FARADAY

供應商資訊安全管理規範

REVISION HISTORY

Document title

Date	Rev.	Revised item

目錄 TABLE OF CONTENTS

1 目的
Purpose

根據內部供應商管理程序，建立本公司供應商資訊安全管理之指導原則，以有效控制供應商所帶來的資訊安全風險，並強化供應鏈資安規範。

2 範圍
Scope

本公司所有供應商。

3 組織與權責
Organization and Responsibility

3.1 委外人員及供應商

3.1.1 應遵守合約要求及雙方協議規定，並簽訂保密協議，確保本公司資訊資產之機密性、完整性及可用性。

3.1.2 委外人員從事與本公司相關作業時，需遵守本公司資訊安全政策及資訊安全相關規定。

4 解釋名詞
Definition

N/A

5 作業重點
Operation Instruction

5.1 定義並溝通資安政策與規範

5.1.1 人員進入管制區與申請設備接入內網規範

5.1.1.1 供應商欲進出管制區域時，應遵守內部門禁相關管理辦法，並根據辦法填寫相關表單。

5.1.1.2 供應商欲進入 8F 機房，應填寫門口所放置的「電腦機房(非授權人員)進出紀錄表」，並完成閱讀「資訊廠商進管制區域須知」; 於廠商離開 8F 機房前，應正確填寫時間並由授權陪同人員確認簽名。

5.1.1.3 供應商欲攜帶非公司設備進入本公司網域或內部網路環境時，應事先填寫「攜帶式設備入場申請表」及「攜帶式設備入場檢核表」， 完成簽核後方能將設備接入本公司內部網路環境，以避免病毒造成損害。

5.1.2 供應商帳號申請及使用規範

5.1.2.1 供應商若欲使用本公司內部系統，應填寫「PAS Service Application Form」，完成簽核後取得一組供應商帳號及相對應權限。

5.1.2.2 供應商帳號僅使用於職務需求相關範圍，不應越權使用。

5.1.2.3 供應商使用內部帳號所接觸之公司資料，應盡資料保護之責，其他規範請詳 5.1.3 資料保護。

5.1.2.4 供應商帳號應遵守本公司訂定之密碼原則，並配合定期執行密碼修改。

5.1.3 資料保護

5.1.3.1 於資料交換前應完成簽署 NDA，並遵守資訊安全條款；NDA 版本應遵循法務部門所發布之最新版本。

5.1.3.2 為避免病毒透過檔案傳送方式傳播，透過電子郵件或其他形式傳送檔案至本公司，必須遵守以下幾項規範：

5.1.3.2.1傳送之檔案不可含有病毒或惡意軟體（FTP, Web Upload, E-Mail…）

5.1.3.2.2傳送之檔案不可壓縮分割或加密（避免掃毒軟體無法正常偵測病毒）

5.1.3.2.3若無法透過電子郵件或 MFT（Secure FTP）方式傳送，應遵循 5.1.1 人員進入管制區與申請設備接入內網規範

5.1.3.2.4機密資訊在傳輸過程中要啟用加密機制（E-Mail<TLS>, MFT<Secure FTP>）

5.1.3.3 供應商若需上傳本公司相關檔案至公司外部，應遵循 NDA 相關規範，確保無資料外洩之風險。

5.1.3.4 供應商若有採用雲端服務，需上傳本公司相關檔案至雲端系統時，應注意此雲端服務是否提供對應之存取控制與資料保護方法，確保無資料外洩之風險，若無法判斷，請洽電子服務部相關人員協助評估。

5.1.3.5 若供應商上傳本公司相關檔案至公開之雲端服務，導致重要資訊外洩，此行為將會違反供應商對本公司之保密義務；如有供應商違反保密協議造成損失，本公司有權在法律允許範圍內，向供應商提出求償。

5.1.4 合格供應商資安合規審核

5.1.4.1 合格供應商應遵循本規範及 NDA 相關規範。

5.1.4.2 定期配合本公司執行資訊安全稽核，應遵循 5.4.2 資安合規性檢查與稽核。

5.2 資訊安全宣導

5.2.1 供應商於合作開始時，由本公司陪同人員協助宣導此規範內容。

5.2.2 因 NDA 為企業間之合約條款，為確保每位接觸本公司資訊之供應商人員皆熟知本公司供應商規範，應於每位人員首次合作時進行此規範之宣導。

5.3 全球資安風險通報與管理

5.3.1 資安威脅告警與建議改善措施

5.3.1.1 供應商應有偵測威脅機制，並針對高風險之資安威脅及告警，應盡快完成修補。

5.3.1.2 本公司若有發現相關威脅，通報給供應商，供應商應至少針對專案範圍完成修補，並回報給本公司。

5.3.2 資安情資蒐集

5.3.2.1 供應商應定期執行情資蒐集，並針對所蒐集之情資檢視供應商環境中是否有相對應之情境，若有較嚴重之情事，應盡快完成改善，以避免影響本公司環境。

5.3.2.2 宜參加資安研討會了解新型攻擊手法及情資，並分享所蒐集之威脅情資。

5.3.3 供應商資安事件處理及追蹤

5.3.3.1 供應商應訂定資安事件通報、處理及追蹤之程序，並定期演練緊急通報流程。

5.3.3.2 緊急通報流程應包含通報本公司之流程，並配合公司所需資訊進一步提供。

5.3.3.3 資訊安全事故發生或知悉有發生之虞後 24 小時內針對本專案服務範圍內之資訊安全事故向本公司回報處理狀況，並協助本公司進行後續處理。

5.4 供應商資安評鑑與改善

5.4.1 資安自我評鑑問卷

5.4.1.1 供應商應配合填寫本公司定期發出之資訊安全評鑑問卷，應如實回答，避免簡答，盡可能描述現況。

5.4.1.2 若本公司檢視問卷後須請供應商提出進一步佐證資訊，供應商應配合本公司需求。

5.4.2 資安合規性檢查與稽核

5.4.2.1 本公司針對合格供應商每年會執行一次資訊安全稽核，供應商應配合本公司安排時間與窗口完成執行。

5.4.2.2 於稽核結束後，供應商應針對建議事項回覆預計改善措施及預計完成改善時間，並於完成改善後告知本公司相關稽核人員再確認。

5.4.2.3 供應商收到本公司寄發之資安問卷，應遵循 5.4.1 資安自我評鑑問卷之規範。

6 參考文件
References

6.1 N/A

7 附件
Attachments

7.1 電腦機房(非授權人員)進出紀錄表

7.2 攜帶式設備入場申請表

7.3 攜帶式設備入場檢核表

電腦機房(非授權人員)進出紀錄表

FARADAY

電腦機房(非授權人員) 進出紀錄表

廠商名稱	人員姓名	進入原因	進入機房		離開機房		陪同人員簽名	完成閱讀廠商須知
			日期(年/月/日)	時間(時:分)	日期(年/月/日)	時間(時:分)		
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐
								☐

攜帶式設備入場申請表

FARADAY

攜帶式設備入場申請表

申請人填寫			
Applicant Information			
*申請人姓名：	*申請人工號：	*申請日期：	
*部門：	*分機號碼：	*使用起始日：	*使用到期日：
查檢項目(請確實勾選及填寫下列內容，以利主管審核您的申請)			
(1)廠商 ：			
(2)您申請攜入設備資訊：	設備品牌/型號:_____ 顏色: _____ MAC address: _____		
(3)申請理由及目的:(必填,請詳述目的)			
[注意事項] 1. 自行攜帶設備內所安裝軟體需具合法性，若有非法，需自行承擔相關法律責任。			
申請單位主管審核及評估建議 (注意：開放設備攜入使用都有資料外漏風險，請審慎評估)			
直屬主管:☐ 核准 ☐ 駁回	部門主管: ☐ 核准 ☐ 駁回	AVP 主管: ☐ 核准 ☐ 駁回	
(評估建議說明) (簽名/日期)_____	(簽名/日期) _____	(簽名/日期)_____	

資料保密同意條約

本人申請私有設備攜入公司使用，同意接受公司對攜入設備進行調整(防毒軟體檢查及安裝及資訊安全 Policy 控管等)。並且嚴格遵守公司保密安全規定，任何公司資料不得私自攜出或透過任何方式傳遞出公司外，一經查獲則依法處理並負擔相關法律責任，本人不得有任何異議。

廠商簽名:_____ 日期:_____

攜入設備 ES 安全性檢查

☐ 安裝防毒軟體並完成 full scan 後無安全疑慮。
☐ 廠商提供其他安全性檢查，並由資安人員檢查後核准。

資安人員簽名:_____ 日期:_____

執行檢查

☐ 申請資訊填寫完整並已完成簽核
☐ 完成 Mac 設定

網管人員簽名:_____ 日期:_____

移除設定

☐ 完成使用後，移除 Mac 值；若有安裝防毒軟體需提醒資安人員一併移除。

網管人員簽名:_____ 日期:_____

攜帶式設備入場檢核表

FARADAY	攜帶式設備入場檢核表
公司名稱 : company name:	
攜帶設備人員: Carrying equipment personnel:	
進廠時間: Into the factory time:	

	檢查項目	佐證畫面	佐證資訊說明	檢查結果說明
1	是否安裝防毒軟體 Antivirus software			
2	防毒軟體病毒碼最後更新日期 Virus version and last update			
3	Windows Update 是否為1個月內 Windows Update within 1 month			
4	7天內掃毒記錄 7 day Antivirus scan log			
5	USB及網路孔是否已貼上智原資安封條貼紙 USB and connector been affixed with a Faraday security seal sticker			