

勞動部勞動力發展署技能檢定中心

115 年度個資與資安宣導課程暨稽核前說明會計畫

- 一、主辦單位：勞動部勞動力發展署技能檢定中心
- 二、協辦單位：資拓宏宇國際股份有限公司
- 三、參與對象：學術科辦理單位
- 四、目的：本中心因辦理技能檢定業務，委託相關學術科辦理單位協助，並因此保有應檢人個人資料。為確保應檢人個資權益，並符合《個人資料保護法及子法》相關規定，本中心將辦理「委外稽核與輔導作業」，以實地稽核方式至各受委託單位進行查核與輔導。為此，本中心特於稽核前舉辦說明會。除宣導辦理檢定業務時應遵守的個人資料保護與資訊安全注意事項外，亦將詳細說明本次稽核的執行方式與相關作業流程。
- 五、講師：資拓宏宇國際股份有限公司/個資與資安顧問
- 六、方式：採線上方式辦理
- 七、線上軟體：Microsoft Teams 視訊會議。可採網頁版方式，參加線上說明會者可不用事先安裝 Microsoft Teams

視訊會議軟體，透過連結即可加入(相關教學請詳附件一)。

八、簡報：簡報資料訂於 9/15(二)起開放下載，檔案置於【技能檢定系統-單位專區-資訊交流】項下。

九、線上報名：即日起至說明會開始前，請至【技能檢定系統-單位專區-課程活動報名】擇一場次報名參加。

十、場次：共 3 場次

場次	日期	時間	線上說明會連結
第 1 場	115/09/16 (三)	14:00-17:00	https://gov.tw/Gaw https://bit.ly/sec260916
第 2 場	115/09/18 (五)	14:00-17:00	https://gov.tw/Jup https://bit.ly/sec260918
第 3 場	115/09/21 (一)	14:00-17:00	https://gov.tw/Qpm https://bit.ly/sec260921

十一、議 程：

時間	議程內容	單位
13:30-14:00	線上簽到	學術科 辦理單位
14:00-17:00	1. 說明會大綱 ※ 案例分享(個資與資安管理) ※ 稽核執执行程序說明 ※ 過往稽核結果分析 ※ 個人資料委外管理監督檢核表說明 ※ 總結 2. 討論發問時段	資拓宏宇 顧問
17:00	結束	

十二、連絡窗口：

- 報名系統諮詢：本中心資訊客服人員 04-22595700#693
- 稽核事宜諮詢：資拓宏宇國際股份有限公司

楊小姐 02-89691969#7503

michelle.yang@iisigroup.com

十三、 相關附件：

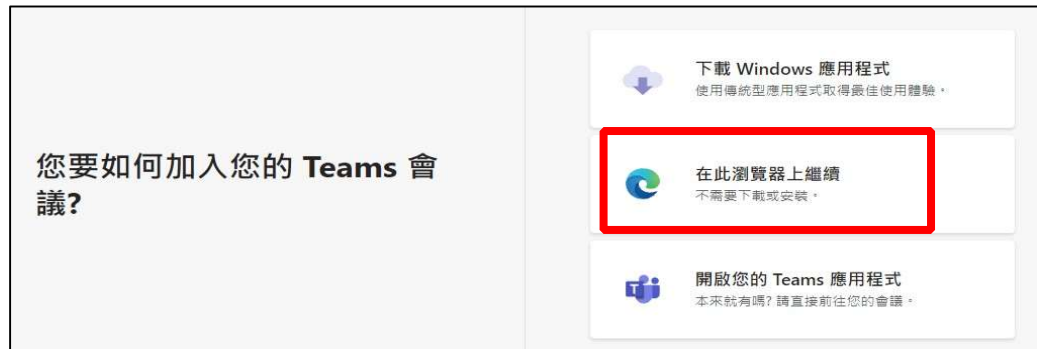
- 附件一：Microsoft Teams 視訊會議操作說明
- 附件二：個人資料委外管理監督檢核表
- 附件三：辦公室資通安全檢查表

附件一

Microsoft Teams 視訊會議操作說明

步驟一：將會議網址貼上瀏覽器網址列中，前往線上會議

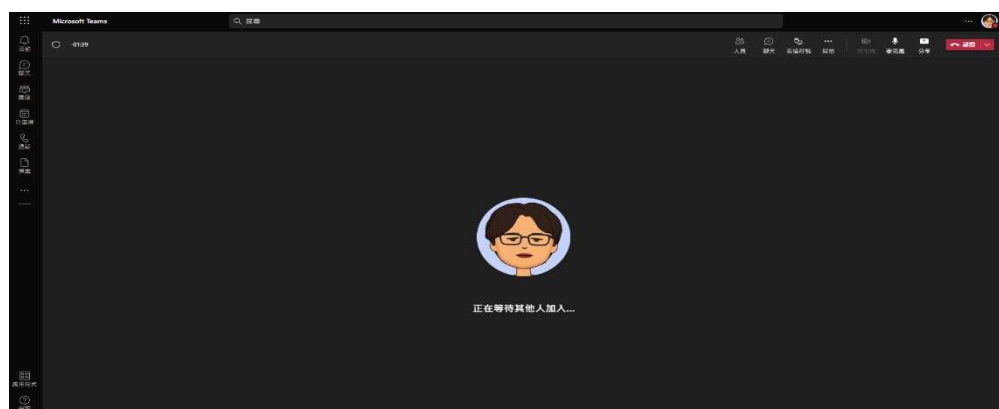
步驟二：點選「在此瀏覽器上繼續」



步驟三：修改來賓顯示名稱「姓名@單位」



步驟四：進入會議畫面



附件二

個人資料委外管理監督檢核表

專案名稱：_____

契約編號：_____

履約期間：_____至_____

執行單位：_____

檢 核 項 目	檢 核 結 果			說明／檢附資料
	符合	不符合	不適用	
(一) 個資法及施行細則要求事項	-	-	-	
1.應符合契約預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。				
2.契約執行期間應定期（每年至少一次）說明個人資料保護之安全維護措施落實情形	-	-	-	
(1) 應設置個資管理組織及成員名冊（含工作職責）。				
(2) 應盤點個人資料，製作盤點清冊，確認管理範圍（至少包含業務流程名稱、資料檔案名稱、目的、資料型式、存放位置，以及蒐集、處理、利用、保存、銷毀單位及方式、揭露對象、方式及範圍）。				
(3) 應制定風險管理規範文件且滾動檢討風險評估並製作報告紀錄（每年至少一次，如電腦下載或外部網路入侵、員工故意或過失、保護認知不足、天然災害等風險）。				
(4) 應制定個人資料蒐集、處理、利用、保存、刪除／銷毀、傳遞之內部管理規範文件（如告知、同意、權利行使、刪除／銷毀、傳遞、資料傳遞方式、拒絕行銷、				

權限管理)。				
(5) 應制定資料安全(紙本、電子文件及資訊系統資料庫, 包含網路、設備及環境安全)管理規範文件並提供管理紀錄(如電腦截圖、拍照)。				
(6) 應建置業務人員(涉及個資業務)工作職責清冊。				
(7) 業務人員(涉及個資業務)應簽署保密切結文件(如提供該文件, 請塗掉部分個資, 以無法識別為原則)。				
(8) 業務人員(涉及個資業務)應具備相關教育背景、經驗或參與教育訓練(內部或派員參加外部訓練), 應留存參訓證明(如證書, 請塗掉部分個資, 以無法識別為原則)。				
(9) 應宣導個人資料保護相關法規及組織之個人資料保護規範要求(如 E-mail)。				
(10) 應制定資料安全稽核機制並留存稽核通知、查核規劃及報告紀錄。				
(11) 應保存管理紀錄、軌跡資料及相關紀錄(如資料傳遞方式及對象清單、當事人權利行使)。				
(12) 應定期召開內部會議, 檢視內部個人資料安全維護整體情形, 以確保持續改善管理現況, 並留存會議及簽到紀錄。				
3.複委託第三方蒐集、處理或利用個人資料之事項, 應獲得本中心同意授權。				
4.應制定個資事件(如竊取、洩漏、竄改或其他侵害者)之緊急應變、通報(本中心)及預防機制文件, 並留存通報及事件處理紀錄。				
5.應於發生個資事件時即時通知本中心, 說明事件的原委與應變、預防				

措施、改善情形，且以適當方式通知當事人。				
6.接獲當事人行使權利之請求時，應依個人資料保護法第 13 條要求進行處理，並立即告知本中心。				
7.廠商指定之專責人員定期清查所保有個人資料之處理及利用是否符合蒐集特定目的，若有非屬特定目的必要範圍之個人資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置，並將處置情形及佐證資料通報機關。				
(二)確實遵守所提交之個人資料檔案安全維護計畫之要求。				
(三)承上，所交付建議書或專案管理計畫書中，對個人資料檔案安全維護之建議要求，除所提交之個人資料檔案安全維護計畫之要求外，應確實遵守額外要求內容。				

註：

- 1.勾選「不適用」或「不符合」應詳述原因。
- 2.說明及檢附資料得擇一，且應具體明確。
- 3.不適用：表示實際作業未發生稽核要項之規範、要求或時間點未到，以致稽核時無法確認、判斷。

〔廠商〕

公司章

檢核人簽章：

負責人簽章：

檢核日期： 年 月 日

辦公室資通安全檢查表

科 室		受檢人員	
檢查類別	☐ 專人檢查 ☐ 自我檢查	檢查日期	年 月 日

序	檢 查 項 目	檢查狀況	查核紀錄
1	個人電腦系統(含應用系統)登入已設定帳號及密碼(套用 AD 之系統使用者其密碼長度應為 12 碼(含)以上；其他非套用 AD 之系統使用者其密碼長度應為 8 碼(含)以上)，字母大小寫、數字、符號，4 種組合中任選 3 種組合而成，密碼未置放於顯而易見之處，另須停用本機管理者或不使用之帳號。	☐ 符合 ☐ 不符合	
2	通行密碼至少每九十天更新一次。	☐ 符合 ☐ 不符合	
3	電腦已啟動螢幕保護程式且設定密碼保護(閒置超過 15 分鐘即啟動螢幕保護程式或鎖定)。	☐ 符合 ☐ 不符合	
4	禁止擅自於公共網路下載安裝或自行安裝非法、用途不明之及未經授權核准之軟體。	☐ 符合 ☐ 不符合	
5	電腦已安裝防毒軟體，且病毒碼已更新至最新(七天內發布版本)。	☐ 符合 ☐ 不符合	
6	確認軟體修補程式已更新，Java 更新則視使用者需求確認。	☐ 符合 ☐ 不符合	
7	作業系統應在 1 個月內之完成修補程式之更新。	☐ 符合 ☐ 不符合	

序	檢 查 項 目	檢 查 狀 況	查 核 紀 錄
8	電腦已安裝及啟用防火牆安全防護功能。	☐ 符合 ☐ 不符合	
9	自由軟體需依本中心許可安裝之軟體清冊(白名單)安裝使用。	☐ 符合 ☐ 不符合	
10	使用瀏覽器瀏覽網站時，將瀏覽器安全性設定為「中高」以上，以限制執行非信任網站之行動碼，並取消自動完成設定。	☐ 符合 ☐ 不符合	
11	禁止將未加密之機敏資料存放於共用磁碟。	☐ 符合 ☐ 不符合	

序	檢 查 項 目	檢 查 狀 況	查 核 紀 錄
12	機敏資料若需上傳至本中心之雲端空間應加密或使用密碼保護之，若有特殊需求需上傳非本中心之雲端硬碟，應經主管核准並加密或使用密碼保護之。	☐ 符合 ☐ 不符合	
13	機敏資料需燒錄光碟時，須經單位主管核准。	☐ 符合 ☐ 不符合	
14	密級及個資資料或文件，原則上對內或對外不得以電子郵件傳送；若有特殊業務需求，需以電子郵件傳送者，則必須以加密方式處理，且密碼不得附於同一封郵件內。	☐ 符合 ☐ 不符合	
15	電子郵件寄件前請檢查收件者是否正確，包括附加之檔案，應事前檢視內容有無錯誤，避免誤寄機敏資訊給不適當的收件者。	☐ 符合 ☐ 不符合	
16	於收件時關閉郵件預覽功能，並應預設為純文字模式讀取郵件，不隨意開啟附件檔及點選不明連結。	☐ 符合 ☐ 不符合	
17	禁止將機敏資料存放於沒有加密或密碼保護之可攜式設備及可攜式儲存媒體(如：外接式硬碟、隨身碟或其他儲存設備)。	☐ 符合 ☐ 不符合 ☐ 不適用	
18	重要之可攜式設備及可攜式儲存媒體(如：外接式硬碟、隨身碟或其他儲存設備)均已置放於有上鎖之抽屜或資料櫃。	☐ 符合 ☐ 不符合 ☐ 不適用	
19	承辦業務之機敏文件，不使用、下班或長時間離座時，應收妥且存放於上鎖資料櫃(確保實體安全)。	☐ 符合 ☐ 不符合	
20	人員離座時，應隨時登出本中心各項應用系統並啟動螢幕保護程式鎖定使用中的資訊設備。	☐ 符合 ☐ 不符合	

序	檢 查 項 目	檢 查 狀 況	查 核 紀 錄
	(按 Windows+L)		
21	影印機、傳真機、印表機、其他事務性機器及廢紙回收處均未遺留機敏文件。	☐ 符合 ☐ 不符合	
22	使用可攜式設備上的通訊軟體(如：Line、WhatsApp、WeChat 等)討論重要資訊或交換檔案，並且避免加入來歷不明的聯絡人。	☐ 符合 ☐ 不符合 ☐ 不適用	
23	可攜式設備應避免連結公開無密碼保護之無線網路功能，且禁止使用公開無線網路傳輸隱私性高或機敏資料。	☐ 符合 ☐ 不符合 ☐ 不適用	

序	檢 查 項 目	檢 查 狀 況	查 核 紀 錄
24	人員下班時應將桌面保持整潔並勿放置機敏文件，各式可攜式設備及儲存媒體應存置於櫃內並上鎖、拔除自然人憑證、放置公文及機敏性文件之資料櫃及抽屜一律需上鎖、管制區域應關門並上鎖。	☐ 符合 ☐ 不符合	
25	電腦設備使用完畢或下班時，應將電腦、印表機及螢幕之電源關閉。	☐ 符合 ☐ 不符合	
26	一般主管與一般同仁(含廠商駐點人員)每年至少參與 3 小時個資與資安相關宣導課程。	☐ 符合 ☐ 不符合	
27	委外受託者應簽訂相關保密切結書和遵循保密切結書內容，且複受託者作業人員也均應簽署保密切結書和遵循之。	☐ 符合 ☐ 不符合 ☐ 不適用	

檢查人員		受檢單位主管	
------	--	--------	--