**和康顧問有限公司**

**「資訊安全管理制度」**

**資訊安全政策**

機密等級：一般

文件編號：ISMS-1-001

版本編號：1.0

發行日期：

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版號** | **發行日** | **修訂者** | **說明** | **核准者** |
| 1.0 |  |  | 初版文件發行 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目錄**

[**1.** 目的 3](#_Toc109306371)

[**2.** 適用範圍 3](#_Toc109306372)

[**3.** 權責 3](#_Toc109306373)

[**4.** 名詞定義 3](#_Toc109306374)

[**5.** 流程圖 4](#_Toc109306375)

[**6.** 作業說明 4](#_Toc109306376)

[**7.** 相關文件 4](#_Toc109306377)

1. 目的

和康顧問有限公司（以下簡稱本公司）為強化資訊安全管理，確保所屬資訊資產之機密性、完整性與可用性，以及提高相關人員資訊安全意識，並符合相關法規要求，俾利本公司資訊服務持續運作之環境，特訂定本政策。

1. 適用範圍
   1. 本公司所有單位。
   2. 資訊安全管理涵蓋14項管理事項：
      1. 資訊安全政策訂定與評估。
      2. 資訊安全組織。
      3. 人力資源安全管理。
      4. 資訊資產管理。
      5. 存取控制安全管理。
      6. 資訊加密管理。
      7. 實體與環境安全管理。
      8. 系統作業管理。
      9. 通訊安全管理。
      10. 資訊系統獲取、開發與維護之安全管理。
      11. 支援關係管理。
      12. 資訊安全事件之通報與應變管理。
      13. 營運持續運作管理。
      14. 相關法規與施行單位政策之符合性。
2. 權責
   1. 資訊安全管理委員會召集人

建立及審核此政策。

* 1. 資訊安全管理委員會

透過適當的標準和程序實施此政策。

1. 名詞定義
   1. 資訊資產：

係指為維持本公司資訊業務正常運作之硬體、軟體、通訊、資料、服務、文件及人員。

* 1. 營運持續運作之環境：

係指為維持本公司各項資訊業務正常運作所需之作業環境。

1. 流程圖

無。

1. 作業說明
   1. 資訊安全政策
      1. 為使本公司業務順利運作，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，以供全體同仁共同遵循。
      2. 應因應資通安全威脅情勢變化，本公司同仁應參與資通安全教育訓練，以提高資通安全意識。
      3. 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。
   2. 責任
      1. 本公司員工及與本公司往來之外部單位、廠商及第三方人員等，皆需遵守本公司資訊安全相關制度及規範，如有違反者，必須自行承擔所有引發的風險及責任。
      2. 所有人員於知悉任何危及資訊安全之事件或風險時，皆需依程序進行通報流程。
      3. 因故意或過失之行為，危害本公司資訊安全者，將視情節輕重追究其民事、刑事及行政責任。
   3. 審查
      1. 定期：

本政策應每年審查1次，以反映法規、技術及業務等最新發展現況。

* + 1. 不定期：

當本公司面臨下列狀況時，應針對資訊安全政策進行檢討與審查。

* + - 1. 本公司營運策略發生重大變更。
      2. 資訊安全管理委員會召集人異動。
      3. 發生重大資訊安全事件。
  1. 實施

本政策發行、修訂與廢止需經資訊安全管理委員會召集人進行審核後，以適當方式公告並實施。

1. 相關文件

無。