衛生福利部中區兒童之家

資訊安全政策

文件等級：一般 內部 限閱

編 號：CRCH-ISMS-1-01

版 本：V1.2

文件制/修訂紀錄表

文件版本	發行日期	修訂內容	修訂單位	修訂人	文件管制員
V1.0	110/08/17	依資通安全管理法、資通安全維護計畫及 ISO 27001 條文要求新增本政策	資安防護組	廖志昇	廖志昇
V1.1	112/03/16	1. 因應法規廢止及更新，修正 2. 依據內容 2. 部分文字修潤(4、6.9)及勘誤(6.11)	策略規劃組	趙慧真	廖志昇
V1.2	113/06/07	因應 ISO 27001:2022 條文 1. 修訂 2.4~2.6 文字敘述 2. 增訂 8.3、8.4，原 8.3 同步更動為 8.5	策略規劃組	趙慧真	廖志昇

目錄

1. 目的	4
2. 依據	4
3. 名詞解釋	4
4. 範圍	5
5. 組織	5
6. 資通安全政策	5
7. 實施內容	6
8. 資通安全政策之宣導與檢討	6

1. 目的

衛生福利部中區兒童之家（以下簡稱本家）資訊相關系統軟硬體設備除提供內部人員作業處理外，亦透過網際網路與民眾互動之溝通管道，其相關資訊系統作業應用之持續性運作，攸關本家業務推動之順遂，故訂定本資訊安全政策，作為資訊安全工作之指導方針，藉以降低資訊風險。

2. 依據

- 2.1. 資通安全管理法
- 2.2. 資通安全維護計畫
- 2.3. 國家資通安全發展方案
- 2.4. ISO/IEC 27001(Information security, cybersecurity and privacy protection–Information security management systems – Requirements)
- 2.5. CNS 27001(資訊安全、網宇安全及隱私保護—資訊安全管理系統—要求事項)
- 2.6. ISO/IEC 27002(Information security, cybersecurity and privacy protection–Information security controls)

3. 名詞解釋

- 3.1. 機密性(Confidentiality)：確保只有經過授權的人才能存取資訊資產。
- 3.2. 完整性(Integrity)：確保資訊資產的完整性(Completeness)及其處理方法的準確性。
- 3.3. 可用性(Availability)：確保授權的使用者在需要時，可以使用資訊資產。
- 3.4. 適法性(Legality)：符合國家相關法令規範。
- 3.5. 資訊機房：本家二樓資訊機房。

4. 範圍

本家資訊安全管理制度適用於本家暨所屬單位所有業務，包含全體員工、與本家業務往來之外部機關、對本家提供服務或勞務之廠商及訪客。

5. 組織

為統籌資訊安全管理等事項之規劃、執行、稽核及矯正活動，應建立資訊安全推動組織，並依資訊安全管理組織程序書辦理。

6. 資通安全政策

為使本家業務順利運作，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，並確保其機密性 (Confidentiality)、完整性 (Integrity) 及可用性 (Availability)，特制訂本政策如下，以供全體同仁共同遵循。

- 6.1. 應建立資通安全風險管理機制，定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
- 6.2. 建立電腦機房實體及環境安全防護措施，並定期實施相關保養。
- 6.3. 應保護本家所提供軟硬體系統機敏資訊及資通系統之機密性與完整性，避免未經授權存取與竄改。
- 6.4. 建置新資訊系統前，應將資訊安全納入考量因素，防範發生危害系統安全之情況。
- 6.5. 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本家同仁之資通安全意識，本家同仁亦應確實參與訓練。
- 6.6. 確保本家資通系統安全，防範資安攻擊事件發生。
- 6.7. 應強固核心資通系統之韌性，確保本家業務持續營運，以達成永續發展目標。
- 6.8. 訂定資訊安全內部稽核計畫，定期執行內部稽核活動。
- 6.9. 人員違反資訊安全相關規定，應依本家相關規定及其他法規處理。若第三方人員違反資訊安全相關規定，則依資通安全事項之獎懲機制及雙方

簽訂之合約處理。

- 6.10. 對於個人資料之蒐集、處理及利用，將依相關法令之規定，僅就其特定目的之用，不會恣意對其他第三者揭露。
- 6.11. 各項資通安全管理規定必須遵守政府相關法規(如：資通安全管理法、刑法、國家機密保護法、著作權法、個人資料保護法及政府資訊公開法等)之規定。

7. 實施內容

相關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效(量測指標)，實施程序參見資訊安全實施程序書。

8. 資通安全政策之宣導與檢討

- 8.1. 本家之資通安全政策、需求及目標，應每年透過教育訓練、會議、張貼公告、利用媒體、函文、網頁、電子郵件及文宣等方式，向本家內所有人員進行宣導，並檢視執行成效。
- 8.2. 本家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)進行資通安全政策宣導、關注議題討論、溝通並檢視執行成效。
- 8.3. 本家各單位進行資訊安全管理作業，如下列項目需進行變更，應依規劃執行之。
 - 8.3.1. 資訊安全管理系統變更。
 - 8.3.2. 發生重大資安事故。
 - 8.3.3. 有新增、變更或移除資訊資產。
 - 8.3.4. 作業環境變更。
- 8.4. 如需進行變更，應考量下列事項
 - 8.4.1. 變更的目的與其潛在之影響。
 - 8.4.2. 管理系統的完整性。
 - 8.4.3. 資源的可用性。
 - 8.4.4. 職責與權限之分配或重新分配。

- 8.5. 本資通安全政策由資通安全長核定，每年於資通安全管理審查會議中檢討其適切性，應至少評估一次，以反映政府機關各項安全政策、法令、技術及業務之最新狀況，確保安全實務作業之可行性及有效性。