資訊安全工程師職能基準

職能基準代碼		INM2529-001v1			
職能基準名稱 (擇一填寫)		**職類**			
		職業	資訊安全工程師		
所屬類別	**職類別**	資訊科技 / 網路規劃與建置管理		**職類別代碼**	INM
	職業別	其他資料庫及網路專業人員		**職業別代碼**	2529
	行業別	出版、影音製作、傳播及資通訊服務業 / 電腦程式設計、諮詢及相關服務業		**行業別代碼**	J62
工作描述		具備相關資訊安全知識，藉由組織內部能力或尋求外部廠商、專家協助，建立符合法規與組織安全需求之系統、網路與安全防護架構，並執行相關維運作業與協助其他單位執行資訊安全相關活動。			
基準級別		4			

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
T1 資訊安全管理系統（Information Security Management System, ISMS）維運	T1.1 資訊安全管理系統維運	O1.1.1ISMS 文件 O1.1.2 ISMS 維運紀錄	P1.1.1 了解機密性、完整性、可用性之定義 P1.1.2 了解可歸責性、不可否認性、鑑別、可靠度之義涵 P1.1.3 具備 ISMS 觀念 P1.1.4 協助撰寫 ISMS 相關文件 P1.1.5 協助 ISMS 相關紀錄產出與留存	3	K01 機密性、完整性、可用性 K02 可歸責性、不可否認性、鑑別、可靠度 K03 戴明循環（Deming Cycle）Plan-Do-Check-Act, PDCA K04 最小權限（Least Privilege） K05 職務區隔（Segregation Of Duties, SOD）	S01 應用機密性、完整性、可用性之概念於日常作業。 S02 應用可歸責性、不可否認性、鑑別、可靠度於日常作業 S03 建立符合 ISMS 精神之架構並落實維運
T2 資產與風險管理	T2.1 建立資產清冊	O2.1.1 資產清冊	P2.1.1 協助各資產負責人盤點並建立資產清冊	3	K06 資產分類	S04 盤點與分類資產 S05 建立資產清冊
	T2.2	O2.2.1 可接受風險判	P2.2.1 參與可接受風險等級判定	4	K08 風險識別、分析與評估	S06 產製風險評鑑報告

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
	風險識別、分析與評估	定準則 O2.2.2 風險識別、分析與評估報告	準則之討論 P2.2.2 協助各單位進行風險分析與評估並產製報告		K09 可接受風險 K10 殘餘風險	
	T2.3 風險處理	O2.3.1 高風險清單 O2.3.2 風險處理計畫	P2.3.1 協助識別不可接受風險項目 P2.3.2 協助風險高於可接受等級項目之權責單位，擬定風險處理計畫 P2.3.3 協助確認風險處理計畫執行之有效性，以確認是否如預期之降低風險值	4	K11 風險處理方式（接受風險、移轉風險、降低	S07 協助需進行風險處理單位，針對高於可接受風險項目，提出風險處理計畫 S08 協助確認風險處理計畫實際執行之有效性
T3 規劃網路系統與資安防護架構	T3.1 網路與系統架構規劃	O3.1.1 網路架構圖 O3.1.2 符合需求之相關網路設備	P3.1.1 協助與網路管理人員，確認網路安全需求 P3.1.2 協助網路管理單位，依據網路安全需求，設計安全網路架構	5	K12 網路拓樸（Topology） K13 Transmission Control Protocol / Internet Protocol (TCP/IP) K14 網路路由（Network Routing） K15 網路服務（Domain Name System, DNS、Dynamic Host Configuration Protocol, DHCP、Server Message Block, SMB、Network Time Protocol, NTP 等） K16 網路與系統弱點 K17 攻擊手法與防禦	S09 規劃網路區隔與路由 S10 依需求選擇適當之網路設備
	T3.2	O3.2.1 系統安全組態	P3.2.1 協助系統管理人員，確認	5	K16 網路與系統弱點	S11 協助設定系統、資料庫、服務相關

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
	系統安全管控規劃	設定規範，包括系統、資料庫、應用程式等 O3.2.2 符合需求之作業系統 O3.2.3 符合需求之資料庫	系統安全需求 P3.2.2 協助系統管理單位，依據系統安全需求，設計足夠之安全系統組態與架構		K17 攻擊手法與防禦 K18 作業系統原理 K19 資料庫原理 K20 服務系統（郵件、File Transfer Protocol, FTP、DNS、網站等）	之安全組態 S12 依需求選擇適當之資料庫、作業系統、服務（含應用程式）
	T3.3 資安架構規劃	O3.3.1 網路端資安防護架構與設備 O3.3.2 主機端資安防護架構與設備 O3.3.3 終端資安防護設備	P3.3.1 與相關人員討論以找出網路、主機、終端設備之安全需求 P3.3.2 依據安全需求，選擇與建置合適之資安防護設備	5	K12 網路拓樸（Topology） K13 Transmission Control Protocol / Internet Protocol (TCP/IP) K14 網路路由（Network Routing） K15 網路服務（Domain Name System, DNS、Dynamic Host Configuration Protocol, DHCP、Server Message Block, SMB、Network Time Protocol, NTP 等） K16 網路與系統弱點 K17 攻擊手法與防禦 K18 作業系統原理 K19 資料庫原理 K20 服務系統（郵件、File Transfer Protocol, FTP、DNS、網站等）	S13 規劃、配置防火牆 S14 規劃、配置網路型入侵偵測/防禦系統 S15 規劃、配置主機型入侵偵測/防禦系統 S16 規劃、配置終端設備惡意攻擊防護機制，例如防毒

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
T4 系統、網路維運	T4.1 身分認證與存取控制	O4.1.1 權限申請/異動/刪除紀錄 O4.1.2 權限定期審查紀錄	P4.1.1 協助設計使用者可以安全存取到適當的網路、系統、終端設備之認證程序 P4.1.2 協助擬定權限（含實體管控、系統、網路、資料庫、終端、資安設備等）之變更管理流程 P4.1.3 協助各網路、系統、終端設備管理人員，進行存取權限審查作業	4	K04 最小權限（Least Privilege） K21 特權管理 K22 變更管理 K23 相關法規、主管機關要求 K24 合約要求、業務需求 K25 識別（Identification）、鑑別（Authentication） K26 識別與存取管理（IAM） K27 權限審查	S17 協助擬定權限申請/異動/刪除程序，並留存相關紀錄 S18 協助擬定權限定期審查程序，並留存相關紀錄
	T4.2 帳號密碼管理	O4.2.1 帳號變更管理程序 O4.2.2 帳號申請/異動紀錄 O4.2.3 帳號定期審查紀錄 O4.2.4 密碼原則 O4.2.5 密碼管理系統	P4.2.1 協助擬定帳號申請/異動、刪除之安全變更程序 P4.2.2 協助擬定符合需求之密碼原則（強度，包括：長度、複雜度、變更週期、最小重複代數等） P4.2.3 向使用者宣導密碼強度要求與重要性 P4.2.4 建置可管理使用者符合密碼原則之管理系統	3	K04 最小權限（Least Privilege） K22 變更管理 K28 密碼複雜度與安全	S19 建立帳號/密碼申請程序 S20 建立符合需求之密碼 S21 協助以安全方式配發密碼 S22 挑選與建置可管理使用者密碼，以符合要求之系統 S23 準備教育訓練教材 S24 執行教育訓練與宣導
	T4.3 資料傳輸安全與金鑰管理	O4.3.1 加密工具選擇與使用 O4.3.2 金鑰管理	P4.3.1 協助擬定傳輸之安全要求，例如加密強度、方式與加密設備之使用 P4.3.2 依需求協助選擇與建立安全通道機制與產品（例如 SSL	4	K29 密碼學 K30 金鑰使用與管理 K31 安全通道相關知識	S25 協助建立資料傳輸規範 S26 協助選擇並建置符合需求強度之加密方式、設備 S27 安全保管金鑰 S28 金鑰更新

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
			VPN） P4.3.3 協助金鑰發放 P4.3.4 協助金鑰保管 P4.3.5 協助更新金鑰			
	T4.4 行動裝置與物聯網安全	O4.4.1 行動裝置安全管控 O4.4.2 物聯網安全	P4.4.1 了解行動裝置安全議題 P4.4.2 協助建立行動裝置安全管控機制 P4.4.3 了解物聯網安全議題 P4.4.4 協助建立物聯網管控機制	4	K32 行動裝置特性 K33 行動裝置弱點與威脅 K34 物聯網身分認證 K35 物聯網加密技術 K36 物聯網弱點與威脅	S29 了解行動裝置弱點、威脅與攻擊手法 S30 協助建立行動裝置安全管控機制 S31 了解物聯網系統弱點、威脅與攻擊手法 S32 協助建立物聯網安全管控機制
	T4.5 弱點管理	O4.5.1 系統、網路、資安設備、終端、行動裝置、資料庫、應用程式等弱點資訊 O4.5.2 弱點通報 O4.5.3 弱點修補紀錄或補償管控措施	P4.5.1 即時蒐集系統、網路、資安設備、終端、資料庫、行動裝置、應用程式等弱點資訊 P4.5.2 通報相關使用者、管理員相關資訊 P4.5.3 定期執行弱點掃描、滲透測試 P4.5.4 協助管理人員修補與追蹤相關弱點，並對無法修補之部分採行必要之補償措施並追蹤執行結果	4	K37 威脅、脆弱性 K38 駭客攻擊手法與對策 K39 弱點掃描工具使用 K40 滲透測試之理論、實作與工具使用 K41 弱點、漏洞之修補 K42 補償措施之選擇	S33 即時蒐集各類脆弱性、攻擊手法相關資訊並通報相關人員 S34 弱點掃描工具選擇與使用 S35 弱點掃描結果之分析與產製報表 S36 於不影響維運之狀況下，執行滲透測試 S37 滲透測試結果之分析與產製報表 S38 各種弱點、漏洞之修補 S39 協助管理人員針對無法修補之弱點與漏洞，提出適當之補償措施
	T4.6 程式碼弱點管理	O4.6.1 程式原始碼掃描紀錄 O4.6.2 程式碼修補紀錄	P4.6.1 協助執行程式原始碼掃描 P4.6.2 協助解釋程式原始碼掃描結果與追蹤修改作業	4	K42 補償措施之選擇 K43 程式語言概念 K44 原始碼弱點、漏洞之修補	S40 原始碼掃描工具選擇與使用 S41 執行原始碼掃描與產製報表 S42 針對無法修補之弱點與漏洞，提出適當之補償措施之建議
	T4.7	O4.7.1 無線網路定期	P4.7.1 定期掃描各區域之無線網	3	K45 無線網路安全性	S43 定期檢查實體區域、機房、設備之

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
	無線網路管理	掃描與處理紀錄 O4.7.2 系統、終端之無線網路使用檢查紀錄 O4.7.3 無線網路認證與傳輸加密機制之選擇與建立	路使用狀況 P4.7.2 定期檢查系統、終端是否連接無線網路 P4.7.3 協助擬定無線網路使用之認證方式與傳輸加密強度		K46 無線網路加密方式 K47 無線網路認證方式 K48 無線網路掃描工具之使用	無線網路使用狀況 S44 協助選擇與建立無線網路設備與認證、加密之機制
	T4.8 協助備份之執行與有效性確認	O4.8.1 備份執行紀錄 O4.8.2 備份有效性確認紀錄	P4.8.1 協助各系統、設備管理人員，選擇合適備份方式 P4.8.2 協助各系統、設備管理人員，建立備份機制 P4.8.3 協助確認備份執行之有效性（例如還原測試或無法直接還原測試時，進行可讀性測試）	3	K49 備份原理 K50 備份方式之特性與優缺點 K51 備份工具之使用 K52 備份還原測試方式之優缺點與風險	S45 協助備份失敗之處置 S46 協助定期還原測試或備份資料有效性檢查
	T4.9 公開資訊與網頁安全	O4.9.1 網頁監控紀錄 O4.9.2 網頁安全定期掃描紀錄	P4.9.1 建立網頁監視機制 P4.9.2 定期網頁弱點掃描並進行必要修補	4	K42 補償措施之選擇 K53 網頁攻擊手法與防禦 K54 網頁監控技術 K55 網頁弱掃與修補	S47 建立網頁安全監控機制，至少包括置換與攻擊警告 S48 持續監控網頁並進行必要處置 S49 定期網頁弱點掃描 S50 協助進行修補或選擇補償措施
	T4.10 委外管控	O4.10.1 委外合約（含明文之安全要求事項） O4.10.2 委外監督紀錄	P4.10.1 協助合約管理單位，於合約中納入必要之安全要求項目 P4.10.2 協助合約管理單位，針對合約之安全相關項目，監督委外廠商之合約履行並留存紀錄	3	K56 了解合約管理單位相關業務之安全議題	S51 識別並於合約中制定所有安全要求 S52 協助監督第三方履約並留存紀錄
T5 日誌收	T5.1 稽核日誌設定	O5.1.1 稽核日誌設定準則	P5.1.1 協助各管理人員，制定系統、網路、資安與終端設備稽核	4	K57 設備事件定義 K58 系統、網路、資安與終	S53 協助確認維運所需注意之系統事件 S54 了解如何於不同系統、網路、資安

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
容、分析與監控		O5.1.2 稽核日誌設定紀錄	日誌啟動之準則（包括對管理者與使用者之行為） P5.1.2 依據準則，設定系統、網路、資安		端稽核日誌設定	與終端設備啟動上述稽核日誌
	T5.2 收容與保護稽核日誌	O5.2.1 日誌收容紀錄	P5.2.1 建立稽核日誌保護機制，例如資安監控中心（SOC）或日誌伺服器 P5.2.2 協助各管理人員，依特性進行系統、網路、資安與終端設備稽核日誌收容，例如 syslog 外拋，或主動連接 Database	4	K59 了解網路、系統、設備事件意義 K60 日誌保護機制，如防竄改方式 K61 維運與法規對紀錄留存之要求 K62 SOC/日誌收容系統建置 K63 SOC/日誌收容系統維運	S55 依業務、法規需求，決定需留存紀錄之日誌時間 S56 建立 SOC/日誌收容機制 S57 維運 SOC/日誌收容系統
	T5.3 日誌分析與通報	O5.3.1 監控日報/月報表 O5.3.2 通報記錄	P5.3.1 分析需求，建立關聯分析規則 P5.3.2 依據關聯分析規則進行判斷 P5.3.3 事件與事故通報	4	K13 Transmission Control Protocol / Internet Protocol (TCP/IP) K14 網路路由（Network Routing） K15 網路服務（Domain Name System, DNS、Dynamic Host Configuration Protocol, DHCP、Server Message Block, SMB、Network Time Protocol, NTP 等）	S58 分析單一事件 S59 交叉關聯分析異質事件 S60 判定攻擊是否成功 S61 即時依程序通報
	T5.4 時間同步	O5.4.1 選定時間同步源 O5.4.2 時間同步設定	P5.4.1 協助決定共同時間同步源 P5.4.2 協助各管理人員，設定系統、網路、資安與終端設備之時	2	K66 時間同步協定(Network Time Protocol, NTP)	S62 協助選定單一時間同步源 S63 協助各管理人員，設定系統、網路、資安、終端設備之時間同步機制

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
		與定期檢查紀錄	間同步 P5.4.3 協助各管理人員，定期檢視設定是否正常運作			S64 定期確認時間同步正常運作
T6 雲端安全管理	T6.1 雲端維運安全管理	O6.1.1 各項雲端服務、系統維運安全管控紀錄	P6.1.1 了解雲端架構 P6.1.2 協助相關人員，進行雲端維運相關安全管理	4	K67 雲端運算架構框架 K68 雲端資料安全 K69 雲端身分認證與存取管理 K70 雲端服務供應商管理 K71 雲端資料中心維運 K72 雲端應用程式安全 K73 雲端事故回應、緊急應變	S65 具備雲端架構概念 S66 維運雲端系統與服務 S67 雲端事故應變處理
T7 資訊安全事故通報、緊急應變及營運持續管理	T7.1 事故通報與期初處理	O7.1.1 事故通報紀錄 O7.1.2 事故期初處置紀錄	P7.1.1 協助各管理人員，建立事故偵測與通報機制 P7.1.2 協助事故期初處置，以減少中斷時間	3	K74 事件、事故定義 K75 事故偵測 K76 事故分類與通報 K77 事故期初處置（Initial Support） K78 補償措施	S68 建立可即時偵測事故發生之機制 S69 協助事故發生單位，即時記錄事故並進行分類 S70 協助事故發生單位，依事故類型盡速進行期初處置，以減少中斷與避免事故擴大
	T7.2 事故分析與修復	O7.2.1 事故分析結果 O7.2.2 事故處理紀錄	P7.2.1 協同事故相關人員，針對事故發生原因，進行評估與分析 P7.2.2 協助事故相關人員，進行必要處置，並盡速恢復運作	3	K79 事故分析與評估 K80 事故修補與復原	S71 協助相關人員進行事故評估與原因分析 S72 協助事故發生單位，進行事故修補，以回復系統運作
	T7.3 事故鑑識與證據留存	O7.3.1 事故鑑識紀錄與相關處理紀錄	P7.3.1 必要時，協助隔離事故區 P7.3.2 協助保存必要之證據（含數位）以作為相關法律議題處理之依據	4	K81 數位鑑識 (Digital Forensic) K82 數位證據留存	S73 協助事故發生單位，判斷是否需留存可能之入侵、犯罪資料 S74 協助事故發生單位，留存法庭上可作佐證之數位與非數位證據

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
	T7.4 由事故中學習與實施預防措施	O7.4.1 事故根因分析結果 O7.4.2 事故矯正改善紀錄	P7.4.1 協助事故發生單位，進行根因分析 P7.4.2 協助事故發生單位，提出矯正改善措施，並確認有效性	4	K83 根因分析 K84 改善、矯正措施 K85 有效性審查	S75 協助事故發生相關人員，進行根因分析 S76 依據根因，協助事故發生單位提出矯正與改善措施 S77 協助審查矯正改善措施之有效性
	T7.5 備援機制規劃與實作	O7.5.1 備援機制	P7.5.1 協助各管理人員，建立備援系統與備援機制	4	K86 備援機制	S78 協助各管理人員，選擇符合需求之備援方式 S79 協助各管理人員，建立備援機制
	T7.6 緊急應變與營運持續 練與改善	O7.6.1 緊急應變計畫書 O7.6.2 營運持續計畫書	P7.6.1 協助分析可能造成需啟動緊急應變與營運持續之事故 P7.6.2 協助各管理人員，撰寫緊急應變計畫書	4	K87 營運衝擊分析 K88 風險評估 K89 緊急應變 K90 營運持續作業方式	S80 依據營運衝擊分析結果，進行風險評估 S81 識別所有可能造成過長中斷時間之事故、威脅
	T7.7 緊急應變與營運持續演	O7.7.1 營運持續演練計畫 O7.7.2 演練紀錄 O7.7.3 演練檢討與改善紀錄	P7.7.1 協助各管理人員，撰寫各系統、設備之各情境應變作業程序 P7.7.2 協助依時程演練並進行檢討與改善	4	K89 緊急應變 K91 系統、網路還原與處置 K92 營運持續演練方式	S82 協助各管理人員，撰寫緊急應變計畫 S83 協助各管理人員演練，及討論演練結果並實施必要之改善
T8 法規遵循	T8.1 識別適用法規	O8.1.1 適用法規清單	P8.1.1 尋求法務單位協助，識別所需遵循相關法規	3	K93 法規識別	S84 了解所屬產業與日常作業需遵循的相關法規 S85 定期更新法規資訊
	T8.2 個人資料保護與智慧財產權	O8.2.1 個資保護作業相關紀錄 O8.2.2 智慧財產遵循檢查紀錄	P8.2.1 協助作業單位，確保維運作業對個人資料蒐集、處理、利用時，皆需符合個人資料保護法 P8.2.2 宣導與協助各單位，資料、音樂、圖片、軟體等使用需符合著作權法	4	K94 個人資料保護法與施行細則 K95 個人資料蒐集、處理、利用 K96 智慧財產權 K97 授課技巧	S86 識別所有涉及個資作業之流程 S87 確認相關個人資料之蒐集、處理與利用，皆符合個資法 S88 資料、音樂、圖片、軟體等使用，皆需符合智慧財產權並定期檢查確認。 S24 執行教育訓練與宣導

工作職責	工作任務	工作產出	行為指標	職能級別 4	職能內涵 (K=knowledge 知識)	職能內涵 (S=skills 技能)
	T8.3 獨立稽核與遵循性檢查	O8.3.1 稽核作業紀錄 O8.3.2 遵循性檢查紀錄	P8.3.1 協助執行稽核，並確保獨立性 P8.3.2 協助定期確認法規遵循性	4	K98 稽核 K99 法規遵循	S89 定期規劃與執行獨立稽核作業 S90 定期確認所有作業遵循所識別之法規
T9 教育訓練	T9.1 資安意識與認知宣導	O9.1.1 資安意識與認知宣導教育訓練教材 O9.1.2 社交工程演練訓練教材 O9.1.3 教育訓練紀錄	P9.1.1 協助準備資安意識與認知宣導教育訓練教材 P9.1.2 協助執行資安意識與宣導教育訓練 P9.1.3 協助執行社交工程演練（例如電子郵件測試）並留存紀錄	3	K97 授課技巧 K100 資訊安全認知 K101 社交工程手法	S23 準備教育訓練教材 S24 執行教育訓練與宣導 S91 執行社交工程演練
	T9.2 職能教育訓練	O9.2.1 協助辦理資安作業相關技能教育訓練 O9.2.2 教育訓練紀錄	P9.2.1 協助準備執行資安作業所需技能教育訓練教材 P9.2.2 協助執行資安作業所需技能教育訓練	3	K97 授課技巧 K102 資安作業相關安全知識	S23 準備教育訓練教材 S24 執行教育訓練與宣導

職能內涵（A=attitude 態度）
A01：溝通協調能力 A02：獨立 A03：細心謹慎 A04：彈性 A05：執行力 A06：正直 A07：自我管理 A08：自主學習 A09：抗壓性 A10：冷靜思考

職能內涵（A=attitude 態度）
A11：問題分析 A12：堅忍 A13：守法

說明與補充事項
● 建議擔任此職類/職業之學歷/經歷/或能力條件： 1.大學或專科以上學歷，或具有資訊安全相關背景，資訊或電機相關科系尤佳。 2.具備英文閱讀能力，具跨領域學習特質者尤佳。