檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
1	基本規範(作業系統面)	二、(一)	不得以擁有系統管理者權限之帳號登入進行業務操作，並不得共用帳號密碼。	1.A.請代檢廠說明並展示作業系統上有哪些帳號具有系統管理者權限(administrators)，又有無使用該帳號登入作業系統進行業務操作之情形。 1.B.請代檢廠提供現行作業系統使用者帳號清單(包含帳號、使用人)，檢查作業人員有無共用帳號登入作業系統進行業務操作之情形。			
2		二、(一)	開啟密碼複雜度原則(設置 8 碼以上英數字混雜之密碼，3 個月更換密碼 1 次)。	2.A.請代檢廠說明並展示作業系統有無開啟密碼複雜度設定，又複雜度原則是否符合要求。 2.B.如前項檢查結果為無，檢查作業系統帳號之密碼是否符合複雜度要求，且每 3 個月更換 1 次。			
3		二、(二)	僅保留必要之使用者帳號，移除閒置帳號，停用 guest 帳號並修改 administrator 名稱。	3.A.請代檢廠展示作業系統帳號，並說明管理方式。 3.B.檢查帳號有無閒置不用或擁有人非現職人員情形。 3.C.檢查作業系統上 guest 帳號是否停用。 3.D.檢查作業系統上 administrator 帳號名稱是否修改或停用。			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
4	系統規範	三、(一)	作業系統、軟體之安全性更新與防毒軟體之重大更新或漏洞修補，應定期或盡速更新，並設定每月定期全機掃描檢查乙次。	4.A.請代檢廠說明並展示作業系統之安全性更新情形，檢查是否於發佈後 30 日內完成。 4.B.檢查防毒軟體、病毒碼之更新是否於發佈後立即完成。 4.C.檢查全機防毒掃描是否至少每月執行一次。（防毒軟體之快速或完整全機掃描，均為本項所指全機掃描） ※有關所使用軟體及作業系統相關產品之安全性更新，可於 NIST 網站弱點資料庫（https://nvd.nist.gov/）> search > Products-CPE 搜尋，以取得最新資訊。			
5		三、(二)	M3 作業電腦應專機專用，不得與其他非車輛檢驗業務共用。	5.A.請代檢廠展示電腦連線或使用紀錄，包含防火牆之網路連線進出紀錄、瀏覽器上網紀錄、項目 14 安裝軟體清單等。 5.B.檢查前述連線及使用紀錄是否逾越車輛檢驗業務需要。 5.C.如前項有逾越之虞，應請代檢廠說明該電腦連線或使用與檢驗業務之相關性，以釐清該電腦有無不當共用情形。			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
6		三、(二)	系統時間需每月與國家標準時間進行校正乙次。	6.A.檢查電腦系統時間是否正確。(可對照手機時間判斷) 6.B.請代檢廠說明並展示系統時間更新方式。 6.C.如為人工手動更新者，檢查每月有無至少校正 1 次之紀錄(任何形式均可)。			
7	網路規範	四、(一)	因緊急維護或其他不可抗力需求，方得以加密遠端連線存取特定之通訊埠(不得使用預設通訊埠)，作業結束後應完全中斷連線並關閉遠端服務。	7.A.請代檢廠說明並展示所使用之遠端連線軟體及連結方式為何。 7.B.如遠端連線軟體連結方式係他方端點直接連結我方端點者，檢查是否變更預設通訊埠。(以第三方中繼服務站方式進行遠端連結之連線工具，應禁止使用) 7.C.檢查遠端連線軟體連線情形，是否於每次維護作業結束後，中斷連線並關閉服務。			
8		四、(二)	檢驗線系統之網路需有基本防護，如防火牆(包含專用防火牆、具管理功能之 IP 分享器及網路提供具防護網路)需關閉未使用的連接埠。	8.A.檢查檢驗線電腦網路是否具備基本網路防護措施，又防護措施為何。 (如採用閘道式防火牆，可不需另行安裝主機式防火牆；否則，每台主機均應安裝主機式防火牆) 8.B.如前述防護措施為防火牆，其採用本地閘道式或主機式防火牆軟硬體，或採電信業者提供之防火牆服務，均屬本項所稱網路基本防護措施。			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
				(提供頻寬分享用途之 IP 分享設備，如不具備限制連出連入 IP、埠號管制之功能，不屬於本項所說網路基本防護措施。) 8.C. 如前述網路防護措施為實體防火牆，檢查是否關閉未使用的連接埠。 8.D. 依籌設須知裝設 VPN 數據線路者，屬符合規範；其餘數據線路可連結網際網路者，須逐項查核。			
9		四、(二)	連入規則的部分應以白名單開放方式設置，不得有 allow any，連出部分視應用狀況適當設置。	9.A. 請代檢廠展示及說明防火牆之網路連線通阻規則。 9.B. 檢查前述規則之連入內部網路部分，是否僅開放必要特定連線主機，且拒絕其他任何連線(deny all)；檢查前述規則之連出外部網路部分，是否限制與車輛檢驗業務無關之連線。 9.C. 請代檢廠展示其實際連線紀錄，檢查有無與車輛檢驗業務無關之連線，並請說明與檢驗業務之關聯性與必要性。 9.D. 依籌設須知裝設 VPN 數據線路者，屬符合規範；其餘數據線路可連結網際網路者，須逐項查核。			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
10		四、(二)	防火牆規則每年應至少確認 1 次，並留存相關紀錄以備查驗。	10.A. 請代檢廠出示並說明防火牆規則確認方式及記錄(線上或紙本記錄均可)。 10.B. 依籌設須知裝設 VPN 數據線路者，屬符合規範；其餘數據線路可連結網際網路者，須逐項查核。			
11		四、(三)	依實際狀況更新網路連結架構圖，標示各系統詳細資訊，並送交所屬監理機關備查。	11.A. 依據代檢廠提供之網路連結架構圖，檢查實際網路配置情形是否相符。 11.B. 網路連結架構圖應包含網路節點及用途、IP 位址、資料流。其中網路節點，應至少包含主機、資料庫、防火牆、集線器、IP 分享器(須標示有線或無線)、資料庫等。 ※RS232 如僅用作單純訊號控制、列印或傳真，則不屬於本規範所稱網路。			
12		四、(四)	無線網路設備應採用加密連線(如 WPA2)且隱藏 SSID，並妥善保管連線密碼。	12.A. 請代檢廠說明檢驗作業有無使用 WiFi 無線網路。 12.B. 檢查所使用無線網路是否採用加密連線(須至少為 WPA 或 WPA2，不可為 WEP)，且是否隱藏 SSID 。 12.C. 請代檢廠說明所使用無線網路之連線密碼保管方式為何，檢查是否妥善保密。 (檢驗用途之無線網路不可同時提供客戶使用，兩者間應有所區隔且不可連通；禁止以 Lan 埠插接實體線路連通 AP 及			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
				Router，或以 WDS 通訊傳輸，使兩無線網路間相互連線）			
13		四、（五）	網路連線設備如防火牆、交換器等，不可安置於公共場所，以確保實體安全。	13.A. 檢視網路連線設備擺放位置，是否具有適度區隔或避免置於公共場所。 13.B. 如置於供內部特定人員進出之辦公室，或置於以門板、櫃子、OA 等適度阻隔之空間，可避免外部不特定人員輕易碰觸到，應屬符合規定。			
14	軟體規範	五、（一）	檢驗線數位化系統僅安裝已知及可信任之軟體，並以白名單方式送交所屬監理機關備查。	14.A. 請代檢廠提供檢驗線數位化系統安裝使用之軟體名單(白名單)，包含軟體名稱及用途。 14.B. 檢查電腦實際安裝之軟體與所提供之白名單是否與相符。			
15		五、（四）	車輛檢驗軟體應有帳號及密碼管控功能，密碼複雜度至少 8 碼且英數字混雜。	15.A. 檢查車輛檢驗軟體(包含登檢、掛號、無紙化、簽證、銷號、錄影)，是否有帳號及密碼管控功能，又密碼複雜度是否符合規定。			
16		五、（五）	系統儲存或暫存數據或資料之資料夾或目錄，應設置存取權限控管功能，	16.A. 請代檢廠說明並展示系統數據、資料儲存(含暫存)之資料夾或目錄。 16.B. 檢查前述資料夾或目錄之安全性設定，存取對象是否僅限定為特定人或群組，又是			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
			不得開啟 Everyone 的完全控制權限。	否未開放 everyone 完全控制權限(含選擇以完全控制或全部項目方式授權)，			
17	資料規範	六、(一)	檢驗線各數位化系統之個人電腦必須有 USB 隨插即用連接埠之使用管制措施。	17.A. 請代檢廠說明檢驗線電腦主機及儲存設備之 USB 連接埠使用管制措施為何。 17.B. 檢查前項 USB 連接埠是否管制並限定特定人員或裝置可插接使用。 17.C. 請代檢廠使用 USB 裝置實際進行插拔測試，檢查是否確實達到管制效果。			
18		六、(三)	儲存或備份檢驗資料之資訊設備或資料庫，應設置管理者帳號及 8 碼以上之英數字混雜登入密碼，並紀錄各項登入活動，登入紀錄應至少留存 6 個月備查。	18.A. 請代檢廠說明並展示儲存備份檢驗資料之設備或資料庫之管理者帳號設定，檢查其密碼複雜度是否符合要求。 18.B. 請代檢廠展示儲存或備份檢驗資料之資訊設備或資料庫之登入記錄，檢查是否留存 6 個月備查。 (如資料庫未提供登入紀錄，而改以自行開發程式進行紀錄者，屬符合規範要求；登入紀錄不包含檔案分享資料夾之存取紀錄) 18.C. 如儲存或備份設備經確認無法於設備本身留存登入活動者，可以遠端存取該設備之電腦登入紀錄取代。			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

項目	類別	規範條款	規範內容簡述	檢查作業指引	查核結果		查核情形紀錄（含限期改善註記）
					符合	不符	
19		六、(四)	供應商提供備用設備作為車輛檢驗系統維護使用前，需先確認無惡意軟體；待修之硬碟或資料儲存設備，應確定資料保護作為，並於維修記錄中備註內含資料類別。	19.A. 請代檢廠說明檢驗系統設備報修或維護方式，並出示近一年報修及維護紀錄；若有報修或維護，請一併說明並提供備用設備連線使用前之惡意軟體檢查作法及紀錄。 19.B. 如前述設備有送出檢驗場外進行維修者，檢查送出前有無先行將機敏資料遮蔽或移除；惟若因此無法達到送檢修目的者，檢查是否於相關維修紀錄中註記資料類別。 19.C. 請代檢廠說明有無汰除檢驗相關電腦設備，並檢查有無針對檢驗資料進行抹除或格式化之紀錄。 ※有關惡意軟體之檢查，可請代檢廠參考使用 VirusTotal 網站 (https://www.virustotal.com/gui/home/upload)上傳軟體程式，進行惡意碼檢測。			

檢驗線電腦系統資訊安全查核表-110 年度車輛委託代檢使用

※注意事項：

1、 委託檢驗合約附件十二「檢驗線電腦系統資訊安全規範」之規範目的，在於使代檢廠善盡資訊安全維護責任，受委託辦理車輛檢驗服務得以順遂進行，並間接提升個資保護水平。

2、 本表僅摘錄可具體查核項目，代檢廠之資安管理責任以規範條文內容為準，不得以本表未摘錄，作為免責之依據。

3、 為保護檢驗資料及維護資訊安全，檢驗線電腦設備以全面管控為原則；惟考量檢驗作業順遂之需要，電腦設備如符合下列 2 條件，代檢廠得填具「代檢廠檢驗線電腦設備排除適用部分資訊安全規範條款備查表」，送轄管監理機關備查。(1)未儲存受託檢驗業務相關資料。(2)作業未涉及人員歸責。

4、 前述排除適用項目，以 1、2、15(對應規範二(一)、五(四))為原則。受檢代檢廠應具體明確說明排除事由及規範條款，檢查人員得依現場情形進行勘查認定；如認定不符前述規範意旨，應明確向受檢代檢廠說明並記錄。

5、 為強化資安作業檢查，受檢代檢廠應配合指派適當人員到場協助檢查，必要時亦應配合出示相關佐證資料。

6、 各項目辦理情形之查檢結果，檢查人員應明確登載具體查核事證，以免爭議；如認定有違反規範情形，應向受檢代檢廠明確說明查核情形，並限期改善。

查核日期：　中華民國_____年_____月_____日

代 檢 廠：_____　　代　表　人：_____

稽核人員：_____　　稽核人員主管：_____

會同人員：_____　　會同人員主管：_____