新竹市稅務局

文件名稱：資訊安全與個人資料保護政策

文件編號：ISMS-1-16001

制定部門：稅務管理科

修訂紀錄				
修訂日期	版次	頁次	修訂內容摘要	機密等級
107/10/30	10	6 7	新增防火牆政策應每年 10 月底前清查一次。 新增特殊權限帳號應按季清查。	普通
108/11/05	11	3、4 4 5 5 6 7 8	1.依據行政院訂定「資通安全責任等級分級辦法」,新增完成 B 級公務機關應辦事項規定及組織新增資通安全專職人員。 2.依據 108 年內稽建議事項修正。 3.配合 107 年 ISO27001 追查評鑑之建議，新增法規整檢審議小組職掌。 4.依據行政院訂定「資通安全管理法及其六個子法」，新增資通安全專職人員職掌。 5.配合 107 年 ISO27001 追查評鑑之建議，修正規定。 6.配合實務作業程序修正。 7.依據行政院訂定「資通安全管理法施行細則」，新增委外應注意事項規定。	普通
109/10/28	12	4 7	1.修正組織圖線條標示不重疊，提升可閱讀性。 2.配合 109 年 4 月 22 日修訂之「系統存取控制管理程序書」內容說明文字修正。	普通
110/10/26	13	4 5	1.配合營運持續計畫內容修正組織圖。 2.配合營運持續計畫內容文字修正。	普通

111/10/17	14	5 8	1.依據行政院「各機關資通安全事件通報及應變處理作業程序」，文字新增。 2.依據行政院「資通系統籌獲各階段資安強化措施」，文字新增。	普通
112/11/03	15	5-6 8	1.依據本局 112 年 9 月 14 日簽奉核准，解散資訊五人小組，故刪除之。 2.依據行政院 112 年 2 月 22 日修正「行政院國家資通安全會報組織架構圖」，文字修正。	普通
113/11/04	16	3 8-10	1.配合行政院及所屬各機關資訊安全管理要點停止適用，文字修正。 2.配合程序書內容說明文字新增。	普通

一、為強化資訊安全與個人資料(以下簡稱個資)保護管理，確保資料、系統、設備及網路安全，係依各關注方之需求與情境，經由組織的評估，決定具共識之目的，並設定方向與目標，依據資訊安全與個人資料保護相關法規，並以 ISO 27001 及 ISO 29100 驗證之精神為標準，特訂定本政策。

二、資訊安全治理與個資保護政策及目標：

（一）政策：確保資訊系統安全與落實個資保護，建立安全及可信賴之租稅環境，提升服務品質，保障民眾權益。

（二）目標：

1. 確保本局資訊處理之機密性、完整性及可用性、作業人員之忠誠度、所使用之事務機器(包括電腦硬體、軟體、周邊)及網路系統之可靠性，並確保上述資源免受任何因素之干擾、破壞、入侵、或任何不利之行為與企圖。
2. 確保本局個資蒐集、處理、利用、保存及資訊資產之管控機制符合法令規定。

（三）可量測目標:

1. 確保機房伺服器可用率，以減少資訊安全事件造成服務中斷所帶來的影響。
2. 確保網路設備可用率，以減少資訊安全事件造成服務中斷所帶來的影響。
3. 確保辦公室個人電腦病毒防護率，以減少資訊安全事件所帶來的影響。
4. 確保非法軟體零使用率，以減少資訊安全事件所帶來的影響。
5. 確保主機弱點掃描/滲透測試執行率，以減少資訊安全事件造成服務中斷所帶來的影響。
6. 確保內部稽核執行率，以減少資訊安全或個資安全事件所帶來的影響。
7. 確保資訊安全與個資保護教育訓練完成率，以減少資訊安全或個資安全事件所帶來的影響。
8. 確保個資盤點與風險評鑑作業之執行率，以減少個資安全事

件所帶來的影響。

9.確保個資非特定目的內之利用零發生率，以減少個資安全事件所帶來的影響。

（四）本政策及目標應充分與各關注方溝通，溝通方式包括公開宣告於本局官網或紙本或電子檔案等型式。

三、 資訊安全與個資保護聲明(Announcement)：

(一)本局各項安全管理規範必須遵守政府相關法規之規定。

(二)以資訊安全、個資保護管理系統之國際標準建立與實施管理制度，使資訊安全與個人資料保護政策得以落實。

(三)依資通安全責任等級分級辦法完成附表三 B 級之公務機關應辦事項。

(四)在合法之組織營運下，依誠實及信用方法，以適切、相關且不過度之原則，於特定目的範圍內，蒐集、處理及利用個資；為特定目的以外之利用時，應告知並取得當事人之同意，以確保當事人之權益。

(五)於委託蒐集、處理及利用個資時，應於契約明定受委託單位個資安全保護責任及保密規定，本局並保有監督及查核權利。

(六)尊重當事人對其個資行使個人資料保護法第 3 條規範之各項權利。

(七)設置「資訊安全與個人資料保護管理執行小組」，負責資訊安全及個資保護事項之協調聯繫等相關事宜。

(八)定期清查本局保有之個資檔案，鑑別特定目的及適法性，並識別其作業流程，評估風險及施以適當控制措施。

(九)建立及實施資訊安全與個資保護管理措施，並識別內外部利害關係者，將相關議題提報管理審查會議討論，以確保管理系統之運作與實行。

(十)建立與維護資訊資產及個資檔案清冊，並視需要進行更新，確保正確性及完整性。

(十一)以合於當時之技術措施及管理制度，建立使用紀錄、軌跡資料之證據保存及設備安全保護。

(十二)提升組織成員、委外人員對資訊安全與個資保護之安全意識及管理能力。

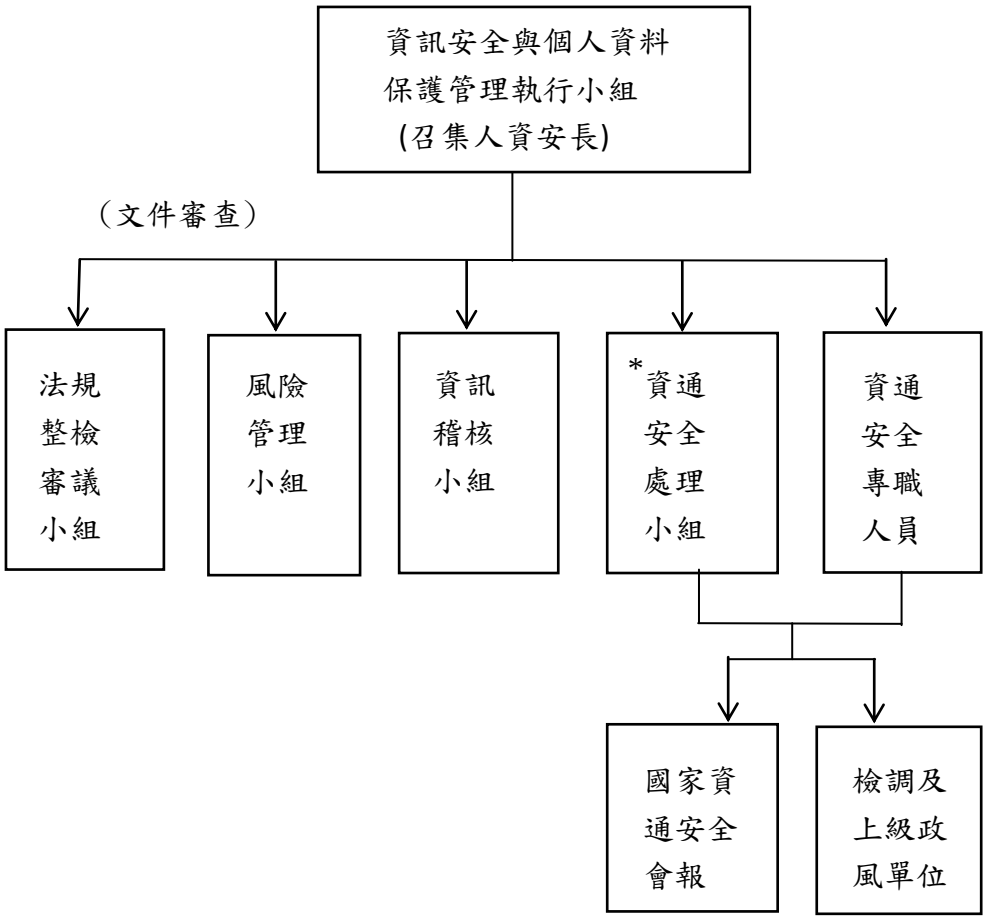
(十三)建立資訊安全、個資外洩事件通報機制，並訂定資訊安全及個資安全事件應變演練計畫定期演練。

(十四)定期辦理內部稽核及召開管理審查會議，以確保管理系統實施之有效性，並符合個人資料保護法規定與國際標準要求。

(十五)應於本局全球資訊網首頁宣告「隱私權政策」，供民眾參閱。

四、 資訊安全與個資保護組織、權責及分工：

（一）資訊安全與個人資料保護管理系統組織架構如下圖，各組織權責及分工依據各相關程序書及規範辦理：



*資通安全處理小組遇1級以上資通安全事件即啟動資通安全事件通報及應變小組任務編組。

（二）資訊安全與個資保護管理事項之協調、推動事宜及成熟度評估，由本局「資訊安全與個人資料保護管理執行小組」統籌辦理。

（三）資訊安全與個資保護相關政策、計畫、措施及安全評估相關事項由風險管理小組辦理。

（四）資訊安全及個資安全事件安全預防、危機處理及稽核工作由資通安全處理小組辦理，遇1級以上資通安全事件即啟動資通安全事件通報及應變小組任務編組，各分組任務參照行政院「各機關資通安全事件通報及應變處理作業程序」，辦理通報、處理及緊急應變事宜；如知悉第三級或第四級資通安全事件後，資通安全長應召開會議研商相關事宜，完成初步損害控制後應召開事件應變會議，並得視情況邀請上級機關或主管機關出席。

（五）資訊安全與個資保護稽核計劃之擬訂及稽核作業之執行、資料彙整與管制，由資訊稽核小組辦理。

（六）資料及資訊系統之安全需求研議、管理及個資保護等事項，由各科室負責辦理。

（七）資訊機密維護、安全稽核及協助資安治理成熟度評估等事項，由政風室會同相關單位負責辦理。

（八）二~四階文件(含表單)訂定、修正及廢止，由法規整檢審議小組審議，提局務會議討論通過，並經核定後實施。

（九）資通安全專職人員2名，由資安幹事及機作人員擔任，負責資訊安全與個人資料保護系統之維運、資通安全維護計畫及實施情形提報及情資分享相關事宜(蒐集回報並會辦各資安業務相關人員因應處理)。

五、資訊安全與個資保護管理範圍：

（一）資訊安全治理。

（二）資訊安全與個資保護風險管理。

（三）人員管理及資訊安全與個資保護教育訓練。

（四）電腦系統安全管理。

（五）網路安全管理。

（六）系統存取控制。

（七）系統發展及維護安全管理。

（八）資訊資產安全管理。

（九）供應者管理。

（十）實體及環境安全管理。

（十一）資訊安全及個資安全事件管理。

（十二）業務永續運作計畫之規劃與管理。

（十三）資訊安全與個資保護稽核。

（十四）管理審查與持續改善管理。

（十五）個資保護蒐集、處理及利用管理。

（十六）當事人權利行使管理。

六、資訊安全治理：

(一)根基於本局營運之目標及策略，在風險管理下，使資訊安全與個資保護策略與業務目標一致、支援業務目標，經由嚴守政策及內部控制確保符合相關法規，以及合宜職責之指派過程，俾以保證資訊安全。

(二)建立指導與監控資訊安全與個資保護活動之機制，以確保承接營運的目標及策略。

七、資訊安全與個資保護風險管理：

（一）建立資訊安全與個資保護風險評鑑制度，進行風險分析與評估作業，發掘資訊、作業流程、資產與組織之安全弱點及其威脅與影響，評鑑其風險等級。

（二）依據評鑑結果彙整成「風險評鑑報告」，由管理審查會或資安長決定可接受之風險等級，並擬定「風險處理計畫」執行及追蹤，以降低本局資訊安全與個資保護風險。

八、人員管理及資訊安全與個資保護教育訓練：

（一）對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

（二）針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全與個資保護教育訓練及宣導，建立員工資訊安全與個資保護認知，提升資訊安全與個資保護水準。

九、電腦系統安全管理：

（一） 辦理資訊業務委外作業，應於事前研提資訊安全需求，契約應明

訂廠商之資訊安全與個資保護責任及保密規定，確實要求廠商遵守並於合約關係中考核。

（二）依相關法規或契約規定，複製及使用軟體，並建立軟體使用管理制度。

（三）採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

十、網路安全管理：

（一）開放外界連線作業之資訊系統，應視資料及系統之重要性，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

（二）與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取，防火牆政策應每年 10 月底前清查一次。

（三）利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

（四）訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。

（五）非經授權不得使用無線網路。

（六）防火牆管理員自資通安全威脅情資取得中繼站清單，應設定防火牆規則進行連線阻擋；瀏覽器(如：Edge、Chrome)進行政府安全組態基準(GCB)套用。

十一、系統存取控制：

（一）訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。

（二）離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

（三）建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新週期，參照國家資通安全研究院發布之政府組態基準(GCB)帳號政策。

（四）對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，課其相關安全保密責任。

（五）特殊權限帳號應按季清查。

十二、系統發展及維護安全管理：

（一）自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量，並依行政院「資通系統籌獲各階段資安強化措施」辦理；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

（二）對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，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

（三）委託廠商建置及維護重要之軟硬體設施，應在本局相關人員監督及陪同下始得為之。

十三、資訊資產安全管理：

（一）建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。

（二）依據國家機密保護、個人資料保護、政府資訊公開及稅捐稽徵法等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。

（三）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。

（四）辦公室區域不得使用非屬本局資訊資產設備，惟外單位或廠商因簡報或系統開發等業務需要，得由相關業務同仁陪同使用，但嚴禁攜入電腦機房。

（五）本局核心資通系統及支援該核心系統之硬體主機、應用系統及作

業系統應進行組態管理。

十四、供應者管理：

（一）委外辦理資通系統之建置、維運或資通服務之提供，選任及監督受託者應參照資通安全管理法施行細則第四條及行政院「資通系統籌獲各階段資安強化措施」規定辦理。

（二）確保對供應者可存取之組織資產的保護，與其協議並以文件紀錄議定之資訊安全要求事項。

（三）建立對供應者之監控、審查與稽核，以維持其資訊安全與個資保護及服務之議定要求。

（四）基於資訊安全，雲端硬碟及雲端主機服務之使用，原則禁止；如確有使用之必要時，需求單位應先進行風險識別及營運衝擊分析，當資訊資產 CIA 值均為低時，方可使用。

十五、實體及環境安全管理：

（一）設備之安全管理包括：電腦配置、通訊纜線安置、電力電源供應、儲存媒體、空調、消防及不斷電系統等。

（二）周邊安全管理包括：周圍環境之安全、人員進出之管制、電腦機房安全管理、辦公桌面之安全管理及電腦設備、資料或軟體移轉之安全管理。

十六、資訊安全及個資安全事件管理：

（一）建立資通安全與個資安全事件通報處理程序及預警機制。

（二）蒐集內外部資通安全威脅相關資訊，以產生威脅情資，並通報資訊技術人員進行更新及改善。

（三）建立管理資訊安全與個資安全事件、事故與重大資訊安全事故及其改善程序。

十七、業務永續運作計畫之規劃與管理：

（一）訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

（二）建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依

規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

（三）依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資訊安全措施。

十八、資訊安全與個資保護稽核：

（一）資訊安全治理與管理之成果評估以資訊稽核方式執行，每年制定資訊安全與個資保護稽核工作計畫定期進行稽核。

（二）稽核業務應採內部稽核與外部稽核兩種方式實施：

1. 內部稽核：包含本局年度定期資訊安全與個資保護稽核、專案不定期稽核、各單位內部自行查核。

2. 外部稽核：接受上級機關定期或不定期派員實施稽核。

十九、管理審查與持續改進管理：

（一）資訊安全與個人資料保護政策及措施，每年定期進行檢討，以反映政府法令、技術及業務等最新發展現況，確保資訊安全與個資保護實務作業之合宜性、適切性及有效性。

（二）持續矯正及改進資訊安全與個人資料保護管理系統異常現象或不符合事項。

二十、個資保護蒐集、處理及利用管理：

（一）個資蒐集應有明確法令依據並限制於所指定目的之必要範圍內，不宜任意蒐集。

（二）個資處理應遵守資料極小化原則，一旦處理之目的終止，無法令依據保有個資時，除因執行職務或業務所必須或經當事人同意者外，應予以刪除或銷毀。

（三）個資之利用、持有及揭露限制於為履行特定、明確及合法目的所必要者，逾期應採安全合宜方式移除或匿名化處理。

二十一、當事人權利行使管理：

（一）建立個資當事人權利行使程序，使其得以簡單、快速及有效率之方式行使權利。

（二）個資當事人對於處理結果有疑義，應循行政救濟程序處理。

二十二、資訊安全之責任分散：

（一）負責重要資訊業務之管理、設計及執行人員應分散權責，建立相互制衡機制，並實施人員輪調，以避免資料或系統遭不法或不當使用。

（二）在資訊人力許可範圍內，應按資訊業務性質分置專人執行下列業務：

1. 業務系統之使用。

2. 資料建檔。

3. 電腦操作。

4. 網路管理。

5. 系統行政管理。

6. 系統發展及維護。

7. 變更管理。

8. 安全管理。

9. 安全稽核。

二十三、資訊安全與個人資料保護政策除尚在進行或準備之方案外，應以書面、電子或其他方式通知員工及與本機關連線作業之有關機關（構）、廠商，如有違反資訊安全與個資保護相關規範，應依相關規定處理。

91 年 12 月 4 日核定實施

93 年 2 月 27 日修正實施

97 年 10 月 30 日修正實施

98 年 5 月 15 日修正實施

98 年 11 月 13 日修正實施

（中華民國 99 年 11 月 2 日新市稅管字第 0990215792 號）

（中華民國 100 年 11 月 9 日新市稅管字第 1000215726 號）

（中華民國 103 年 11 月 5 日新市稅管字第 1030215136 號）

（中華民國 104 年 10 月 29 日新市稅管字第 1040215026 號）

（中華民國 105 年 10 月 6 日新市稅管字第 1050215020 號）

（中華民國 106 年 11 月 15 日新市稅管字第 1060215013 號）

（中華民國 107 年 10 月 30 日新市稅管字第 1076215051 號）

（中華民國 108 年 11 月 5 日新市稅管字第 1086215059 號）

（中華民國 109 年 10 月 28 日新市稅管字第 1096215079 號）

（中華民國 110 年 10 月 26 日新市稅管字第 1106215038 號）

（中華民國 111 年 10 月 17 日新市稅管字第 1116215053 號）

（中華民國 112 年 11 月 3 日新市稅管字第 1126215058 號）

（中華民國 113 年 11 月 4 日新市稅管字 1136215042 號）