YAN-ISMS-03-02

網路及系統安全管理說明書

_V2.2_20230804

延宇資訊股份有限公司

「資訊安全暨隱私資訊管理系統」

網路及系統安全管理說明書

機密等級: 一般

編號: YAN-ISMS-03-02

版本編號: 2.2

修定日期: 2023/08/04

使用本文件前 ，如對版本有疑問 ，請與修訂者確認最新版次。

文件編號: **YAN-ISMS-03-02**

機密等級: ¢一般 £限閱 £密 £機密

本文件歷次變更紀錄:

版次	修訂日	修訂者	說明	核准者
1.0	2020/01/31	梁維志	新增	楊文欽
1.1	2020/04/23	梁維志	因外部稽核建議事項，修訂 5.1.1.3 / 5.2.3.3	楊文欽
2.0	2021/11/08	梁維志	因應導入 ISO 27701，修訂相關規範。	楊文欽

2.1	2023/03/01	梁維志	因應 ISO 27001:2022 改版，新增 Ch5.4 網頁過濾、Ch5.5 監視活動管理程序 規範。	楊文欽
2.2	2023/08/04	梁維志	因應外部稽核發現點，修訂 Ch5.6遠端存取。	楊文欽

本程序書由 資訊安全執行小組（個人資料保護推動執行小組） 負責維護。

本資料為延宇資訊股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

目錄:

1 目的

2 適用範圍

3 權責

4 名詞定義

5 作業說明

6 相關文件

1 □□

1.1
□□□

5 作業說明

5.1 使用者作業規範:

5.1.1 系統組態及作業變更控制

5.1.1.1 軟體變更: 公司內列管使用者能在電腦上執行的軟體之清單 (軟體使用清單)

。同樣地，使用者亦不得允許軟體自動安裝程式於公司內的電腦上執行。有特殊需求者，可事先請求資安長報告，除此之外，使用者不得在電腦上安裝其他的軟體套件。

5.1.1.2

作業系統變更: 使用者不得變更由公司內所提供之電腦硬體上的作業系統、系統組態設定值、升級既有的作業系統、或者安裝新的作業系統。

5.1.1.3 如果有必要變更以上各項設定，則需由資訊執行小組:

5.1.1.3.1 親自於實體機上變更設定。

5.1.1.3.2 如須以遠端操作方式處理，須依照「 YAN-ISMS-02-08 存取控制管理程序書」之 5.7遠端存取之限制規範辦理。

5.1.1.4

使用者須隨時檢查作業系統漏洞修補通知，或於系統自動更新通知啟動時立即進行系統修補作業。

5.1.2 硬體控制

5.1.2.1

硬體變更: 由公司內所提供的電腦硬體設備不得以任何方式加以變更，若因業務上之考量，得事先取得部門主管簽核，再送交資訊安全執行小組檢視其硬體變更需求。

5.1.3 存取控制

5.1.3.1 □□□□

5.1.4.4

□□□

5.2.2 □□□□

5.2.2.1

□□□

5.3.1 網路管理規範

5.3.1.1

資訊安全執行小組為本公司網路之管理單位，負責制訂各項網路管理及使用規範，並依規範之要求有效管制本公司網路之使用。

5.3.1.2

本公司人員若因業務需求攜帶非本公司採購之個人電腦或筆記型電腦進入公司內，並使用本公司網路服務，須填寫「YAN-ISMS-04-35網路連線申請表」，說明使用單位、網路卡號（MAC Address）等資訊，經資訊安全執行小組登記核准後始可使用本公司網路服務。

5.3.1.3

經過授權的網路使用者必須依本公司網路使用規範使用網路服務，違反使用規範者得依相關之懲戒規定處理。

5.3.1.4

本公司人員因業務需求，皆需使用網際網路相關服務，無需額外申請。

5.3.1.5 資訊安全執行小組依以下規定管理本公司網路:

5.3.1.5.1 使用 DHCP Server

將授權使用網際網路之使用者電腦配賦一指定IP，並隨時監看IP使用情形。

5.3.1.5.2 P2P點對點傳輸軟體(如: foxy...)禁止使用。

5.3.1.5.3

來賓僅限使用專用之無線路由器連接外部網路，除資安長同意外，禁止使用公司內部網路及相關設備。

5.3.2

網路使用規範: 取得本公司網路使用權之人員，必須依下列規範使用網路服務:

5.3.2.1

5.3.2.1.1

5.3.2.1.2

5.3.2.1.3

5.3.2.1.4 BBS

5.3.2.1.5

5.3.2.1.6

5.3.2.2

5.3.2.2.1

5.3.2.2.2

5.3.2.2.3

5.3.2.2.4

5.3.2.2.5

5.3.2.2.6

(BBS)

或類似功能之方法散布詐欺、毀謗、侮辱、猥褻、非法軟體交易或其他違法之訊息。

5.3.2.2.7

利用本公司之網路資源從事與業務無關之活動或違法行為。

5.4 網頁（外網）過濾管理程序:

本公司應降低人員造訪非法資訊、含病毒或釣魚網站之風險:

5.4.1 本公司應確定人員不該造訪及接觸的網站類型如下:

5.4.1.1 具有資訊上傳功能的網站，除非有正當理由且被核准。

5.4.1.2

已知或可疑的惡意網站（例如：發送惡意軟體或網路釣魚內容之網站）。

5.4.1.3 從威脅情資中獲取的惡意網站。

5.4.1.4 提供非法內容的網站。

5.4.2 本公司應識別惡意外部網站，並記錄於「惡意網站清單」。於清單內之網站，應使用防火牆之設定，阻止本公司同仁進行存取。 YAN-ISMS-04-56

5.5 監視活動管理程序

本公司應根據營運、資訊安全要求及相關法規之考量，來決定監控範圍及監控等級，並在所規範的保存時間內予以維護監視影像及記錄，所需考量之監視事項如下:

5.5.1

本公司透過網路防火牆監控網路進出及應用系統之通行，並產生流量記錄，該項記錄由資訊單位每年檢視，並記錄於「60防火牆政策檢視記錄單」。 YAN-ISMS-04-

5.5.2 □□□□

6.2 YAN-ISMS-04-34電腦操作帳號申請表

6.3 YAN-ISMS-04-35網路連線申請表

6.4 YAN-ISMS-04-36外對內連線服務申請表

6.5 YAN-ISMS-04-37系統使用權限管理名冊

6.6 YAN-ISMS-04-38權限帳號檢視申請紀錄單

6.7 YAN-ISMS-04-50網路架構圖。

6.8 YAN-ISMS-04-56惡意網站清單

6.9 YAN-ISMS-04-59日誌審查檢視表

6.10 YAN-ISMS-04-60防火牆政策檢視記錄單

Revision #2
Created 2026-06-14 07:54:48 UTC by Yantech
Updated 2026-06-14 08:10:28 UTC by Yantech