資訊安全管理政策

HOYA BIT

文件編號:	ISM-1-001
資產等級:	內部使用
權責單位:	資安部
版次:	V1.0

文件修訂沿革

發行/修訂版次	發行/修訂生效日期	發行與變更說明	發行/修訂人員	核准人員
V1.0	2025/04/18	新版文件發行	資安部同仁	技術資訊處處長

目 錄

1. 目的

為強化資訊安全管理、確保資訊的機密性、完整性與可用性，免於因外在之威脅或內部人員不當之管理與使用，防止資訊被竊取、竄改、毀損、滅失、洩漏、不法利用或其他侵害等風險。特制訂資通安全政策(以下簡稱本政策)，以作為本公司資訊安全管理最高指導方針

2. 範圍

本政策適用範圍為『禾亞數位科技股份有限公司』(公司英文縮寫為HOYA BIT，以下簡稱本公司)管轄之資訊資產及使用資訊資產之相關人員，內容如下:

2.1 本公司所有員工、協力廠商、外包人力及其他得接觸本公司相關資訊者。

2.2 所有資料、文件與報告。

2.3 所有主機、伺服器、個人電腦、終端設備、通訊線路，以及與上述資訊設備相關或是與本公司資訊系統相連等之硬體設備資訊資產。

2.4 所有存放資訊設備之實體環境。

2.5 所有應用系統和資訊等之軟體資訊資產。

2.6 其他定義為本公司管轄範圍內之所有資訊資產，且包括其他雖可能未實際持有，但由於法律及法規所賦予之責任而可支配之資訊。

2.7 本公司位於他國之單位為符合當地法令要求，得另訂定相關作業管理規範。

3. 定義及說明

3.1 資訊(Information):包括以任何型態顯示及以任何媒體(含紙張)儲存之未經處理之原始資料、經處理過之資訊、轉換提昇後之知識等。資訊也是一種資產，就像一些重要的企業資產一樣，對組織而言是有價的，因此必須被適切的保護。

3.2 資訊資產(Information Asset):與資訊處理相關之資產皆屬之，包括硬體、軟體、資料、文件及人員等，皆視為資訊資產。

3.3 資訊安全(Information Security):目的在確保資訊的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)、私密性(Privacy)及合法性(Compliance)，使資訊能安全地(safely)、正確地(accurately)、適切地(adequately)及可靠地(reliably)被運用在達成本公司經營目標之規劃、執行、管理及相關作為上。

4. 角色權責單位

4.1 資訊安全工作小組:

審核資訊安全工作分組統籌資訊安全管理體系等事項。

4.2 資訊安全工作分組:

統籌資訊安全管理體系等事項之協調、規劃、查核及推動，由本公司單位主管選派召集人，成立資訊安全推動組織，並進行跨部之協調。

5. 資訊安全政策聲明

本公司秉持維護其作業環境之資訊安全及服務客戶之理念，除基本必要之資訊安全控管措施，更在於確保所有資料及處理過程均獲安全保障，本公司將強化資訊安全管理並持續提昇重要個人及交易資料等資訊之機密性、完整性及可用性，落實推動資訊安全管理作業，以提昇本公司之服務品質。本公司資訊安全聲明如下:

5.1 資訊安全管理體系應成立適當組織，執行資訊安全管理作業，確保本公司符合法令法規，並維持資訊安全管理體系維運之正常運作。

5.2 工作分派應考量職能分工，職務責任範圍應予區分，以避免資訊或服務遭未授權修改或誤用。

5.3 所有人員凡其使用本公司資訊以提供資訊服務或執行專案工作等，均有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。

5.4 所有人員有義務保護客戶資料，包含交易資料與基本資料，禁止未授權的情況下接觸、使用或是將該資訊揭露、告知予與業務無關之同仁、廠商及其它客戶。

5.5 應強化電腦資訊實體環境的安全保護，如管制區門禁、空調、不斷電設備等，避免資訊、資產遭未經授權存取、損害或意外災害，影響營運活動正常運作。

5.6 所有人員不得私自串接外部網路與本公司內部網路，應設置必要之安全設施以保護內外部網路。

5.7 系統維護管理應於初始階段考量安控機制之佈置，委外廠商管理部分應強化控管及合約之資訊安全要求，系統維護管理、修改及建置應符合並遵循資訊安全管理規範。

5.8 應建立威脅情報的收集、分析和處理流程，防止安全漏洞被利用、惡意软件和代码的入侵及未經授權的軟件和代碼安裝。

5.9 所有人員對於有發生安全事件、安全弱點及違反資訊安全管理體系實施規範與管理程序之虞者，應隨時保持警戒，並依程序進行通報。

5.10 應依業務需求訂定業務持續運作計畫，並定期測試演練，維持其適用性。

5.11 建立與權責機關和特殊關注群組之聯繫程序，包括指定聯絡人、記錄聯繫資訊、遵循法規要求、尊重隱私權、提供支持和協助、建立回饋機制、建立合作關係，並定期評估和改進相關政策和程序。資訊安全工作小組依據資訊安全政策及組織權責，擬訂資訊安全目標並由資訊安全工作小組審核後實施。

5.12 資訊安全目標應涵蓋機密性、完整性與可用性並呼應資訊安全政策要求產生之。

6. 資訊安全之組織管理與分工

6.1 為統籌資訊安全管理體系等事項之協調、規劃、查核及推動，應成立資訊安全工作小組，由本公司技術資訊處副總擔任工作小組代表/高階主管，協調資訊安全管理體系相關事宜，並向總經理進行報告。

6.2 資訊安全政策、計畫及技術規範之研議及建置等事項，由資訊安全工作小組交由權責部門負責辦理。

6.3 資訊安全查核政策及其計畫之研議事項，由稽核小組會同相關部門負責辦理。

7. 人員安全管理及教育訓練

7.1 負責重要資訊系統之管理、維護、設計及操作之人員，應妥適職務分工，並視需要建立制衡機制，建立人力備援制度。

7.2 人員離/調職時，應適時取消使用各項資訊資產之所有權限，並列入人員職務異動之必要手續。

7.3 定期辦理資訊安全教育訓練及宣導，促使員工瞭解資訊安全的重要性，以提高員工資訊安全意識，促其遵守資訊安全規定。

8. 資訊資產管理

8.1 本公司所有資訊資產係屬本公司擁有或依法擁有使用權，所有在本公司管轄範圍內之資訊系統設備及網路資源上所處理、儲存或傳輸交換之資訊均受本公司管理，應依行內規範進行存取、複製、刪除之作業。

8.2 本公司所有員工、協力廠商及其他得接觸本公司相關資訊者，凡其使用本公司資訊以提供資訊服務或執行專案工作等，均有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。確保資訊資產之機密性、完整性及可用性。

8.3 嚴禁使用來源不明之儲存媒體及非法之軟體程式。

8.4 電腦設備須裝置防毒軟體，並開啟即時掃瞄功能。

8.5 因業務所需提供網路資源分享時，須經申請並獲得適當授權許可。

8.6 本公司重要資料檔案內容之變更應有授權及覆核機制。同時考量應有適當之備份異地貯存作業。

8.7 應有適當的程序，以確保在使用智慧財產權方面的物品及他人專有的軟體產品時，能符合法律的限制。

9. 系統存取控制

9.1 遵循本公司訂定資訊系統存取控制規定，並以書面或其他電子方式記錄之;權責部門應訂定各應用系統存取控制管理程序，並明定使用本公司及使用人員的系統存取權利。

9.2 使用者之存取管理，應遵循使用者申請管理程序，包含管制系統存取特別權限、使用者密碼之管理制度及暫時不使用或無人看管的設備，適當的安全保護措施。

9.3 開放本公司以外的使用者從公眾網路，或從本公司網路以外的網路與本公司連線作業，建立遠端使用者身分鑑別機制，降低未經授權存取系統的風險;應避免允許維修廠商以遠端登入方式進入正式環境維修，否則應經審慎評估簽報資訊單位主管核可，並應加強安全控管，建立名冊，課其相關安全保密責任。

9.4 不同領域的網路系統，每一領域宜以特定的安全設施加以保護。

9.5 建立自動化的身份鑑別系統，以鑑別連上網路的使用者身份，以明責任歸屬;如有在例外的情況下，可為本公司的整體效益，經權責主管人員之同意，核發群組內人共用同一使用者識別碼，但應採取額外的安全控制措施，明確規範使用者的責任。

9.6 依資訊存取規定，配賦應用系統的使用者(包括應用系統支援人員)與業務需求相稱的資料存取及應用系統使用權限;另對應用系統原始程式資料之存取，建立安全控制機制。

9.7 應建立及製作資訊安全事件的稽核軌跡，並保存一段的時間，以作為日後調查及監督之用。

10. 密碼學

10.1 採用密碼式控制措施時，為達成不同資訊安全目標，可使用之密碼式控制措施範例如下:

10.1.1 機密性(confidentiality):使用資訊加密以保護機敏或關鍵資訊，於其儲存或傳輸時。

10.1.2 完整性/真確性(integrity/authenticity):使用數位簽章或訊息鑑別碼以查證所儲存或傳輸的機敏或關鍵資訊之真確性或完整性。

10.1.3 不可否認性(non-repudiation):使用密碼技術以提供事件或行動之發生或未發生的證據。

10.1.4 鑑別性(authentication):使用密碼技術以鑑別使用者及其他系統個體,當其請求對系統使用者、個體及資源之存取或與之交易時。

10.2 密碼金鑰生命週期之要求事項,包括產生、儲存、封存、檢索、分發、汰除及銷毀金鑰。

10.3 應依最佳實務選擇密碼演算法、金鑰長度及使用之實務作法。適切之金鑰管理必須具備供密碼金鑰之產生、儲存、封存、檢索、分發、汰除及銷毀所使用之安全過程。

11. 實體及環境安全

11.1 設備應安置在適當的地點並予保護,以減少環境不安全引發的危險及減少未經授權存取系統的機會。

11.2 應予保護電腦設備之設置,以防止斷電或其他電力不正常導致的傷害。

11.3 應妥善地維護設備,以確保設備的完整性及可用性。

11.4 含有儲存媒體的設備項目應在報廢前詳加檢查,以確保任何機密性的資料及軟體已經被移除。

11.5 實體環境的安全保護,應以事前劃定的各項周邊設施為基礎,並以設置必要的門禁措施,達成安全控管的目的;管制區內應有適當的進出管制保護措施,以確保只有被授權的人員始得進入。

11.6 資訊設施的實體保護程度,以及實體障礙設置的位置,得依資訊資產價值及安全的風險決定。

12. 電腦系統安全及資料、文件與媒體安全

12.1 遵循系統管理文件規定,並以書面或其他方式載明之,以確保員工正確及安全地操作及使用電腦,並以此作為系統維護、管理及測試作業的依據。

12.2 為降低因人為疏忽或故意,導致資料或系統遭不法或不當之使用,或遭未經授權的人員竄改,對本公司的資訊業務,應建立職務分工機制。

12.3 系統維護管理及測試作業可能會有變更軟體及共用電腦資源之情形，為降低可能的安全風險，應將系統維護管理及正式作業的設施分散，以減少作業軟體或資料遭意外竄改，或是遭未經授權的存取。

12.4 隨時注意及觀察系統的作業容量及網路容量使用狀況，以避免容量不足而導致電腦當機。

12.5 在維護管理重要的應用系統時，應確定系統的功能及確保系統的作業效能能夠滿足使用單位需求;新系統上線作業前，應執行適當的測試作業，以驗證系統功能符合既定的標準。

12.6 規劃資訊系統設備損害或電腦當機時，可維持本公司營運持續作業替代性的備援作業方法。

12.7 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，促使員工正確認知電腦病毒的威脅，提升員工的資訊安全警覺，健全系統存取控制機制。

12.8 應準備適當及足夠的備援設施，定期執行必要的資料及軟體備份與備援作業，以便發生災害或是儲存媒體失效時，可適時回復正常作業。

12.9 針對攜帶及移動的儲存媒體，建立使用管理程序，規範磁帶、磁碟等媒體之使用。

12.10 針對單位內使用之文件，應建立適當管控。

12.11 儲存機密性及敏感性資料的資訊媒體，當不再使用時，應以安全抹除或其他合宜之報廢方式處理。

12.12 應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。重要的資料檔案應依相關規定，以安全的方式保存;超過規定保存時限的檔案，可依相關規定刪除或銷毀，惟應事前考量是否對本公司造成不利的影響。

12.13 外部與本公司間進行資料交換，需訂定正式的協議，將機密性及敏感性資料的安全保護事項及責任列入協議。

12.14 電腦媒體運送及傳輸過程，應有妥善的安全措施，以防止資料遭破壞、誤用或未經授權的取用。

13. 網路安全

13.1 遵循電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取;如利用公眾網路傳送敏感性資訊，應採取特別的安全保護措施，以保護資料在公共網路傳輸的完整性及機密性，並保護連線作業系統之可用性。

13.2 本公司與外界網路連接的網點，應加裝防火牆，以控管外界與本公司內部網路之間的資料傳輸與資源存取。

13.3 對外開放的資訊系統，以防火牆與本公司內部網路區隔，提高內部網路的安全性。

13.4 依據電子郵件的安全管理機制，以降低電子郵件可能帶來的業務上及安全上的風險。

13.5 為維持本公司網路的持續正常運作，各重要網路設備宜有備援。

13.6 本公司網路如有被入侵或有疑似被侵入情形，依訂定的處理程序，採取必要的行動。

14. 應用系統維護管理安全

14.1 資訊系統規劃之需求分析階段，即將安全需求納入;新維護管理的資訊系統，或是現有系統功能之強化，依據資訊安全需求，將安全需求納入系統功能。

14.2 除由系統自動執行的安控措施之外，亦可考量由人工執行的安控措施;若採購套裝軟體時，亦須進行相同的安全需求分析。

14.3 系統內部的作業，應建立驗證資料正確性的作業程序，避免正確輸入資料到應用系統中，卻因系統處理錯誤或是人為因素而遭受破壞。

14.4 系統內部作業是否採取特別的資料處理控制程序，應視應用系統的性質及資料遭破壞，對本公司業務的影響程度而定。

14.5 對機密性的資料，宜在傳輸過程中以加密方法保護。

14.6 宜保護及控制測試資料，避免以含有個人資料的真實資料庫進行測試;如須應用真實的資料，儘可能事前將足以辨識個人的資料去除或轉換。

14.7 建立正式的變更控制程序，以降低可能的安全風險;任何的系統變更作業，皆應獲得權責主管人員的同意。

14.8 作業系統應定期更新(如安裝新的版本);作業系統變更時，應審查其對應用系統是否造成負面的影響，或是產生安全上的問題。

15. 資訊作業事故之反應及處理

15.1 遵循本公司處理資訊作業事故之作業程序，並賦予相關人員責任，以便迅速有效處理本公司資訊作業事故。

15.2 如發現或懷疑有資訊安全類之事故時(包括系統有安全漏洞、受威脅、系統弱點及功能不正常事件等)，應依訂定的通報管道，迅速通報權責主管及窗口立即處理。

16. 委外作業管理

16.1 委託廠商建置及維護重要軟硬體設施時，應由保管人員或受託者監督及陪同下始得為之。

17. 業務持續營運管理

17.1 為避免因各種人為及天然災害造成資訊業務運作受影響，須針對系統救援回復及定期備份制定適當之計畫並由應用系統負責人落實執行。

17.2 應定期演練並測試資訊安全持續性之過程、程序及控制措施之功能性，以確保其與資訊安全持續目標一致。

18. 遵循性

18.1 應對每個資訊系統及組織，宜明確識別、以文件記錄及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

18.2 應確保遵循與智慧財產權及專屬軟體產品使用相關之法律、法令、法規及契約的要求事項。

18.3 應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布

18.4 應依適用之相關法令、法規中之要求，確保隱私及個人可識別資訊之保護。

18.5 所採用之密碼式控制措施，應遵循所有相關協議、法律及法規。

18.6 應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全之作法及其實作(亦即資訊安全之各項控制目標、控制措施、政策、過程及程序)。

18.7 應以適切之安全政策、標準及所有其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。

19. 其它

19.1 為達成上述政策，本公司制定政策落實之衡量指標，資訊安全政策目標與衡量指標彙整於「ISM-1-001-F01-資安管理目標量測表」

19.2 本政策如有未盡事宜，悉依相關法令及本公司相關規定辦理。

19.3 本政策奉核定後實施，修訂時亦同。

20. 表單**/**附件

20.1 ISM-1-001-F01-資安管理目標量測表