**水利署**

**ISMS資訊安全政策**

 **V1.1**

|  |  |
| --- | --- |
| 文件編號 | ISMS-1-A050-0-00 |
| 分類等級 | 組室使用 |
| 初版日期 | 02/11/2015 |
| 修訂日期 | 12/09/2015 |

|  |  |  |  |
| --- | --- | --- | --- |
| 核准 | 會辦 | 審查 | 制訂 |
| 9542 |  | 何丁武職章 | 9624 |

**本文件為水利署所有，禁止翻印**

**文件編修紀錄**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 發行／修訂版本 | 發行／修訂生效日期 | 發行/修訂內容說明 | 制訂 | 審查 | 核准 | 備註 |
| V1.0 | 02/11/2015 | 因應ISO 27001:2013新版標準進行調整 | 黃貴麟 | 審核評估分組 | 資訊安全管理審查會議 |  |
| V1.1 | 12/09/2015 | 修訂資訊安全目標 | 黃貴麟 | 審核評估分組 | 資訊安全管理審查會議 |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**目錄**

[0. 目的 4](#_Toc237257909)

[1. 依據 4](#_Toc237257910)

[2. 範圍 4](#_Toc237257911)

[3. 資訊安全定義 4](#_Toc237257912)

[4. 資訊安全政策 4](#_Toc237257916)

[5. 資訊安全目標 5](#_Toc237257918)

[6. 管理階層責任 5](#_Toc237257939)

[7. 法令規章遵循性 6](#_Toc237257967)

[8. 資訊安全管理系統建置要求 6](#_Toc237257975)

[9. 不可接受風險處理 7](#_Toc237257980)

[10. 適用性聲明書 7](#_Toc237257981)

[11. 修訂與實施 7](#_Toc237257982)

# 目的

水利署(以下稱本署)為強化資訊安全管理暨落實個人資料之保護，建立安全及可信賴之資訊環境，確保資訊資產免於遭受內部或外部、蓄意或意外之威脅與破壞，特訂定本政策。

# 依據

本政策係依據「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」、並參酌行政院頒「建立我國通資訊基礎建設安全機制計畫」、經濟部「資訊安全政策」、法務部「個人資料保護法」等有關法規，以及ISO27001資訊安全管理系統標準，同時考量本署業務需求而訂定，以建立資訊安全管理機制、強化資訊安全防護、加強個人資料安全防護，提昇資訊安全之水準。

# 範圍

本署資訊安全管理系統之實施範圍，涵蓋資訊安全管理制度（ISMS）驗證範圍內之所有員工(含約聘人員、臨時人員)、委外駐點處理資訊業務之人員、委外廠商、第三方資訊使用人員，並包括所轄管之網路及機房維運，各項資訊系統之開發、維護、操作，及其所有相關資訊資產之安全管理。

# 資訊安全及個人資料安全定義

## 資訊安全係指保護資訊之

* + 1. 機密性：確保只有獲得授權的使用者，才得以存取資訊。
		2. 完整性：保障資訊與處理方法的正確與完整。
		3. 可用性：確保獲得授權的使用者於有需要時，能適時存取資訊及相關資產。

## 個人資料安全係指保護

 自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、緍姻、家庭、教育、職業、病歷、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方式識別該個人之資料。

# 資訊安全政策

本署一貫秉持以精益求精、不斷革新之精神，為提供優質服務而努力，以期建立安全及可信賴之電子化政府。因此，特強化資訊安全管理，確保資料、系統、設備、網路及個人資料安全，部署創新的資訊安全防護技術，以落實推動資訊安全管理作業，並達到保護資訊資產之機密性、完整性及可用性等目標。

# 資訊安全目標(每年至少進行1次有效性量測)

|  |  |  |
| --- | --- | --- |
|  | 資訊安全目標 | 投入資源 |
| 1 | 保障資訊之機密性及防止非法存取 | 1.門禁系統及相關監控設備2.各應用系統營運管理3.SOC及NOC監控維運中心、防毒機制4. ISMS體系運行 |
| 2 | 確保所有資料安全 |
| 3 | 確保資產之可用性、完整性，以確保業務運作之有效性及持續可用 | 1.各應用系統營運管理2.系統效能及服務監測機制3.基礎環境設備資源4. ISMS體系運行 |
| 4 | 確保資安措施符合政策及法令要求 | ISMS體系運行 |

##

# 管理階層責任

## 管理階層應完成下列工作，以充分表示對資訊安全管理發展及增進的支持：

## 核定資訊安全政策，確立資訊安全目標及計畫。

## 授權資通安全處理小組或相關職掌單位，執行資訊安全作業。

## 覆核資訊安全管理體系稽核與執行成果。

## 核定可接受風險水準。

## 提供資訊安全管理體系運作必要資源。

# 審查

## 本政策應每年至少審查1次，以反映政府法令、技術及業務等最新發展現況，並確保本署業務永續運作之能力。

## 本署應考量內、外部議題及利害相關者要求，定訂適當之資訊安全管理制度實施範圍，經由管理階層審核、確認後實行。

## 資訊安全管理制度實施範圍應定期或不定期視內、外部環境之變更或執行狀況，如：法令法規之要求、組織異動、資安事件發生、管理制度落實狀況等因素，經由組室權責主管或資訊管理審查會議核定後實行。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **內部議題** | **外部議題** | **利害相關者** | **利害相關者要求** | **備註** |
| 組織政策、目標 | 主管機關要求 | 主管機關 | 各項法令、法規 |  |
| 政府單位要求 | 政府單位 | 各項法令、法規 |  |
| 組織文化 | N/A | 內部人員 | 組織內部規範 |  |
| 相關資源需求（包括：人力、技術、預算等） | N/A | 內部人員 | 訓練 |  |
| 高階主管 | 績效（KPI） |  |
| 資訊安全事件資訊技術 | 客戶 | 合約內容（SLA） |  |
| 供應商 | 合約內容 |  |
| ISO國際標準 | ISO國際組織 | ISO 27001 |  |
| 第三方稽核單位 |  |

# 法令規章遵循性

## 資訊安全，人人有責。

## 本政策應遵循法律、法規及合約的要求。

## 實施資訊安全及個人資料保護教育訓練，以加強員工認知安全意識，相關教育訓練由本署資訊室或協同其他單位共同辦理。

## 執行各項資訊作業時，應依「ISMS-0-0929-07-220\_行政院及所屬各機關資訊安全管理要點」、「ISMS-0-0929-07-230\_行政院所屬各機關資訊安全管理規範」、「ISMS-0-0425-11-010\_個人資料保護法」及相關法令規定辦理，並遵守本署其他各項規範及與第三方簽訂之契約。

## 本署資訊安全管理制度（ISMS）驗證範圍內之資訊及網路系統因遭受破壞、不當使用所造成危安或重大災害事件，應依「持續營運計畫書」辦理，資通安全處理小組應在最短期間內訂定應採行應變措施，並將處理情形記錄備查。

## 本署人員違反資訊安全規定者，依「經濟部暨所屬經建人員獎懲標準表」辦理。有「公務員懲戒法」第2條所定情事，應付懲戒者，依該法第19條規定辦理；有觸犯「刑法」之嫌疑者，應予移送司法機關調查；有涉及國家賠償事件者，應依「國家賠償法」等相關法律追究損害賠償責任。非本署人員違反資訊安全規定時，亦應依相關法律規定追究民刑事責任。

# 資訊安全管理系統建置要求

## 應在整體資訊營運活動與其所面臨風險的狀況下，建立、實施、操作、監督、審查、維持及持續改進資訊安全管理系統。

## 應採取矯正措施，以消除與資訊安全管理系統要求不符合之原因，防止其發生。

## 為防止再發，應採取長期性策略措施，以消除與資訊安全管理系統要求潛在不符合之原因。

## 應藉由資訊安全政策、資訊安全目標、稽核結果、監督事件之分析、矯正措施以及管理階層審查，以持續改進資訊安全管理系統之有效性。

# 不可接受風險處理

執行風險評鑑後，對於風險值高於「可接受風險水準」之資產，應訂定「風險處理計畫」據以監督控管，並落實追蹤執行。

# 適用性聲明書

本署資訊安全管理制度（ISMS）依據ISO27001標準要求產出適用性聲明書，以書面方式列舉資訊資產是否適用其標準所列之控制措施，對不適用者應說明其不適用之原因。

# 修訂與實施

本政策應至少每年1次或因組織、業務、法令或環境等因素之改變，予以適當修訂，並須經組室權責主管或資訊安全管理審查會議簽核後實施，並透過公告程序，使本署資訊安全管理制度（ISMS）驗證範圍內之同仁及相關人員瞭解資訊安全政策之相關規定。