德欣寰宇

資訊安全白皮書

壹、前言

德欣寰宇股份有限公司（以下簡稱本公司）致力於系統工程整合服務的研發、營運與行銷，以客戶需求提供專業化、個人化、創新化、品牌化的安全整合解決方案及最佳市場訊息，並因應當前網際網路的蓬勃發展趨勢規劃實用的產品，落實「客戶滿意度即為品質」之服務理念。

貳、範圍

本資訊安全白皮書將介紹本公司在資訊安全管理上的作法，具體涵蓋資訊安全政策、資訊安全組織、人力資源安全、資產管理、存取控制、密碼學、實體及環境安全、運作安全、通訊安全、系統獲取開發與維護、供應者關係、資訊安全事故管理、營運持續管理、遵循性等14個領域。

參、資訊安全管理架構定義

一、資訊安全政策[A5]

本公司服務之資訊安全目標為:建置符合國際標準所要求之資訊安全管理系統(Information Security Management System)，以確保顧問服務如ISO 27001、ISO 20000、ISO 29100、BS 10012等驗證輔導，及資安技術服務如SOC監控服務、資安健診、社交工程、弱點掃描及滲透測試等之機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)及適法性(Compliance)。

本公司服務營運以確保資訊安全為前提,而達成資訊安全的目標則是全體公司同仁的責任，提供無虞之服務亦為本公司的決心與承諾。

二、資訊安全組織[A6]

(一)、 資訊安全團隊

本公司為了提供國內外企業(電信、醫療、證券金融業等)、公私立學校及政府機關(構)最安全完善的服務，成立了資訊安全管理團隊，團隊組成由專案管理部、技術部、顧問部等團隊所組成，團隊成員的專業能力分別有：資訊安全管理、個資安全管理、第三方支付安全管理、合規安全管理、系統安全管理、事件回應管理、網路安全管理及數位鑑識管理。

(二)、 安全稽核組

安全稽核組是本公司資訊安全組織,負責維護資訊安全的有效性，其中包含了：控制環境、風險評估、控制作業、資訊溝通及監督，透過稽核以滿足法令法規及內部程序之遵循性要求。

(三)、 獨立的第三方驗證機構驗證：

本公司已取得第三方驗證機構之ISO 27001、ISO 20000、ISO 29100、BS 10012等國際驗證，我們的管理系統涵蓋資訊機房管理、SOC監控中心、各部門的資訊安全、技術服務管理與個資安全。

1. 什麼是ISO 27001？

ISO 27001是針對資訊安全管理系統的國際驗證規範，明確

定義資訊安全管理系統(ISMS)的需求標準，包含建立、實施、檢查、改進等層面。透過嚴謹、具有高度公信力的稽核單位，確保組織採用系統化的作業流程來管理組織內部及客戶個人資料的安全。

2. ISO 27001對本公司的意義

藉由導入ISO 27001資安管理機制，證明本公司經營團隊具有完善的資訊安全管理體系，其涵蓋範圍包括資訊安全政策、資訊安全組織、人力資源安全、資產管理、存取控制、密碼學、實體及環境安全、運作安全、通訊安全、系統獲取開發與維護、供應者關係、資訊安全事故管理、營運持續管理、遵循性等作業；透過健全的資安管理體系，除能有效對用戶資訊安全提供保障，也進階提升團隊競爭力，達到永續經營的目標。

三、人力資源安全[A7]

本公司對甄選及晉用之人員均會檢核與確認其所學、經歷及專業資格，負責重要業務活動前，會針對該項活動所需之技能、人員的資格、適任與否予以評估。

新進人員到職後，由財管部及相關部門實施新進人員訓練，使其了解本公司組織、管理規章及安全事項。

另有專責部門辦理定期或不定期之資訊安全教育訓練及宣導，促使所有人員瞭解資訊安全之重要性及各種可能的安全風險，並說明違反資訊安全規定時可能招致的處罰及法律責任，以提高本公司人員資訊安全意識，促其遵守資訊安全規定；如人員因工作職責須使用機敏性資訊或/及設施，需經過授權核准使用。

所有人員須依相關法令及本公司規範負保密責任，並簽訂保密切結書。

四、資產管理[A8]

本公司採取嚴謹的風險評鑑方法論進行預測，與風險處理，以確保資料資產安全。

每年均進行資產盤點活動，將資產類別、資產名稱、型號、說明、放置地點、數量、資產擁有者、風險管理者、資產管理者及資產使用者等項目納入並執行風險評鑑與風險處理。

五、存取控制[A9]

本公司採取嚴謹的控制措施避免未經授權的存取，以保護客戶和自身的資料資產安全。

權限控管與識別特殊權限是存取控制的基本原則，本公司每位員工皆擁有唯一的帳號和密碼，並依據其角色職責賦予最小化之權限。

如需特殊權限存取相關的資源，員工則須依據本公司的安全規定進行申請和核准。

六、密碼學[A10]

(一)、 使用密碼式控制措施之政策

藉由使用密碼控制措施，保護資訊的機密性、鑑別性或完整性，並建立適當的密碼管理措施。

(二)、 金鑰安全管理

1. 金鑰(含實體卡片及檔案形式)由金鑰保管人保管，並建冊管制且定時清查。
2. 實體卡片金鑰須存放於可上鎖之儲存櫃內，非授權人員不得取用；非經單位主管核可，不得攜出辦公處所。
3. 檔案形式金鑰存放目錄須設定權限管制，非授權人員不得存取、複製、刪除，金鑰保管人須至少備份一份並妥善保管。
4. 金鑰保管人離職或職務異動時，須辦理移交作業，並立即更新金鑰清冊。
5. 金鑰的申請/發放與註銷及失效金鑰之處理，依金鑰發行單位之相關作業規定辦理。

七、實體及環境安全[A11]

本公司採取嚴謹的實體控制措施避免未經授權的進出入，以保護資料資產安全。

(一)、 門禁管理

資訊機房之外牆使用結構堅固之材質，設有24小時運作之錄影監控設備，以維資訊機房之安全，並設有適當防護，如門禁系統、人員駐守等以避免未經授權之進入。

存放有敏感資訊之區域，皆加以管制，避免非相關人員隨意進出；來賓或訪客進資訊機房與辦公室，須有本公司同仁陪同。

本公司不定期對進入資訊機房人員登記情況進行查核，嚴格控制非授權人員進入資訊機房。

(二)、 環境控制

為避免因電源失效而導致設備毀損、資料遺失及服務中斷，建置不斷電系統以支持其持續運作;具有多重路線連接到電信服務提供廠商。

本公司之資訊機房採用空調系統以保障伺服器及其他設備能夠在恒溫的環境下運作，並對資訊機房的溫濕度進行監控。

資訊機房內配置有火災偵測及滅火設備，均符合消防法規，防止重要資訊硬體設備被損毀與破壞。

八、運作安全[A12]

為了維護本公司日常維運及相關活動安全，定期執行內部稽核及第三方稽核以確保營運安全。

本公司設有7X24小時之工程師負責隨時監控以維持資訊處理和通訊服務品質，由技術人員進行日常維護保養、巡檢並填寫維運日誌。

定期與關注方(如客戶)及產、官、學界等資訊安全先進進行安全評估或交流建議。

九、通訊安全[A13]

因應日漸擴大的各種外部攻擊，本公司採用階層式防護縱深的策略，僅允許被授權的服務和傳輸協定，確保未經授權的服務與傳輸。

本公司網路的資通訊安全防護由下列組成

(一)、 採用符合國際標準的防火牆及路由設備等，對網路進行區隔與隔離政策。

(二)、 防火牆策略的管理包括申請、核准、設定等變更管理及存取稽核。

(三)、 限制授權管理人員對重要網路設備的存取，及定期檢視存取紀錄。

(四)、 制定技術隔離措施和存取控制管理流程，對使用的各類網站和應用系統進行內部流量監控，並透過攻擊防護和入侵防護以達到安全的服務。

(五)、 自動化監控程式碼、應用系統、作業系統、資料庫等異常活動與非授權資料存取活動。

(六)、 定期執行弱點掃描分析，及時發現潛在風險並補強安全性弱點。

(七)、 區分資料安全的危害程度，及資訊資安事件類別和等級。

十、系統獲取開發與維護[A14]

本公司為符合資訊安全管理要求，建立系統與軟體開發、變更維護或軟體獲取之管理機制。

(一)、 SDLC (Software Development Life Cycle)

系統發展生命週期，指發展一套系統的順序，用以開發完善的資訊系統，以功能性為導向。主要可分為以下階段：

1. 需求分析(Requirement)
   著重需求定義，以符合業務內容及使用者需求為目的。

2. 架構設計(Design)
   根據需求分析結果，進行包含系統任務目標、功能關聯、邊界範圍、各階層使用者的角色等內外部使用的規劃。

3. 程式開發(Develop)
   依據分析及架構設計結果，發展符合使用者需求之操作介面、資料處理、功能運作等功能。

4. 系統測試(Test)
   進行運作模擬，檢驗系統完成度，確保各項功能皆可符合既定的需求。

5. 上線部署(Deploy)
進行系統之上線部署，確保過程中系統運作無誤，並安排教育訓練，使人員能正確操作系統之功能。

6. 運作與維護(Maintain)
確保穩定的系統服務之運作維持和更新。

(二)、 SSDLC (Security Software Development Life Cycle)
系統發展生命週期的資訊安全整合，除考量系統功能性的同時，導入安全性的思維，於系統整個開發過程，進行各項必要的資訊安全防護措施，以降低系統後續維護的成本，以及遭受到攻擊行為時的損失。

十一、 供應者關係[A15]

本公司與供應商訂有適當之資訊安全需求及服務相關契約，內容包含人員資格審查、保密切結書、履約期間之監控與服務交付事項等，以確保符合相關服務要求。

十二、 資訊安全事故管理[A16]

本公司建置了資安事件管理平臺(SOC資安監控中心)來管理相關資安事件，範圍涵蓋權責人員、事件與事故、處理進度及事後通告過程。當資安事件發生時，資安工程師依據紀錄和嚴重程度進行優先順序處理(直接影響客戶的資安事件將被賦予最高優先順序對待)，並於事件發生後透過數位鑑識來分析以防止事件再次發生。

十三、 營運持續管理[A17]

為降低事故對營運之影響，進行業務衝擊分析並建立相關計畫與模擬演練，並規劃具有高可用度的備援機制以符合控制規範。

十四、 遵循性[A18]

(一)、 本公司符合遵循政府之法律、法規與資訊安全需求相關之義務，其中包含智慧財產權與隱私及個人可識別資訊之保護。

(二)、 資訊系統及環境皆定期實施資訊安全檢查及稽核，以達成資訊安全政策目標、聲明及標準之要求。

(三)、 本公司與供應者均有簽署保密合約，並透過定期監控與審查方式，查核有關之資訊資安事件控制、錯誤追蹤與服務中斷、服務績效是否遵照雙方協議等相關紀錄。

肆、結語

本公司秉持著提供更安全便利的系統整合與全方位的專業顧問服務，依國際標準組織(ISO)、美國國家標準技術研究所（NIST）與美國資訊系統稽核與控制協會（Information Systems Audit and Control Association, ISACA）所訂定的安全標準，落實在資訊安全的架構、營運及治理之資料、網路及法規等風險管理。

最新之資訊安全白皮書請參閱 www.tsc-tech.com