用率	機電提供之服務可用率計算方式為: $\frac{(24小時\times365天-X)}{(24小時\times365天)}\times100\%$ 註：X 為因供應商因素造成之機電服務中斷時數	≥99.5%	電腦機房操作日誌	年	資訊單位
		說明： 1.非供應商因素所造成之機電服務（如發電機或不斷電系統等機電設備）中斷時間不列入計算。 2.因供應商因素所造成之機電服務中斷時間全年不得超過 43.8 小時。				
資通安全認知與訓練	資通安全教育訓練合規率	合規率=〔（達資通安全管理法要求訓練時數之使用者人數）/（全機關電腦帳號使用者人數）〕×100%	100%	公務人員終身學習時數	每年	資訊單位
		說明： 1.資通安全教育訓練含個資保護教育訓練。 2.全機關電腦帳號使用者包含委外人力及替代役人員等。 3.資通安全責任等級分級辦法規定： （1）資通安全專職人員每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。 （2）資通安全專職人員以外之資訊人員每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。 （3）一般使用者及主管每年接受三小時以上之資通安全通識教育訓練。 4.各機關人事單位需提供本項量測指標所需正式職員及終身學習時數紀錄。 5.委外人力、替代役人員等由該等人員管理單位提供自行參訓之各項佐證紀錄。 當年度在職累計未達一個月的人員不列入計算，以電腦系統帳號有效期間為準。				

領域	量測指標項目	量測方式	目標值	量測來源	量測頻率	量測執行單位
	電子郵件社交工程演練成果比率	電子郵件社交工程演練成果，依開信率與點擊率計算方式為： (1)開信率 $\frac{X}{Y}\times 100\%$ 註：X 為開啟社交工程電子郵件之人數；Y 為機關參與演練人數 (2)點擊率 $\frac{X}{Y}\times 100\%$ 註：X 為點閱社交工程電子郵件所附連結或檔案之人數；Y 為機關參與演練人數	開信率≤10%、點擊率≤6%	電子郵件社交工程演練紀錄	半年	資訊單位
		說明： 每次演練應獨立計算。				
法令遵循	「個人資料檔案」盤點	盤點機關保有及管理之個人資料項目之作業次數	>=1	個人資料檔案盤點紀錄	每年	資訊單位(或個資保護專責單位)
		說明： 依據個人資料保護法第 17 條: 公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同： 一、個人資料檔案名稱。 二、保有機關名稱及聯絡方式。 三、個人資料檔案保有之依據及特定目的。 四、個人資料之類別。 各單位應每年盤點、確認所涉個人資料蒐集、處理及利用之檔案項目是否變更以更新公告清單，並經彙整公開於機關網站。				

制訂單位	文 件 名 稱	文件編號	版 次
衛生福利部資通安全管理暨個資保護小組	衛生福利部暨所屬機關資通安全與隱私保護政策	CC-IS-01-001	V2.0

領域	量測指標項目	量測方式	目標值	量測來源	量測頻率	量測執行單位
	「資訊資產」盤點	盤點機關之作業次數	>=1	資訊資產盤點紀錄	每年	資訊單位
		說明： 依據資通安全管理法施行細則第 6 條: 一、本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項: (六)資通系統及資訊之盤點，並標示核心資通系統及相關資產。 二、資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關經其上級或監督機關同意，得由其上級、監督機關或其上級、監督機關所屬公務機關辦理。 三、各單位應每年進行一次資訊資產盤點作業。				