延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-25	保存年限：2 年
日期：114年 08月 01日	紀錄編號：YAN-ISMS-G-25-11408-01	版本：2.0

派駐人員資訊安全守則

1 目的：

為落實延宇資訊股份有限公司（以下簡稱本公司）及顧客之資訊通訊安全作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。

2 範圍：本守則適用於派駐之正職人員與臨時人員。

3 基本要求：

3.1 電腦應設定密碼確實保密。

3.2 電腦應設定螢幕保護程式（10 分鐘）並設定密碼保護。

3.3 電腦之作業系統漏洞應即時更新修補。

3.4 電腦應安裝公司或顧客選用之防毒軟體並即時更新病毒碼。

3.5 應定期將重要資料備份存放。

3.6 使用通行密碼應注意下列要點：

3.6.1 應保護通行密碼，維持通行密碼的機密性；

3.6.1.1 資訊系統之管理者應至少每 3 個月更換通行密碼一次，並禁止重複使用相同的密碼。

3.6.1.2 系統一般使用者應至少每 3 個月更換通行密碼一次，並禁止重複使用相同的密碼。

3.6.2 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

3.6.3 當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。

3.6.4 通行密碼的長度最少應有 8 位長度以上，且需有數字、特殊符號、英文共同組成之密碼。

3.6.5 密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：

3.6.5.1 個人姓名、出生年月日、身分證字號。

3.6.5.2 公司或單位名稱識別代碼或是其他相關事項。

3.6.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

3.6.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

3.6.5.5 電話號碼。

3.6.5.6 英文或是其他外文字典的字彙。

3.6.5.7 專有名詞。

3.6.5.8 空白。

3.7 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

3.8 除公司及顧客核定同意外，任何人不得在任何公開的新聞群組、論壇、或公布欄中透露任何有關本公司資訊細節。

3.9 在丟棄任何曾經儲存本公司資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀或實體破壞至無法解讀之程度。

3.10 限閱等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。

3.11 重要機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼或採用其他保密措施。

3.12 開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。

3.13 當有跡象顯示系統可能中毒時，應儘速通知相關人員。

3.14 禁止濫用系統及網路資源，複製與下載非法軟體。

3.15 電腦軟體版權之使用與管理

3.15.1 經由公司採購流程所取得之合法軟體，始可於公司內部使用。

3.15.2 本公司所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

3.15.3 除公務使用外及未經公司主管級以上主管或顧客權責單位同意，不可複製公司及顧客之內部之軟體、文件資料至公司或顧客指定以外之場所使用或販賣。

3.15.4 軟體之重製應以符合該軟體授權合約書之條約內容為基準，且需單位主管同意；不得為任何合約書規定以外的拷貝、複製行為。

3.15.5 不可複製非經公司及顧客採購的非法軟體（含共享軟體）到公司安裝使用。若為測試軟體應經單位主管同意始可使用。超過測試（試用）期間應予移除。

3.15.6 應確定電腦內軟體具有合法版權後再行使用，以維護個人的權益；如發現公司及顧客內有任何不法使用之軟體及相關文件，應即告知管理單位，並由資訊人員協助處理。

3.15.7 任何私人可攜式媒體（NB、隨身碟、SD 卡..）上的程式或資料，造成公司及顧客內部電腦設備有所損害或中毒或破壞電腦資料，則需負擔起賠償責任。

3.15.8 個人因職務所獲得公司及顧客內部系統的帳號、密碼（如進防

火牆、伺服器、銷存系統、E-mail 帳號…等）皆屬顧客或公司資產應妥善保管，不得公開（或與其他人共用）。

3.15.9　不試圖入侵（hacking）公司及顧客任何電腦系統（個人有意或無意使用他人帳號、密碼亦屬入侵行為）。

3.15.10　本公司人員若有安裝軟體需求時，需填寫「設備異動申請單」，經權責主管以上核准後，始得執行安裝。

4　除第三項基本要求外，如派駐之機關（單位）之資訊安全相關要求與本手冊有不同時，必須依較嚴格之要求為遵循。

5　顧客之相關資訊如需與公司資料交換時，應採取適當之保護措施，如墊子資訊應加密後傳遞、書面資料須彌封後親自送交公司或採掛號、快遞寄回公司等作為。

6　應遵守「個人資料保護法」規範，保護個人資料使用之合法性及機密性。

7　保密協定

7.1　本公司人員應填具「派駐人員保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密（包含客戶提供之個資），非經主管授權不得對外透露或加以濫用。

8　本公司員工及臨時人員若未遵守上述規定或資訊安全政策及程序者，得呈報管理部，依本公司相關懲戒程序處置違紀人員。

本守則由資訊安全委員會核准後公告實施，修訂時亦同。

謝孟勳 2025/8/1

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-25	保存年限：2 年
日期：115 年 1 月 5 日	紀錄編號：YAN-ISMS-G-25-1150l-01	版本：2.0

派駐人員資訊安全守則

1 目的：

為落實延宇資訊股份有限公司（以下簡稱本公司）及顧客之資訊通訊安全作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。

2 範圍：本守則適用於派駐之正職人員與臨時人員。

3 基本要求：

3.1 電腦應設定密碼確實保密。

3.2 電腦應設定螢幕保護程式（10 分鐘）並設定密碼保護。

3.3 電腦之作業系統漏洞應即時更新修補。

3.4 電腦應安裝公司或顧客選用之防毒軟體並即時更新病毒碼。

3.5 應定期將重要資料備份存放。

3.6 使用通行密碼應注意下列要點：

3.6.1 應保護通行密碼，維持通行密碼的機密性；

3.6.1.1 資訊系統之管理者應至少每 3 個月更換通行密碼一次，並禁止重複使用相同的密碼。

3.6.1.2 系統一般使用者應至少每 3 個月更換通行密碼一次，並禁止重複使用相同的密碼。

3.6.2 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

3.6.3 當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。

3.6.4 通行密碼的長度最少應有 8 位長度以上，且需有數字、特殊符號、英文共同組成之密碼。

3.6.5 密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：

3.6.5.1 個人姓名、出生年月日、身分證字號。

3.6.5.2 公司或單位名稱識別代碼或是其他相關事項。

3.6.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

3.6.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

3.6.5.5 電話號碼。

3.6.5.6 英文或是其他外文字典的字彙。

3.6.5.7 專有名詞。

3.6.5.8 空白。

3.7 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

3.8 除公司及顧客核定同意外，任何人不得在任何公開的新聞群組、論壇、或公布欄中透露任何有關本公司資訊細節。

3.9 在丟棄任何曾經儲存本公司資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀或實體破壞至無法解讀之程度。

3.10 限閱等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。

3.11 重要機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼或採用其他保密措施。

3.12 開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。

3.13 當有跡象顯示系統可能中毒時，應儘速通知相關人員。

3.14 禁止濫用系統及網路資源，複製與下載非法軟體。

3.15 電腦軟體版權之使用與管理

3.15.1 經由公司採購流程所取得之合法軟體，始可於公司內部使用。

3.15.2 本公司所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

3.15.3 除公務使用外及未經公司主管級以上主管或顧客權責單位同意，不可複製公司及顧客之內部之軟體、文件資料至公司或顧客指定以外之場所使用或販賣。

3.15.4 軟體之重製應以符合該軟體授權合約書之條約內容為基準，且需單位主管同意；不得為任何合約書規定以外的拷貝、複製行為。

3.15.5 不可複製非經公司及顧客採購的非法軟體（含共享軟體）到公司安裝使用。若為測試軟體應經單位主管同意始可使用。超過測試（試用）期間應予移除。

3.15.6 應確定電腦內軟體具有合法版權後再行使用，以維護個人的權益；如發現公司及顧客內有任何不法使用之軟體及相關文件，應即告知管理單位，並由資訊人員協助處理。

3.15.7 任何私人可攜式媒體（NB、隨身碟、SD 卡..）上的程式或資料，造成公司及顧客內部電腦設備有所損害或中毒或破壞電腦資料，則需負擔起賠償責任。

3.15.8 個人因職務所獲得公司及顧客內部系統的帳號、密碼（如進防

火牆、伺服器、銷存系統、E-mail 帳號…等）皆屬顧客或公司資產應妥善保管，不得公開（或與其他人共用）。

3.15.9 不試圖入侵（hacking）公司及顧客任何電腦系統（個人有意或無意使用他人帳號、密碼亦屬入侵行為）。

3.15.10 本公司人員若有安裝軟體需求時，需填寫「設備異動申請單」，經權責主管以上核准後，始得執行安裝。

4 除第三項基本要求外，如派駐之機關（單位）之資訊安全相關要求與本手冊有不同時，必須依較嚴格之要求為遵循。

5 顧客之相關資訊如需與公司資料交換時，應採取適當之保護措施，如墊子資訊應加密後傳遞、書面資料須彌封後親自送交公司或採掛號、快遞寄回公司等作為。

6 應遵守「個人資料保護法」規範，保護個人資料使用之合法性及機密性。

7 保密協定

7.1 本公司人員應填具「派駐人員保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密（包含客戶提供之個資），非經主管授權不得對外透露或加以濫用。

8 本公司員工及臨時人員若未遵守上述規定或資訊安全政策及程序者，得呈報管理部，依本公司相關懲戒程序處置違紀人員。

本守則由資訊安全委員會核准後公告實施，修訂時亦同。

劉紀明