限定使用

台灣中油股份有限公司

資訊系統管理

d-80-10-0-01 資訊管理政策彙編

第二十版

各單位資訊部門編撰

資訊處處長核定

核定日期 2014 年 11 月 30 日

.索引.

文件修正一覽表

文件修正一覽表			
修改次數	修改日期	修改版別	修改內容
1	95/3/1	1	彙編資訊安全政策
2	95/5/23	2	1.配合 ISO27001 版，修訂相關參考文件，資訊安全範圍與資訊安全之原則、標準 2.配合 ISO27001 版，修訂各項政策
3	95/6/15	3	1.增加 4.9 內容：運用新興科技或處理新型態資安威脅之程序 2.財政部證期會更名為行政院金融監督管理委員會證期局
4	95/6/22	4	行政院金融監督管理委員會證期局需更名為行政院金融監督管理委員會
5	95/7/19	5	頁首編碼錯誤需更新
6	95/11/24	6	定義資訊安全管理政策
7	95/12/15	7	增修資訊安全監控中心政策、網管監控中心政策、備份政策、視訊交換、傳真交換政策
8	96/3/3	8	更改公司名稱
9	96/3/21	9	更改參考文件中之公司名稱
10	96/6/01	10	修改使用通行碼政策對應之作業要點為網路使用作業要點
11	96/6/29	11	依據經濟部 96.6.11 經資字 09600579560 號函辦理,資訊傳播政策，增加 17.4 項
12	97/3/26	12	資訊推動暨資通安全處理小組更名

文 件 修 正 一 覽 表			
修改次數	修改日期	修改版別	修改內容
			為資通安全處理小組
13	98/7/22	13	增訂使用自由及免費軟體之政策。
14	99/10/22	14	個人資料保護法更名。
15	100/05/09	15	配合 100 年資訊業務研討會提案決議，修改第 9.1.2 節。
16	100/06/15	16	修訂 17.資訊傳播政策，新增 17.5.知識管理相關條文。
17	101/06/22	17	內控檢視
18	101/09/10	18	修改 12.2 通行碼八位以上
19	103/07/16	19	增加 28.行動裝置及雲端安全政策
20	103/11/30	20	配合 ISO27001 2013 年版修正

1.目的

為提升本公司資訊安全整體意識及關於資訊安全之各項行動原則，特依照本公司營運與法律或法規要求、契約安全義務、與本公司策略性風險管理連結建立評估風險之準則，建立資訊安全管理(ISMS)政策，作為相關人員遵循之依據，如有違反本原則之各項規定，初犯函送單位主管給予糾正，再犯則停止其帳號之使用並送交人事部門依情節輕重予以申誡或記過之懲處。

2.適用範圍

2.1.本公司資訊人員，資訊使用者，業務相關之第三方人員。

2.2.本資訊管理安全彙編，除資訊安全政策編定與修訂需經資通安全處理小組核准後實施，其餘資訊安全管理政策視性質由資訊主管核准後實施。

3.相關參考文件

3.1.國家機密保護法及本公司機密業務資料管理實施要點。

3.2.行政院及所屬各機關資訊安全管理要點及規範。

3.3.經濟部標檢局資訊技術-安全技術-資訊安全管理系統-要求。

3.4.行政院金融監督管理委員會公開發行公司建立內部控制制度處理準則。

3.5.個人資料保護法。

3.6.行政機關電子資料流通實施要點。

4.資訊安全政策

4.1.為確保本公司資訊的機密性，完整性，可用性，並符合公司營運需求，特制定資訊安全政策。以貫徹「資訊安全認知人人有

責，資訊安全管理人人做到，習慣成自然」。

4.2. 資訊安全定義：將安全保護措施的規則應用於電腦系統，並使電腦系統可正常無誤的運作。

4.3. 資訊安全目標：強化資訊安全管理，建立安全及可信賴之電腦系統，確保資料、系統、設備及電信通訊安全，保障本公司及社會大眾權益。資訊安全目標以量化方式轉化成績效衡量項目定期考核。

4.4. 資訊安全範圍：

4.4.1. 資訊安全政策。

4.4.2. 資訊安全之組織。

4.4.3. 人力資源安全。

4.4.4. 資產管理。

4.4.5. 存取控制。

4.4.6. 密碼學。

4.4.7. 實體與環境安全。

4.4.8. 運作安全。

4.4.9. 通訊安全。

4.4.10. 系統取得、開發及維護。

4.4.11. 供應者關係。

4.4.12. 資訊安全事故管理。

4.4.13. 營運持續管理之資訊安全層面。

4.4.14. 遵循性。

4.5. 資訊安全之原則、標準：

4.5.1.國家機密保護法及本公司機密業務資料管理實施要點。

4.5.2.行政院及所屬各機關資訊安全管理要點及規範。

4.5.3.經濟部標檢局資訊技術-安全技術-資訊安全管理系統-要求。

4.5.4.行政院金融監督管理委員會公開發行公司建立內部控制制度處理準則。

4.5.5.個人資料保護法。

4.6.員工應負的一般性及特定的資訊安全責任，並遵守下列事項之要求及規定：

4.6.1.政府法令及契約對機關資訊安全之要求及規定。

4.6.2.台灣中油股份有限公司工作規則。

4.6.3.資訊安全教育及訓練。

4.6.4.電腦病毒防範。

4.6.5.業務永續運作計畫。

4.7.資訊安全工作之組織、權責及分工：

4.7.1.本公司成立資通安全處理小組，負責督導、推動及協調資訊安全相關政策、計畫及措施。

4.7.2.資訊安全管理之分工原則：

(1)資訊安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項，由資訊單位負責辦理。

(2)資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。

(3)資訊機密維護由政風單位會同相關單位負責辦理。

(4)稽核使用管理事項由稽核單位會同政風單位辦理。

(5)未設置資訊及政風單位者，由機關首長指定適當的單位及人員負責辦理資訊安全管理事項。

4.8.資通安全事件發生時依據緊急應變計畫暨作業處理程序處理。

4.9.資訊安全之評估：採用 PDCA（Plan，Do，Check，Act）過程模式定期進行獨立及客觀的評估，以反映政府資訊安全管理政策、法令、技術及機關業務之最新狀況，運用新興科技或處理新型態資安威脅之程序，確保資訊安全實務作業確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。資訊安全評估的對象如下：

4.9.1.資訊設施及系統提供者。

4.9.2.資訊及資料擁有者。

4.9.3.使用者。

4.9.4.管理者。

4.9.5.系統維護者。

4.9.6.其他有關人員。

4.10.資訊安全風險評鑑機制：針對資產價值，弱點產生之衝擊性、威脅發生機率評鑑風險值，產生風險評鑑報告，由資通安全處理小組決定風險可接受程度，各單位提報風險處理計畫與控制措施，將風險值降低至風險可接受程度內。

4.11.資訊安全政策及規定之宣達：需以書面、電子或其他方式通知員工及與本公司連線作業之公私機構及提供資訊服務之廠商

共同遵行。

4.12. 本資訊安全政策經資通安全處理小組核准後實施，修訂時亦同。

5.組織整體政策

（對應之作業要點：d-80-10-0-00 資訊安全管理規範）

請參閱台灣中油公司外部網頁/永續經營政策。

6.人員篩選政策

（對應之作業要點：d-80-10-0-00 資訊安全管理規範）

請參閱台灣中油股份有限公司工作規則。

7.淨空政策

（對應之作業要點:d-60-20-0-01 網路使用作業要點,d-80-50-0-01 實體與環境安全作業要點）

7.1.螢幕淨空

7.1.1.除非有適切的鎖定機制，當作業結束時，應關閉有效的通信管道。

7.1.2.當通信結束時，應完全登出電腦系統，不宜只關閉電腦系統或是端末機。

7.1.3.當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及端末機的安全。

7.2.桌面淨空：機敏資料不應置於桌面，需置於上鎖抽屜中。

8.電子郵件政策

（對應之作業要點：d-60-20-0-04 電子郵件使用原則）

8.1.電子郵件具有正式文件之效力，同仁應以負責的態度與合法的方式予以有效的應用。

8.2.使用電子郵件時應尊重智慧財產權。

8.3.嚴禁使用電子郵件傳遞本公司或商業夥伴之業務機密。

8.4.如有違反本公司電子郵件使用原則之各項規定，初犯函送單位主管給予糾正，再犯則停止其帳號之使用並送交人事部門依情節輕重予以申誡或記過之懲處。

9.存取控制政策

（對應之作業要點：d-70-10-0-02 資訊系統正式作業要點）

9.1.使用者註冊控制

9.1.1.使用者必須經過系統所有人確認授予存取權限等級是否符合營運目的。

9.1.2.使用者因調職或離職、留職停薪、請長假、出國進修，應於接獲人事單位通知後，立即移除其使用權限。

9.2.正式作業過版控制

9.2.1.對納入正式作業之程式館及資料檔案，應制定過版作業程序，如遇緊急狀況時，亦應制定緊急狀況處理程序以為因應。

9.2.2.對正式作業之原始程式碼及資料檔案，應依業務所需，制定存取權限控制措施。

9.2.3.對正式作業之原始程式碼，應有版本控制措施，以確保必要時之復原。

9.3.網路存取控制

9.3.1.對公司內部及外部網路服務的存取行為應加以控制。

9.3.2.必須確保存取網路和網路服務的使用者不會破壞網路服務的安全性。

9.3.3.公司內部及外部網路與其他組織擁有的網路或公共網路間需有適當的介面。

9.3.4.對使用者和設備有應建立適當的身份鑑別機制。

9.3.5.應建立強制性的通道，防止未被授權的使用者從不同的管

道進入電腦系統。

9.3.6. 開放公司以外的使用者從公眾網路，或從公司網路以外的網路與本公司連線作業，應建立遠端使用者身分鑑別機制，以降低未經授權存取系統的風險。

9.3.7. 應建立遠端電腦系統與本公司連線作業之身分鑑別安全機制。

9.3.8. 網路系統規模過於龐大者，可考量將不同使用者及電腦系統分開成不同的領域，以降低可能的安全風險。

9.3.9. 為確保系統安全，跨公司機關的網路系統可限制使用者之連線作業能力。

9.3.10. 分享式的網路系統，應建立網路路由的控制，以確保電腦連線作業及資訊流動，不會影響應用系統的存取政策。

9.3.11. 使用公用或私有網路，應評估網路服務提供者之安全措施是否足夠、是否提供明確的安全措施說明，並應考量使用該項網路對維持資料傳輸機密性、完整性及可用性等各種安全影響。

9.4. 作業系統存取控制

9.4.1. 為防止未經授權的電腦存取，應採用作業系統層級的安全設施來限制對電腦資源的存取，這些設施應能鑑別和確認身分。

9.4.2. 記錄存取系統成功和失敗的動作。

9.4.3. 提供適當的身份鑑別方法，如果使用通行碼管理系統，應確保提供嚴謹的通行碼。

9.4.4.必要時得限制使用者的連線時間。

9.5.資訊系統存取管理

9.5.1.資訊系統應對正式資料、測試資料、原始程式及作業軟體制定存取限制。

9.5.2.資訊系統應對具有特別權限及特定人員存取權限加以控管。

9.5.3.應制定第三者存取之安全契約。

9.5.4.應制定資訊作業委外服務之安全管理。

10. 網路服務政策

（對應之作業要點：d-60-20-0-02 網路管理作業要點）

10.1. 本公司個人電腦之網址一律加入本公司網域，遵循資訊部門所分配之網址，不得自行更改指定。

10.2. 本公司內部網路(Intranet)只開放本公司同仁使用，非本公司同仁只能至網際資訊網站瀏覽相關資料，至於公司外部網路（Extranet）則僅開放業務相關同仁與第三方使用。

10.3. 提供給內部人員使用的網路服務，與開放有關人員從遠端登入內部網路系統的網路服務，應執行嚴謹的身分辨識作業，或使用防火牆進行安全控管。

10.4. 對敏感或重要營運應用程式、或是與處於高風險區域的使用者連線時，應建立控制措施。

11.可攜式設備政策

（對應之作業要點：d-80-50-0-01 實體與環境安全作業要點）

11.1.可攜式設備之核發，悉依本公司一般物品管理要點相關規定辦理。

11.2.可攜式設備介接公司內部網路，使用前應先確認未感染病毒。

11.3.第三方人員因業務需求於公司內部可攜式設備應經相關業務部門核准後始得攜入，介接公司內部網路，亦應經申請並經核准後方得介接。

11.4.使用單位對單位內部可攜式設備負有督導與管理責任，如發現違反規定者，初犯函送單位主管糾正，再犯停止使用可攜式設備。

12.使用通行碼政策

（對應之作業要點：d-60-20-0-01 網路使用作業要點）

12.1.使用者選擇及使用通行碼時，應遵守公司資訊安全規定。

12.2.新建帳號之預設通行碼應避免以明文方式轉交使用者，經使用者確認無誤後需回應系統管理者，且於第一次使用時應即更換通行碼，須至少為八位以上之文數字，爾後應定期更換通行碼，每三個月更新一次為原則，並避免重複使用前六次之舊通行碼。

12.3.個人應負責保護通行碼，維持通行碼的機密性避免通行碼洩漏遭人竊取冒用。

12.4.當有跡象足以顯示系統及使用者通行碼可能遭破解時，應立即更改通行碼。

12.5.使用帳號通行碼連續錯誤三次帳號將暫停使用。

12.6.使用帳號通行碼忘記或遭暫停使用時，若欲重新啟用應提出異動需求，經系統管理人員確認身份後進行異動處理。

13.飲食吸菸政策

（對應之作業要點：d-80-50-0-01 實體與環境安全作業要點）

13.1.機房、電腦教室內嚴禁吸煙、飲食。

13.2.在特定的作業環境下，可考慮使用鍵盤保護膜。

14.惡意軟體政策

（對應之作業要點：d-60-20-0-02 網路管理作業要點）

14.1.應採行必要的事前預防及保護措施，防制及偵測電腦病毒、特洛依木馬及邏輯炸彈等惡意軟體的侵入。

14.2.應依「事前預防重於事後補救」的原則，採行適當及必要的電腦病毒偵測及防範措施，健全系統之存取控制機制。

15.資訊分享政策

（對應之作業要點：d-60-20-0-02 網路管理作業要點）

15.1.資訊分享應依據國家機密保護、個人資料保護、政府資訊公開等相關法規及本公司「文書處理手冊」規定。

15.2.提供資訊分享之資訊，應有保護措施避免遭到未經授權存取與竄改。

15.3.各單位資料欲公佈於資訊網站時，需先徵得該單位主管之同意，並需保持資料之正確性。

16. 資訊傳送政策

（對應之作業要點：d-50-20-0-01 資訊系統開發作業要點）

16.1. 電子資料傳送：機關與來往對象進行電子資料傳送，應視資料特性採行不同等級的安全保護措施，以確認身分並防止未經授權的資料存取及竄改。

16.2. 書面資料傳送：機關與來往對象進行書面資料傳送，應有傳送清冊雙方確認。

16.3. 視訊傳送：提供視訊會議服務應考量採取適當安全機制，確保資訊傳送安全。召開具機敏性內容之會議，須避免使用網路視訊會議。

16.4. 傳真傳送：傳真機敏性內容文件，應親自或由專人傳送並予以登記，以控制文件之送達及收受管理。

16.5. 網路語音電話：提供企業內部 VoIP 網路語音電話服務，相關通話紀錄應採取適當保護機制，確保通話紀錄之安全。並須避免使用網路語音電話談論機敏性內容之議題。

17.資訊傳播政策

（對應之作業要點：d-60-20-0-01 網路使用作業要點）

17.1.配合本公司各項業務資訊之上網公告需要，應考量資訊安全需求與資訊之使用對象，俾據以設定審核程序及授權瀏覽範圍與對象。

17.2.本公司內部網路及全球資訊網資訊之上網，應由資料提供單位主管審核，確認授權瀏覽範圍與對象，並依網站內容授權出版程序，由各單位自行上網，或委由網站負責單位上網刊載；各單位處室網站資訊之上網由各單位處室自行負責。

17.3.電子公佈欄資訊之公告，凡以總公司或各單位名義發文公告周知之公文或消息均應依照本公司電子公佈欄管理要點辦理，其他業務資訊及企業活動訊息等公告之發佈應由公告提供單位主管審核後始得進行。

17.4.於電子化政府入口網提供服務，應依據行政機關電子資料流通實施要點規定，提供銓釋資料及分類檢索規範。

17.5.本公司知識管理系統知識文件之上傳，應遵循本公司知識管理推動辦法之規定，由文件提供單位確認授權瀏覽範圍與對象，並由各單位處室授權同仁負責自行上傳。

18. 資訊授權政策

（對應之作業要點：d-60-20-0-01 網路使用作業要點）

18.1. 資訊資源應予保護，使用者須取得授權始可存取運用。

18.2. 針對離、退、留職停薪、請長假、出國進修及異動人員，應檢視其所取得之相關授權並予移除。

18.3. 定期清查各使用者所取得之授權是否妥適。

18.4. 第三方之授權，除權，與變更權限，除須與契約範圍吻合外亦須依據本政策辦理。

19.資訊分級政策

（對應之作業要點：d-60-30-0-01 資訊資產管理作業要點）

19.1.應依據國家機密保護、個人資料保護、政府資訊公開等相關法規及本公司「文書處理手冊」,建立資訊安全等級之分類標準，以及相對應的保護措施。

19.2.應納入安全等級分類的項目，包括書面報告、儲存媒體、電子訊息、檔案資料及電腦報表，可依據相關法規區分機密性、敏感性及一般性等三類。

19.3.已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

19.4.界定資訊安全等級之責任，應由資料的原始產生者，或是由指定的系統所有者負責。

20.閘道及防火牆政策

（對應之作業要點：d-60-10-0-01 電腦系統管理作業要點）

20.1.本公司網際網路出入通道，皆應設立防火牆管制。

20.2.為確保網路安全至少需區分公司外部網路、隔離區(DMZ)與公司內部網路區段。

20.3.防火牆原則設定為阻絕所有服務，只讓特定許可的服務通關。

20.4.對外開放網路資源時，需限制使用者身份、來源位置、服務內容與使用時間，並應加強使用者身份認證機制。

20.5.防火牆進出皆需保有紀錄，並需經常檢視以發現異常紀錄。

21.紀錄保留政策

（對應之作業要點：d-70-20-0-01 電腦系統操作作業要點，d-60-30-0-01 資訊資產管理作業要點）

21.1.記錄應按記錄類型進行分類及保存至符合法律或法規要求的規定時間。

21.2.應考慮儲存記錄的儲存媒體壞損的可能性，定期進行復原測試。

21.3.應實施適切的控制措施保護記錄，以防止遺失、遭毀壞和竄改，且支援必要的營運活動。

21.4.在規定時間期滿後如果組織不再需要記錄，應採用適切的方式予以銷毀。

22.遠距工作政策

（對應之作業要點：d-60-20-0-02 網路管理作業要點）

22.1.公司外部取得授權的電腦主機或網路設備，與公司內部網路連線作業時，應確實遵守網路安全規定及連線作業程序。

22.2.提供第三方以遠端登入方式進入電腦網路系統進行業務活動的通信作業埠，亦須納入管控，並採取特別的安全控管機制。

22.3.開放公司以外的使用者從公眾網路，或從公司網路以外的網路與本公司連線作業，應建立遠端使用者身分鑑別機制，以降低未經授權存取系統的風險。

22.4.可考量使用資料加密等安全技術，鑑別網路使用者之身分。

23.使用授權軟體政策

（對應之作業要點：d-60-30-0-01 資訊資產管理作業要點）

23.1.不應保有及使用未取得授權的軟體。

23.2.須在原授權許可之外的機器上使用軟體時，應取得正式的授權或另行採購。

23.3.定期稽核使用者軟體數量、版權及軟體使用情形。

23.4.使用有智慧財產權的軟體，應遵守相關法令及契約規定。

23.5.自由及免費軟體，未經核准，不得自行安裝使用，使用時需了解版權宣告並遵守。申請使用時，應附該軟體使用聲明供審查，避免違反著作權法保護智慧財產。

24.銷毀轉讓政策

（對應之作業要點：d-60-30-0-01 資訊資產管理作業要點）

24.1.軟體及硬體設備，報廢、銷毀及轉讓，應依固定資產管理辦法規定辦理，報廢、銷毀時須確認資產中的資訊已清除。

24.2.軟體功能無法滿足業務所需，或已無法搭配現行作業平台使用，甚或原廠已無法提供版本更新時，資產管理權責人員，於每年定期清查後列印硬軟體設備報廢表經陳核後送財產管理部門銷帳。

24.3.爲了防止複製品損壞而製作備份複製品。這些備份複製品不得通過任何方式提供給他人使用，並在所有人喪失該合法複製品的所有權時，負責將備份複製品銷毀。

24.4.軟體終止授權時，應依約或依提供人要求返還或移除、銷毀，如有複製時亦同。

24.5.軟體應依固定資產管理辦法規定辦理須經資產管理權責人員核報，經核准後，始得將其全部或部分移轉頂讓予第三人。

25.資訊安全監控中心政策

（對應之作業要點：d-60-20-0-05 資安監控中心管理作業要點）

25.1.資訊處為本公司安全監控中心專責部門。

25.2.資訊安全監控中心旨在提供企業重要網路安全設備，如防火牆、入侵偵測系統、網頁檔案保全系統等之 7*24 即時監控服務。

25.3.針對任何偵知並通報各單位的資訊安全事件，嚴重等級屬緊急者於 4 小時內處理完成、屬高度者於 3 天內處理完成、屬中度者於 5 天內處理完成為原則，並回報處理情形。

25.4.本中心必要時得委外維運，惟需明訂專案之服務水準協定，並定期評估廠商之運作績效。

26.網管監控中心政策

（對應之作業要點：d-110-10-0-01 電信服務管理作業要點）

26.1.資訊處電信所為本公司網管監控中心專責部門。

26.2.網管監控中心提供本公司電信通信網路系統、設備以及實體光纖路由之 7*24 小時即時監控服務。

26.3.針對任何監控偵知之通信障礙或通訊阻斷等各項網路傳輸異常狀況，立即填報相關表單並通知所屬轄區或負責人員處理，以及記錄與確認障礙或阻斷修復時間。

26.4.本中心必要時得委外維運，惟需明訂專案之服務水準協定，並定期評估廠商之運作績效。

27.備份政策

（對應之作業要點：d-70-10-0-01 營運持續管理作業要點）

27.1.定期執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

27.2.系統資料備份及備援作業，應符合公司業務持續營運之需求。

27.3.正確及完整的備份資料，除存放在主要的作業場所外，應異地存放，以防止主要作業場所發生災害時可能帶來的傷害。

27.4.重要系統之異地存放媒體資料應有加密保護措施。

27.5.重要資料的備份，以維持三代為原則並訂定保存期限。

27.6.備份資料應有適當的實體及環境保護，其安全標準應與主要作業場所的安全標準相同。

27.7.應定期測試備份資料，以確保備份資料之可用性。異地存放之媒體應有加密措施。

28. 行動裝置及雲端安全政策

（對應之作業要點：d-60-30-0-03 智慧型行動裝置管理機制）

28.1. 智慧型行動裝置應安裝防毒軟體，使用人需注及更新病毒碼至最新版本，並視業務需要增設相關通行碼。

28.2. 智慧型行動裝置介接公司內部網路，使用前應先確認未感染病毒。

28.3. 智慧型行動裝置從外部介接公司內部網路，需透過虛擬私人網路(VPN)，對使用者進行身分認證，加密資料流，以防止未經授權的非法存取。

28.4. 第三方人員因業務需求於公司內部智慧型行動裝置應經相關業務部門核准後始得攜入，介接公司內部網路，亦應經申請並經核准後方得介接。

28.5. 請勿將公司資料儲存於公司外部公有雲，避免資料可能洩漏之缺失。