行政院農業委員會

農業金融局

■一般 □限閱 □密

資訊安全政策

文件編號：1-01

版本：2.1

施行日期：中華民國 95 年 08 月 01 日

審核單位	
權責單位	資訊安全推行委員會

版本修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人
1.0	95.08.01	文件初版	第一組	林有恆
1.1	99.10.23	更改個人資料保護法名稱	第一組	林有恆
1.2	100.05.04	修訂文件安全等級	第一組	林有恆
1.3	102.06.11	修正資訊安全推行委員會工作小組之召集人層級	第一組	林有恆
2.0	104.01.30	配合本局資訊安全標準 ISO 27001：2005 轉版為 ISO 27001：2013	第一組	林有恆
2.1	107.12.22	根據資通安全管理法增修資通安全事件名稱及召集人職稱為資通安全長	第一組	林有恆

行政院農業委員會農業金融局資訊安全管理規範

第一章、總則

一、行政院農業委員會農業金融局（以下簡稱本局）為強化資訊安全管理、維護網路資訊系統的正常運作、確保網路資訊傳輸交易安全，並保障本局電腦處理資料之機密性、完整性與可用性，特訂定本規範。

第二章、資訊安全組織與分工

二、成立資訊安全推行委員會，由督導資訊業務之副局長或高層主管人員負責擔任總召集人兼資通安全長，委員會成員由各單位指派人員兼任之，負責制定及定期評估本局資訊安全政策，並統籌負責推動、協調及督導資訊安全管理事項及資源調度之協調研議。

三、成立資訊安全推行委員會工作小組，由資訊單位主管擔任召集人，小組成員為資訊單位同仁及相關科室之同仁，負責制定、評估本局資訊安全之要點、程序及表單。

四、相關資訊安全管理業務之辦理如下：

（一）相關資訊安全教育訓練，由資訊單位及政風單位會同有關單位辦理。

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

（三）稽核相關作業由政風單位會同資訊單位辦理。

（四）人員安全評估由政風單位負責辦理。

第三章、規範內容

五、本局應依有關法令，考量業務需求，進行資訊安全風險評估，採行適當及充足之資訊安全措施，確保本局資訊蒐集、處理、傳送、儲存之安全。

六、有關下列事項，應訂定資訊安全相關規定並切實執行：

（一）資訊安全政策的制定及評估。

（二）資訊安全組織及權責。

（三）人員安全管理及教育訓練。

（四）電腦系統安全管理。

（五）網路安全管理。

（六）系統存取控制。

（七）系統發展及維護之安全管理。

（八）資訊資產之安全管理。

（九）實體及環境安全管理。

（十）業務永續運作計畫之規劃及管理。

（十一）全景風險評鑑。

（十二）其他資訊安全管理事項。

七、本規範所稱資訊安全政策，係指本局為達成資訊安全目標訂定之資訊安全管理作業辦法、注意事項及其他相關規範等。

第四章、資訊安全目標

八、為確保資訊資產之機密性及防止非法使用，非法存取之事件，每年發生次數不得超過 3 次。

九、為確保資訊系統及設備之完整性、可用性及安全性，每一資訊系統因資通安全事件導致服務停頓，每半年小於 3 次(含)以下，每次不得超過 36 小時。

十、為確保資訊業務運作之有效性及持續性，每半年至少需執行 1 次「資訊業務持續運作計畫」之演練。

十一、為確保組織全景風險評鑑之有效性及持續性，每 1 年至少需執行 1 次「全景風險評鑑」。

十二、為確保職員對資訊安全有一定認知，每人每年至少應接受 4 小時以上的資訊安全教育訓練。

十三、為確保資安措施符合政策及法令要求，每半年至少稽核 1 次。

第五章、資訊安全政策訂定

十四、本局應依實際業務需求，訂定資訊安全政策，並以書面、電子或其他方式告知本局員工及相關機構共同遵行。

十五、本局所訂定之資訊安全政策，應每半年配合資安推行委員會召開評估 1 次，並得視需要隨時評估，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

第六章、人員管理及資訊安全教育訓練

十六、　人員進用時，應填具保密切結書及著作權約定書，以明權責。

十七、　對負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，實施

人員輪調，以建立人力備援制度。

十八、 加強資訊安全管理人力之培訓，提升資訊安全管理能力。

十九、 資訊安全教育訓練及宣導應定期或不定期實施。

第七章、電腦系統安全管理

二十、 辦理資訊業務委外作業，應明定廠商之資訊安全責任及保密規定，並列入業務委外之契約，要求廠商遵守。

二十一、對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

二十二、應依相關法規規定或契約約定於電腦及其相關設備上，複製及使用軟體，並禁止使用非法軟體。

二十三、須裝置防毒軟體於電腦設備，以偵測及防制電腦病毒，確保系統正常運作。

第八章、網路安全管理

二十四、本局利用公眾網路傳送資訊或進行交易處理，應評估安全風險，確定安全需求，研擬妥適的安全控管措施。

二十五、與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與本局內部網路之資料傳輸及資源存取。

二十六、機密性資料或文件除經加密外，不得以電子郵件傳送；機密性資料以外之敏感性資料如有需要，應經加密處理後傳送。

第九章、系統存取控制管理

二十七、依各級人員執行職務所需，賦予必要之系統存取權限；若使用者調整職務及離職時，應儘速註銷其系統存取權限。

二十八、電腦使用者應列冊管理，建立識別碼、通行碼（密碼）管理制度，並要求使用者應定期更新通行碼。

二十九、重要資料如需委外建檔者，應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

第十章、系統發展及維護安全管理

三十、 程式版本之更換，應訂定作業程序，據以辦理。

三十一、資訊檔案之更新、更正或註銷，應建立變更程序。

三十二、對委外廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，資訊單位應視實際作業需要核發識別碼及通行碼供廠商使用，並於使用完畢後立即取消其使用權限。

三十三、委託廠商建置及維護重要軟硬體設施時，應在本局相關人員監督及陪同下始得為之。

第十一章、全景風險評鑑

三十四、首先取得資訊安全推行委員會對組織營運宗旨與目標的看法與共識。

三十五、參考行政院國家資通安全會報「資訊系統分級與資安防護基準作業規定」，將個別資訊系統安全等級分為普、中、高三級，依資料保護受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及財物損失等六大影響構面，分別考量資訊系統於發生資訊安全事故時可能造成的衝擊，即衡量資訊系統資料外洩、資料遭竄改、系統故障等情事時可能造成的後果嚴重程度，並據以評估、設定衝擊等級，如全景風險評鑑衝擊等級表。

三十六、識別所有資訊系統並依特性完成安全等級評估，針對等級「中」以上，資訊系統擬定對應策略，投注相當資源，以維持組織正常運作。

三十七、依據 CNS 31000 要求，鑑別內、外部關注方之需求與期望。

三十八、針對關注事項提出因應策略或現有控制措施，透過討論或其他程序，取得相當的共識，內部關注者可能包含管理階層、其他部門等，外部關注方可能包含上級機關、平行機關、供應者等。

三十九、將相關評鑑過程及記錄、結果、建議事項，填註於「全景風險評鑑評估表」(需編號)，由資訊安全推行委員會評估各項需求與目標，決定是否將本系統納入資訊安全管理系統實施或驗證範圍，並留存相關紀錄。

四十、　經決策程序納入資訊安全管理系統實施或驗證範圍之資訊系統，依照資產風險評鑑程序實施風險評鑑。

第十二章、資訊資產安全管理

四十一、各項資產依據其作業內容特性，區分為電子化資訊資產、實體資產、軟體資產、服務資產、書面文件資產及人員資產等六大類。

四十二、各類資產並依照其所具有之機密性、完整性及可用性評估該資產反應出之價值。

四十三、根據資產本身之脆弱性、威脅及衝擊，評鑑其風險等級。經分級與評鑑後，依其所具備之價值，施以適當程度之安全控管。

四十四、執行風險評鑑後，將資產區分為不同風險等級，其中屬於「不可接受風險」

之資產，應訂定「風險控制計畫」據以監督控管，並落實執行追蹤控制。

四十五、各類資訊資產應指定專人統籌管理，並列冊備查。

四十六、資訊檔案中個人資料，應依「個人資料保護法」相關規定辦理。

四十七、資訊檔案中金融檢查報告如有涉及存款、放款及匯款等個人資料，參照銀行法第 48 條第 2 項規定之意旨予以保密。

第十三章、實體及環境安全管理

四十八、對需要長期保留或重要檔案之備份媒體，應使用專用保險設備並另處存放。

四十九、電腦機房作業環境，應依電腦設備安裝標準，設置電源、空調、防災及電路等設備，並指定專人負責管理。

五十、　電腦設備應訂定維護合約，並督促廠商確實維護及保養。

五十一、電腦機房等重要場所，應指定專人負責管理，並加強門禁管制及有關安全防護措施。

五十二、對進出電腦機房等重要場所之人員與物品，應加以管理。

五十三、確保遠距工作及使用行動裝置之安全。

第十四章、業務永續運作計畫管理

五十四、建立資通安全事件緊急處理機制，在發生資通安全事件時，應依規定之處理程序，立即向權責主管單位或人員通報，採取反應措施。

第十五章、其他資訊安全管理事項

五十五、本局各項資訊作業，均須遵循本規範規定辦理，各單位為配合作業實際狀況，得增訂相關規範辦理。

第十六章、附則

五十六、本規範未訂定之事項依行政院所訂頒之「資通安全管理法」及相關子法、「行政院所屬各機關資訊安全管理規範」及相關規定辦理。