管理辦法編號	管理辦法名稱	版次	項次	內文	備註
2-068	人員安全管理規定	1.2	5.1.4	外部人員、訪客若需進入本公司紅區，應簽署「人員保密切結書」	
			5.1.13	委外人員之管理規範，請參考「資訊委外管理規定」(2-073)之相關規定。	
			5.2.3	對本公司人員進行資訊安全教育及訓練之政策，亦適用於約聘（僱）人員、臨時人員及委外駐點	
			5.2.4	本公司得要求委外廠商提供服務人員之資訊安全相關受訓證明，若無相關訓練證明，則應參與本公司資訊安全相關教育訓練。	
			5.3.1	本公司人員、約聘（僱）人員與委外人員於任何資訊安全事件發生時，應依照正式通報程序通知相關負責人員。	
2-069	實體安全管理規定	1.2	5.1.3	若外部人員或本公司未具安全區域進出權限人員，因執行業務需求進入安全區域時，必須由權責單位指派人員陪同並填寫「人員進出登記表」(7635)後方可進出安全區域，並遵守相關資訊資產	
			5.2.2	若外部人員或本公司未具交付及裝卸區域進出權限人員，因執行業務需求進入交付及裝卸區域時，必須由權責單位指派人員監控或隨行，並填寫「人員進出登記表」(7635)後方可進出交付及裝卸區域，並遵守相關資訊資產管理之規定。	
			5.9.1	所有資訊設備維護契約，應由專人負責保管與定期審查契約時間是否過期與該資訊設備是否仍有維護需求，若仍有維護需求則應依「資訊委外管理規定」(2-073)簽訂維護契約。	
2-071	存取控制管理規定	1.1	5.6.3.	對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。	
			5.9.4	通知主機供應商提供必要的回復協助。	
2-072	系統獲取、開發與維護規定	1.1	5.1.1	（6）C. 應要求系統委外供應商，配合本公司提出系統安全之風險與機會評鑑資料。	
			5.7.16	對往來廠商之軟體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之帳號及通行密碼。	
			5.7.17	建立往來廠商人員管理之相關程序，請參閱本公司「資訊委外管理規定」(2-073)。	
			5.1.1	委外供應商應提供負責系統維護、聯絡窗口及電話諮詢服務，並解決系統相關事宜，並配合本公司相關程序辦理異常排除及通報事宜，如必要應提供駐點服務。	
			5.1.2	委外供應商於提供服務過程，如接觸本公司「機密」等級含以上 之資料，應遵守相關法令及本公司之相關規定，並應簽署「正新保密契約」。	
			5.1.3.	委外供應商履行合約應提供其使用之軟體，且均須為合法軟體，並不得違反智慧財產權之規定，如有違反事情發生，委外供應商須承擔所有法律責任。	
			5.1.4.	委外供應商使用之工具軟體及處理作業之執行紀錄，本公司有權進行稽核，供應商不得異議。	
			5.1.5.	委外供應商應留存異常處理紀錄，本公司得視需要查核。	
			5.1.6.	委外供應商所交付之標的物如侵害第三人合法權益時，應由承包供應商負責處理並承擔一切法律	
			5.1.7.	委外供應商如因其員工執行業務之過失，造成本公司損失或傷害，委外供應商需負損害賠償責	
			5.1.8.	委外供應商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及作業權限。	
			5.1.9.	委外供應商人員，於支援業務時所獲知「內部使用」等級(含)以上資訊，不得對外透露。	
			5.1.10.	「內部使用」等級(含)以上資訊需進行傳遞、處理或存儲作業時，應參考「通信與作業管理規定」(2-070)之加密相關規範。	
			5.4.1	系統若委由外部供應商開發，供應商應提供完整之系統架構說明、系統分析設計、資料庫欄位設計等相關文件，經由本公司相關人員確認後方能執行。	
			5.4.2	委外供應商應確實控管程式與文件版本之一致性。	
			5.4.3	委外供應商進行系統開發與維護時，不得任意複製或攜出本公司「內部使用」(含)等級以上之業務資料。	
			5.4.4	委外供應商需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式。	

			5.4.5	若系統、軟體由委外供應商開發者，應由本公司人員測試及驗收上線之程式，確定符合相關需求後，方得依照「系統獲取、開發與維護規定」(2-072)之程序進行上線。	
			5.4.6	程式修改與開發需遵守本公司「系統獲取、開發與維護規定」(2-072)之規定，若有例外，須經資訊單位主管同意以後，方可實施。	
			5.5.2	委外供應商之人員如因作業需求，需對本公司系統進行存取，應參考「存取控制管理規定」(2-071)之相關管理規範。	
			5.5.3	委外供應商人員對於系統帳號應善盡保管之責，系統帳號不得任意交由非作業相關人員使用。	
			5.5.4	委外供應商人員對於系統之操作，本公司各系統管理者應盡監督之責，委外供應商人員不得從事非工作範圍內之操作。各系統管理者並應於委外供應商人員完成工作後檢視系統紀錄。	
2-073	資訊委外管理規定	1.3	5.7.1	委外供應商如需攜帶可攜式電腦或儲存媒體如磁片、光碟、隨身碟、外接式硬碟等進入本公司安全區域使用，需經陪同之單位承辦人員同意並註記於「人員進出登記表」(7635)，並定期由權責單位主管審閱。	
			5.7.2	供應商人員進入安全區域並使用可攜式電腦或儲存媒體時，須有監控設備進行監控或本公司人員全程陪同。	
			5.9.1	(1) C. 如專案委外辦理，應訂定供應商應遵守之法律、法規要求(如著作權法、智慧財產權相關法規、個人資料保護法等)，並敘明是否允許轉包/分包。	
				(1) G. 訂定遵守本公司相關資訊安全管理要求之義務，如事件通報程序、提供聯繫窗口，供應商之資訊安全責任及違反之後果。	
			5.9.3	(4) 主辦單位承辦人應於確認選商後，針對委外供應商服務內容，依據「委外供應商安全評估表」(7720)進行安全評估，評估結果應經主辦單位主管審核，風險值加總後如為19(含)以上，應定期(每3年一次)/不定期進行監督，如定期舉辦專案會議針對安全議題進行說明、主辦單位進行實地查核或由供應商提供具結保證之自我查檢紀錄等；風險總值19以下之供應商，如於提供服務過程，會存取本公司「機密」等級（含）以上之資訊資產者，則應每3年進行一次自評作業，以確	
			5.9.4	(4) 主辦單位應檢視委外供應商提供之產品、資訊或服務，要求委外供應商針對所提供之產品、資訊或服務之適法性(如著作權、智慧財產權之歸屬等)、安全性(如弱點掃描、滲透測試等)，進行整體資通訊技術供應鏈之適當安全性檢測或監督作業，並視需要提供佐證資料。	
				(5) 主辦單位應評量與管理專案之安全風險，如委外供應商人力或能力不足、需求變動頻繁及技術面臨瓶頸等，必要時採取應變措施。而所提出之相關風險項目可納入「委外供應商安全評估表」(7720)進行評估，防止新委外供應商重覆犯錯。	
			5.9.6	(6) 視專案需要，應於評估後要求委外供應商於專案驗收時提供交付標的之安全技術檢測報告(例如：弱點掃描與滲透測試報告)，且應以採用國際弱點資料庫（如：CVS）之檢測工具進行檢測作業。	
				(7) 專案委外供應商於驗收交付之專案標的，若尚有未修復/補之各種高風險弱點，專案供應商應提供修補計畫並報請本公司同意後始得驗收。	
MM-C3-025	遠端存取作業管理辦法	1.2	5.2.2	若代為委外廠商申請，宜提供委外廠商固定來源IP，若無簽訂維護合約，需請廠商填寫保密切結	