商工行政服務e網通系統
資訊安全政策

ISMS-A01

版本：3.01

機密等級：■一般 □敏感 □密

經濟部商業司

生效日期：中華民國 104 年 05 月 13 日

【文件修訂記錄】

制／修定版本	生效日期	制／修定摘要說明	備註
V1.01	96/08/01	新擬訂文件	
V1.02	96/10/01	修正「三、資訊安全政策」	
V2.00	99/08/06	依據內稽建議更新並統一文件版本。 依據商業司資訊安全政策增修適用範圍。	
V2.01	101/11/05	依據(101 年)ISO 27001 追查評鑑稽核建議本政策（四）：修改對應之目標以符合國家法令達成業務持續運作之目標。	
V2.02	102/07/09	依據內稽建議更新法令法規相關資訊安全要求	
V3.00	**104/02/04**	**依據「ISO 27001:2013」年版條文要求修訂資訊安全政策之內容。**	
V3.01	**104/05/13**	**增訂「資訊服務管理」相關內容。**	

一、 依據

依據「ISO/IEC 27001:2013 資訊安全管理系統」、「經濟部資訊安全政策」、「經濟部商業司資訊安全政策」相關要求，為建構一套完整的資訊安全管理制度，同時落實資訊服務運行之品質，藉由此制度之實踐達成資訊安全目的，特訂定此政策。

二、 適用範圍

本政策適用於「商工行政服務 e 網通系統」（以下簡稱「本系統」），其作業範圍包括委外服務之機房及下列相關設備與人員：

（一） 國光機房及富國(備份)機房實體環境安全與門禁管制。

（二） 國光機房及富國(備份)機房內本系統所屬連外骨幹網路及硬體維護。

（三） 本系統軟體及所屬資料備份。

（四） 本系統管理、開發、維護及督導。

資訊安全管理涵蓋 14 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本機關帶來各種可能之風險及危害。管理事項如下：

（一） 資訊安全管政策之制定及評估

（二） 資訊安全組織之職責與分工

（三） 人力資源安全

（四） 資訊資產管理

（五） 存取控制

（六） 密碼措施

（七） 實體與環境安全

（八） 作業安全

（九） 通訊安全

（十） 資訊系統獲取、開發及維護

（十一） 供應商關係

（十二） 資訊安全事故管理

（十三） 營運持續管理之資訊安全層面

（十四） 遵循性。

三、 資訊安全政策

因應本機關資訊安全與資訊服務需求，制定本制度資訊安全與資訊服務政策要求如下：

（一） 確保本系統業務相關資訊之機密性，保障國家機密與民眾隱私。

（二） 確保本系統業務相關資訊之完整性及可用性，提高行政效能與品質。

（三） 配合國家資訊安全政策之推動，提昇資訊安全防護能力。

（四） 符合國家法令及合約達成業務持續運作之目標。

（五） 建立資訊服務管理相關作法，以提升商工行政服務 e 網通系統之資訊服務品質。

（六） 強化資訊治理能力，以快速因應各項政策推動及本司業務擴展。

四、 資訊安全與資訊服務目標

因應本制度資訊安全與資訊服務之需要，所有安全與管理作業應以達到下列目標為原則。

(一) 本系統應具備保障國家機密與民眾隱私之機密性要求：提報「經濟部資通安全處理小組」資訊安全事件每年應小於（含）4 次。

(二) 本系統應具備提高行政效能與品質確保完整性及可用性之要求：經風險評鑑結果之重要系統，其個別系統可用度應維持 99.4%以上，亦即平均每月非計畫性系統中斷服務時間應低於 5 小時。

(三) 本系統應具備提昇資訊安全防護能力之要求，應設置適當的防駭保護：資安漏洞修補率至少為 99%(含)以上、風險評鑑殘值應低於 3(含)等級、員工資安訓練至少 3(含)小時以上。

(四) 本系統應具備達成業務持續運作之目標，演練及切換應每年至少進行 1 次業務持續計畫之測試及檢核。

(五) 提供優質資訊服務，確保本系統資訊服務水準協議指標達成率達 99.4%以上。

(六) 提高本司業務單位對資訊服務之滿意度，每年至少進行 1 次「商工行政服務 e 網通系統」資訊服務滿意度調查。

五、 資訊安全要求

為確保本系統相關資訊之機密性、完整性及可用性，並對應本政策資訊安全目標之要求，建置符合下列相關安全要求之制度，並擬定相關規範。

(一) 組織全景之鑑別

1. 應決定與營運目的相關，且會影響資訊安全管理制度(ISMS)預期成果之內部與外部議題，鑑別出與本系統所提供服務相關之利害關係者，以及這些利害關係者對本系統的需求與期望，並讓高階主管知悉並取得共識，用以客觀決定資訊安全管理制度(ISMS)之範圍。

2. 應制定組織全景鑑別管理作業程序，用以系統化地鑑別本系統之核心業務、與核心業務相關之利害關係者以及這些利害關係者對本系統核心業務之需求與期望，並判別若無法達到些需求與期望會對本機關造成何種程度之衝擊，並將上述評估及分析結果供高階主管用以決策 ISMS 之導入及驗證範圍。

(二) 資訊安全與資訊服務責任及組織

1. 依「資訊安全推行小組」要求，應設置「商工行政服務 e 網通系統資訊安全作業小組」（以下簡稱本小組），由副司長（資訊）擔任召集人，應定期向「資訊安全推行小組」報告。本小組應設置相關功能之負責人員，以推動並監督資訊安全管理與資訊服務相關事項之計畫、執行與管理工作。本小組應包含與本系統安全與資訊服務有關之業務單位人員，以提升安全應變與資訊服務能力。

2. 應決定及建立與資訊安全管理制度(ISMS)相關的內部與外部溝通之需求及準則，內容須包含：要溝通什麼、何時溝通、和誰溝通、應是誰溝通以及應實現哪種溝通過程，確保 ISMS 各項資訊安全業務與資訊服務在內部適度的溝通與傳達，以利 ISMS 之推動與管理。

(三) 資訊資產分類分級

本系統相關之資訊資產須指派其保管者，並維護完整之資訊資產清冊。所使用資訊資產須適當分類，並鑑別安全等級（即資產價值），分類

須考量該資產之共用性、限制性、風險同質性及與業務有關之衝擊性。另有關個人資料盤點及管制作法，依「經濟部及所屬機關個人資料保護管理要點」及相關規範辦理。

(四) 存取管控

須針對本系統所提供之網路管理、系統管理、監控服務及機房實體區域環境設定存取權限。存取權限之設計須依據使用者職務所需接觸最少資訊為原則，使用者若有職位變動須立即變更其存取權限。為確保存取權限之適當性與正確性，存取權限須經授權程序並應有定期覆核機制。

(五) 風險評鑑及風險管理

須對於本系統整體之作業及相關資訊資產，進行資訊安全風險評鑑及風險管理。風險評鑑過程須包括：建立資訊資產清冊、威脅評估與弱點評估、既有控制方法確認、風險程度評估、可行性控制方法建議等步驟。風險管理須包括設定安全保障水準（可接受的風險等級）、評估控制方法的成本效益、考量相關的法律因素等。本系統相關組織或營運環境變遷致作業程序有重大變更時，應比照上述原則重新進行風險評鑑及風險管理。風險評鑑結果及處理計畫須經本小組之審查。

(六) 實體安全

本系統須採取適當的實體安全保護，以防止對此系統之資訊資產不當處理或造成損害，重要的資訊設備應設置於有適切門禁管制之場所。應制定門禁管制之授權程序，並經授權方可進入本系統所在之機房，其進入及離開須於進出紀錄簿簽名。機房設施應有適當之監控及警示系統，包括門禁、備援電力、消防及空調系統，以確保機房作業環境之安全。

(七) 網路安全

本系統須採取適當的網路防護措施，以防止電腦或網路系統遭受不當存取、異動或損害，重要之系統與網路設備應有適切之防護措施。應指派專責管理人員負責網路安全管控。

(八) 病毒及惡意軟體之防護

本系統須建置防範電腦病毒及惡意軟體之機制，並應定期執行弱點掃描及滲透測試，系統管理人員並須依照規定更新電腦病毒碼與系統漏洞修補。除了經合法授權之系統及應用軟體外，禁止使用其它軟體。

(九) 資安認知與訓練

本系統有關之作業人員須接受與職務相關之資訊安全與資訊服務教育訓練，以確保足夠之資訊安全認知與資訊服務能力。教育訓練應配合適當的評估方法，以確認其應有之效果。

(十) 資訊安全事件通報及處理

資訊安全事件係指可能會對本系統資訊資產之機密性、完整性、可用性造成損害的事件。本系統作業人員在發現時須立即通報，並依照程序研判發生原因、損害程度及可能影響範圍，並採取適當之控制對策，所有採取之行動及所作之研判必須加以記錄。

(十一) 系統開發與維護

本系統應維持一個穩定的作業環境，測試環境與測試資料應予區隔，相關重要資訊需考慮備援及備份處理，並嚴格管理上線及變更作業，應維護必要的操作手冊並更新，應控制系統可能被利用之弱點以及機密資料加密的處理；同時應考量使用者提出之服務諮詢、作業請求或針對服務之抱怨或意見回饋，並應設置服務台以專責處理。

(十二) 業務持續營運管理

須制定一套業務持續營運計畫，以確保本系統不受中斷之影響，業務持續營運計畫須能確保本系統之服務符合需求，本小組須對所訂之計畫進行測試及評估，以確保熟悉在該計畫中所負責之工作內容及執行步驟。業務持續營運計畫須隨時更新及配合年度演練。

(十三) 內部稽核

本制度含括資訊安全管理與資訊服務相關作法，有關對實際運作所進行之稽核，應定期每年進行 2 次，對稽核作業應由本小組之資訊安全稽核組成員負責，並對資訊安全管理與資訊服務之完整性及有效性執行稽核。

(十四) 管理審查

本小組須對本系統之資訊安全管理與資訊服務之完整性及有效性執行審查，以確保資訊安全管理制度足以達成資訊安全目標，並確認資訊服務符合需求單位之期待。審查應定期每年進行 2 次，有重大安全事件時，應不定期召開。審查結果應呈報本機關「資訊安全推行小組」會議。

(十五) 業務委外服務

1. 本系統之建置及維運委外服務作業，應與廠商簽訂委外合約，並簽署書面的資訊安全聲明及服務等級協議(Service Level Agreement, SLA)，以確保廠商人員了解並遵循資訊安全與資訊服務相關政策及目標，恪守資訊安全管理制度(ISMS)各項作業流程、管理規範及相關法令法規之要求。資訊安全聲明中應包含保密協定、服務水準、應交付之文件及相關罰則。故意或過失違反者，將視其違反情節及所造成之衝擊，依契約規章及法令法規予以懲處。

2. 第三方承包廠商在執行本機關委外業務時若有複委託之需求，應評估複委託業務相關之資訊安全風險。並要求承包廠商依資訊安全管理制度(ISMS)等相關規定對複委託廠商進行適當之監督與管理。

(十六) 委外專案之資訊安全要求

對內部及外部專案管理的過程中，應明訂及陳述與專案相關之各項資訊安全要求，並由風險評鑑之結果用以決定及實作資訊安全控制措施，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊(含個人資料)外洩及違反法令之風險。

(十七) 智慧型裝置的管理

應制定可攜式資訊設備(包含智慧型移動裝置)及可攜式儲存媒體之管理要求，要求相關人員落實執行，並定期針對可攜式資訊設備(包含智慧型移動裝置)及可攜式儲存媒體進行風險評鑑，依據風險評鑑之結果選擇適切之控制措施，定期執行查核作業，確保使用可攜式資訊設備及儲存媒體之風險受到監控，降低機密資料外洩之風險。

(十八) 文件管理與公告

因應本系統及資訊安全管理需要，應責成適當人員制訂及維護相關文件（包括書面及電子形式）並依本系統相關管理程序之規定辦理。

(十九) 法令遵循與懲處

本系統相關之作業人員須遵守資訊安全及**個資法**相關法令，並遵守合約之規範。本系統相關作業人員應簽署「資訊安全保密協定」，以確保人員均了解並遵循上述法令規範。違反本政策各項規定之人員，視情節重大程度依相關規章議處。

(二十) 本系統應參考資訊服務管理系統流程關聯參考圖(如下圖)，逐步推展及落實。

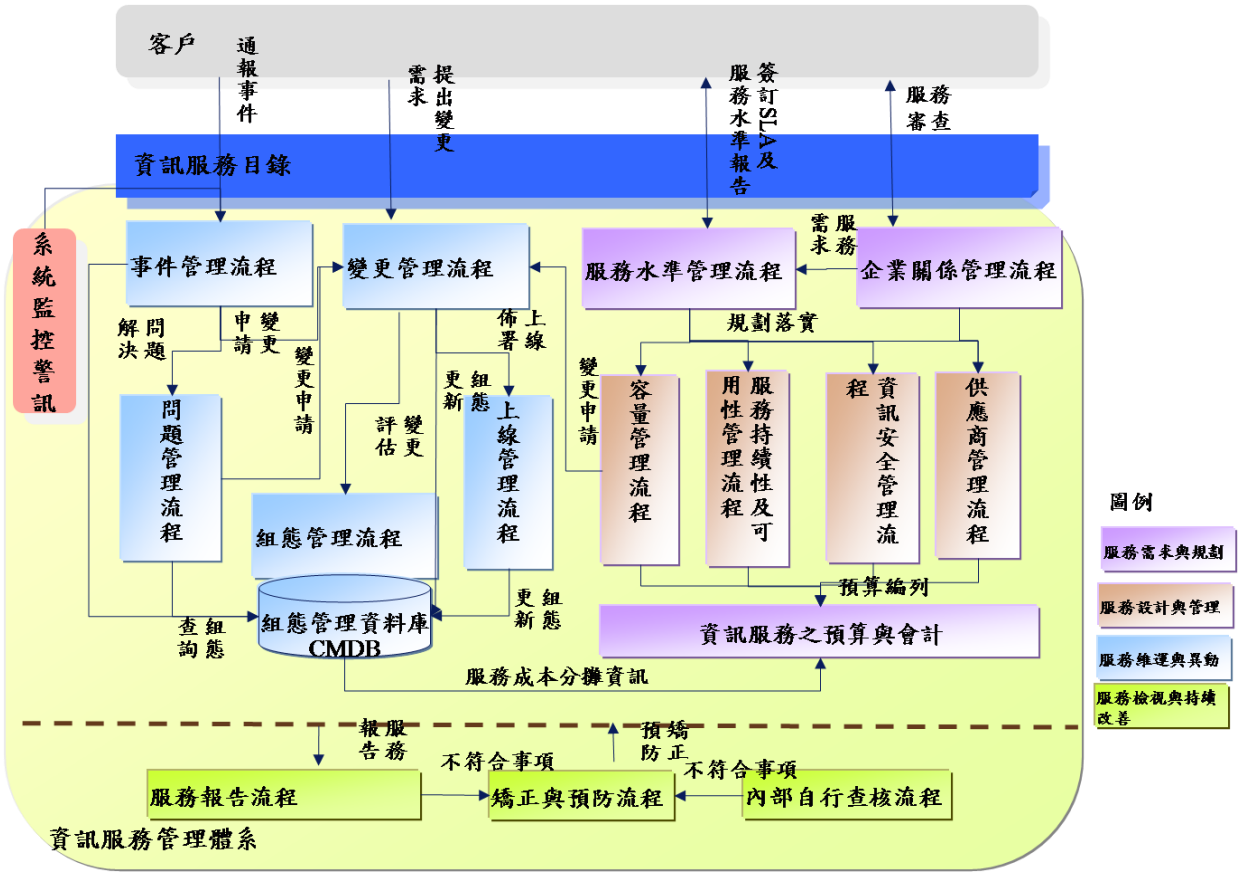

圖1.　資訊服務管理系統流程關聯參考圖

六、 修訂與公告

(一) 本政策每年應至少審視一次，以反映新的資訊安全需求、政府法令法規、外在網路環境變化及資訊安全技術等最新發展現況，以確保 ISMS 對於維持營運和提供適當服務的能力。

(二) 本政策如遇重大改變時應立即審視，以確保其適當性與有效性。在必要時應告知相關單位、人員及委外廠商，以利共同遵守。

(三) 本政策之管理、擬定與修正由本小組負責，提送「商業司資訊安全推行小組」會議審議通過後發布實施。