檔　　號：
保存年限：

臺中市工程技術顧問商業同業公會
115.01.06
收文號：001

行政院公共工程委員會　函

406537
臺中市北屯區南興路868號14樓之6

受文者：臺中市工程技術顧問商業同業公會

地址：110207 臺北市信義區松仁路3號9樓
聯絡方式：(承辦人)黃政羚
(聯絡電話)02-87897766
(傳真)02-87897674
(E-mail)kathleen18@mail.pcc.gov.tw

發文日期：中華民國114年12月29日
發文字號：工程技字第1140032401號
速別：普通件
密等及解密條件或保密期限：
附件：如說明二

主旨：函轉經濟部114年12月19日經授產字第11451040910號函有關「公司或有限合夥事業投資智慧機械與第五代行動通訊系統與資通安全人工智慧產品或服務及節能減碳抵減辦法」第4條修正條文對照表勘誤表1份，請轉知所屬會員，請查照。

說明：

一、「公司或有限合夥事業投資智慧機械與第五代行動通訊系統與資通安全人工智慧產品或服務及節能減碳抵減辦法」業經經濟部會銜財政部以114年11月27日經產字第11451033650號、台財稅字第11404671720號令修正發布在案。

二、檢附旨揭函文影本及其附件各1份。

正本：各工程技術顧問同業公會
副本：本會技術處

主任委員 陳金德

檔　　號:
保存年限:

經濟部 函

地址：台北市大安區信義路三段41-3號
聯絡人：唐克敏
聯絡電話：(02)2754-1255 分機2636
電子郵件：kmtang@ida.gov.tw
傳真：(02)2704-3784

受文者：行政院公共工程委員會

發文日期：中華民國114年12月19日
發文字號：經授產字第11451040910號
速別：普通件
密等及解密條件或保密期限：
附件：如主旨（510409100_勘誤附件一第4條修正條文對照表勘誤表.odt）

主旨：檢送「公司或有限合夥事業投資智慧機械與第五代行動通訊系統與資通安全人工智慧產品或服務及節能減碳抵減辦法」第4條修正條文對照表勘誤表1份，請惠予更正。

說明：「公司或有限合夥事業投資智慧機械與第五代行動通訊系統與資通安全人工智慧產品或服務及節能減碳抵減辦法」業經本部會銜財政部於中華民國114年11月27日以經產字第11451033650號、台財稅字第11404671720號令修正發布在案。

正本：立法院、司法院秘書長、行政院法規會、行政院經濟能源農業處、行政院公共工程委員會、金融監督管理委員會、內政部、文化部、交通部、法務部、財政部、農業部、數位發展部、經濟部能源署、經濟部商業發展署、經濟部產業發展署（金屬機電產業組、電子資訊產業、民生化工產業組、知識經濟產業組、永續發展組）

副本：財政部法制處、經濟部經濟法制司、經濟部產業發展署[產業政策組（法規通報專責人員）]、法源資訊股份有限公司(均含附件) 電子公文交換章 2025/12/19 13:56:07

行政院公共工程委員會
技術處 1140032401

「公司或有限合夥事業投資智慧機械與第五代行動通訊系統與資通安全人工智慧產品或服務及節能減碳抵減辦法」第四條修正條文對照表勘誤表

更正後文字			原列文字		
修正條文	現行條文	說明	修正條文	現行條文	說明
第四條　本辦法所稱資通安全產品或服務，指為防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，確保其機密性、完整性及可用性，運用於終端與行動裝置防護、網路安全維護或資料與雲端安全維護，並具有下列功能之一之硬體、軟體、技術或技術服務： 一、辨識（Identify）：建立資通安全管理規則以管理人員、端點裝置、網路設備、雲端資產、數位資料之網路安全風險，並符合下列功能之一： （一）資通安全治	第四條　本辦法所稱資通安全產品或服務，指為防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，確保其機密性、完整性及可用性，運用於終端與行動裝置防護、網路安全維護或資料與雲端安全維護，並具有下列功能之一之硬體、軟體、技術或技術服務： 一、辨識（Identify）：建立資通安全管理規則以管理人員、端點裝置、網路設備、雲端資產、數位資料之網路安全風險，並符合下列功能之一： （一）資通安全治	本條未修正。	第四條　本辦法所稱資通安全產品或服務，指為防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，確保其機密性、完整性及可用性，運用於終端與行動裝置防護、網路安全維護或資料與雲端安全維護，並具有下列功能之一之硬體、軟體、技術或技術服務： 一、辨識（Identify）：建立資通安全管理規則以管理人員、端點裝置、網路設備、雲端資產、數位資料之網路安全風險，並符合下列功能之一： （一）資通安全治	第四條　本辦法所稱資通安全產品或服務，指為防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，確保其機密性、完整性及可用性，運用於終端與行動裝置防護、網路安全維護或資料與雲端安全維護，並具有下列功能之一之硬體、軟體、技術或技術服務： 一、辨識（Identify）：建立資通安全管理規則以管理人員、端點裝置、網路設備、雲端資產、數位資料之網路安全風險，並符合下列功能之一： （一）資通安全治	本條未修正。

理及風險評估：依據企業組織之目標及整體需求，建立、規劃資通安全治理政策或方案；或評估及擬定企業組織之資通安全風險對策。	理及風險評估：依據企業組織之目標及整體需求，建立、規劃資通安全治理政策或方案；或評估及擬定企業組織之資通安全風險對策。		理及風險評估：依據企業組織之目標及整體需求，建立、規劃資通安全治理政策或方案；或評估及擬定企業組織之資通安全風險對策。	理及風險評估：依據企業組織之目標及整體需求，建立、規劃資通安全治理政策或方案；或評估及擬定企業組織之資通安全風險對策。	
（二）資產管理：依據企業組織之目標及風險策略，對人員、資料、設備或系統進行識別和管理。	（二）資產管理：依據企業組織之目標及風險策略，對人員、資料、設備或系統進行識別和管理。		（二）資產管理：依據企業組織之目標及風險策略，對人員、資料、設備或系統進行識別和管理。	（二）資產管理：依據企業組織之目標及風險策略，對人員、資料、設備或系統進行識別和管理。	
二、保護（Protect）：建立和實施適當之資通安全措施以確保重要服務、設備、企業營運的運行，並符合下列功能之一：	二、保護（Protect）：建立和實施適當之資通安全措施以確保重要服務、設備、企業營運的運行，並符合下列功能之一：		二、保護（Protect）：建立和實施適當之資通安全措施以確保重要服務、設備、企業營運的運行，並符合下列功能之一：	二、保護（Protect）：建立和實施適當之資通安全措施以確保重要服務、設備、企業營運的運行，並符合下列功能之一：	

（一）端點裝置防護：透過軟體、硬體對企業設備裝置和使用者強制執行原則，藉此加強網路安全和存取管理。	（一）端點裝置防護：透過軟體、硬體對企業設備裝置和使用者強制執行原則，藉此加強網路安全和存取管理。		（一）端點裝置防護：透過軟體、硬體對企業設備裝置和使用者強制執行原則，藉此加強網路安全和存取管理。	（一）端點裝置防護：透過軟體、硬體對企業設備裝置和使用者強制執行原則，藉此加強網路安全和存取管理。	
（二）網路安全防護：透過網路設定、來源與端點驗證或效能及安全管理等，使企業可有效掌握整體網路安全管理。	（二）網路安全防護：透過網路設定、來源與端點驗證或效能及安全管理等，使企業可有效掌握整體網路安全管理。		（二）網路安全防護：透過網路設定、來源與端點驗證或效能及安全管理等，使企業可有效掌握整體網路安全管理。	（二）網路安全防護：透過網路設定、來源與端點驗證或效能及安全管理等，使企業可有效掌握整體網路安全管理。	
（三）資料加密與保護：運用資料加密技術針對機敏或價值資料提供保護或去識別化，並符合法規遵循及管理	（三）資料加密與保護：運用資料加密技術針對機敏或價值資料提供保護或去識別化，並符合法規遵循及管理		（三）資料加密與保護：運用資料加密技術針對機敏或價值資料提供保護或去識別化，並符合法規遵循及管理	（三）資料加密與保護：運用資料加密技術針對機敏或價值資料提供保護或去識別化，並符合法規遵循及管理	

需求。 （四）應用服務保護：為強化帳號密碼管理，使用各種智慧卡、憑證、動態密碼或生物特徵等多因子驗證技術，以強化身分驗證之安全防護。 三、偵測（Detect）：制定並實施適當的作為以識別資通安全事件的發生，並符合下列功能之一： （一）端點及網路偵測與回應：包括即時監控與收集端點及網路惡意行為資料，並具備自動回應機制，可偵	需求。 （四）應用服務保護：為強化帳號密碼管理，使用各種智慧卡、憑證、動態密碼或生物特徵等多因子驗證技術，以強化身分驗證之安全防護。 三、偵測（Detect）：制定並實施適當的作為以識別資通安全事件的發生，並符合下列功能之一： （一）端點及網路偵測與回應：包括即時監控與收集端點及網路惡意行為資料，並具備自動回應機制，可偵		需求。 （四）應用服務保護：為強化帳號密碼管理，使用各種智慧卡、憑證、動態密碼或生物特徵等多因子驗證技術，以強化身分驗證之安全防護。 三、偵測（Detect）：制定並實施適當的作為以識別資通安全事件的發生，並符合下列功能之一： （一）端點及網路偵測與回應：包括即時監控與收集端點及網路惡意行為資料，並具備自動回應機制，可偵	需求。 （四）應用服務保護：為強化帳號密碼管理，使用各種智慧卡、憑證、動態密碼或生物特徵等多因子驗證技術，以強化身分驗證之安全防護。 三、偵測（Detect）：制定並實施適當的作為以識別資通安全事件的發生，並符合下列功能之一： （一）端點及網路偵測與回應：包括即時監控與收集端點及網路惡意行為資料，並具備自動回應機制，可偵	

測並調查主機和端點上之可疑活動。 （二）使用者行為分析：使用機器學習、人工智慧或巨量資料等技術來分析一般日常活動之差異，進而識別惡意行為。 （三）網路威脅情資運用：利用網路威脅情資，掌握目前外部威脅趨勢及作出正確的資安決策。 四、回應（Respond）：對偵測到之資通安全事件，規劃並實施適當的行動，包括但不	測並調查主機和端點上之可疑活動。 （二）使用者行為分析：使用機器學習、人工智慧或巨量資料等技術來分析一般日常活動之差異，進而識別惡意行為。 （三）網路威脅情資運用：利用網路威脅情資，掌握目前外部威脅趨勢及作出正確的資安決策。 四、回應（Respond）：對偵測到之資通安全事件，規劃並實施適當的行動，包括但不		測並調查主機和端點上之可疑活動。 （二）使用者行為分析：使用機器學習、人工智慧或巨量資料等技術來分析一般日常活動之差異，進而識別惡意行為。 （三）網路威脅情資運用：利用網路威脅情資，掌握目前外部威脅趨勢及作出正確的資安決策。 四、回應（Respond）：對偵測到之資通安全事件，規劃並實施適當的行動，包括但不	測並調查主機和端點上之可疑活動。 （一）使用者行為分析：使用機器學習、人工智慧或巨量資料等技術來分析一般日常活動之差異，進而識別惡意行為。 （三）網路威脅情資運用：利用網路威脅情資，掌握目前外部威脅趨勢及作出正確的資安決策。 四、回應（Respond）：對偵測到之資通安全事件，規劃並實施適當的行動，包括但不	

限於資通安全事件之後的數位證據保存、數位鑑識、數位資產監控追蹤。 五、復原（Recover）：制定並實施適當的措施以修復因資通安全事件受損的功能和服務，並符合下列功能之一： （一）異地備援：應變規劃應涵蓋營運衝擊分析、備援與復原策略、備援中心、復原計畫制定或應變計畫等軟硬體之技術考量。 （二）資料備份：災難發生或設備故障時，保護資料避免遭受	限於資通安全事件之後的數位證據保存、數位鑑識、數位資產監控追蹤。 五、復原（Recover）：制定並實施適當的措施以修復因資通安全事件受損的功能和服務，並符合下列功能之一： （一）異地備援：應變規劃應涵蓋營運衝擊分析、備援與復原策略、備援中心、復原計畫制定或應變計畫等軟硬體之技術考量。 （二）資料備份：災難發生或設備故障時，保護資料避免遭受		限於資通安全事件之後的數位證據保存、數位鑑識、數位資產監控追蹤。 五、復原（Recover）：制定並實施適當的措施以修復因資通安全事件受損的功能和服務，並符合下列功能之一： （一）異地備援：應變規劃應涵蓋營運衝擊分析、備援與復原策略、備援中心、復原計畫制定或應變計畫等軟硬體之技術考量。 （二）資料備份：災難發生或設備故障時，保護資料避免遭受	限於資通安全事件之後的數位證據保存、數位鑑識、數位資產監控追蹤。 五、復原（Recover）：制定並實施適當的措施以修復因資通安全事件受損的功能和服務，並符合下列功能之一： （一）異地備援：應變規劃應涵蓋營運衝擊分析、備援與復原策略、備援中心、復原計畫制定或應變計畫等軟硬體之技術考量。 （二）資料備份：災難發生或設備故障時，保護資料避免遭受	

到破壞或將破壞的程度減緩至最小。 前項規定之資通安全產品或服務，屬安裝於個人電腦之防毒軟體或防火牆者，不適用之。	到破壞或將破壞的程度減緩至最小。 前項規定之資通安全產品或服務，屬安裝於個人電腦之防毒軟體或防火牆者，不適用之。		到破壞或將破壞的程度減緩至最小。 前項規定之資通安全產品或服務，屬安裝於個人電腦之防毒軟體或防火牆者，不適用之。	到破壞或將破壞的程度減緩至最小。 前項規定之資通安全產品或服務，屬安裝於個人電腦之防毒軟體或防火牆者，不適用之。	