

法務部及所屬機關人員資訊安全管理規範第三點 修正對照表

修正規定	現行規定	說明
<p>三、辦理資訊安全應注意事項</p> <p>(一) <u>明確界定本部及所屬機關資訊工作相關人員及廠商人員的資安角色、責任與所需能力，並於資訊作業委外時明確規範於契約中，使相關人員均能清楚認知其安全責任與符合職務需求。另對委外廠商及其相關人員之資訊安全約束依法令及契約等相關規定辦理。</u></p> <p>(二) 本部及所屬機關人員應依相關法規負保守公務機密之義務，對於其主管與非主管事務之機密性與敏感性資訊，均不得洩漏，退(離)職後亦同。</p> <p>(三) 委外廠商駐點服務人員、專責維護人員，或在本部及所屬機關停留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結本部網路者為限）及經常至本部及所屬機關資訊單位洽公之業務人員，均應簽署保密切結。</p> <p>(四) 資訊作業工作職責為可存取機密性與敏感性之資訊或系統者，</p>	<p>三、辦理資訊安全應注意事項</p> <p>(一) 對委外廠商及其相關人員之資訊安全約束依法令及契約等相關規定辦理。</p> <p>(二) 本部及所屬機關人員應依相關法規負保守公務機密之義務，對於其主管與非主管事務之機密性與敏感性資訊，均不得洩漏，退(離)職後亦同。</p> <p>(三) 委外廠商駐點服務人員、專責維護人員，或在本部及所屬機關停留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結本部網路者為限）及經常至本部及所屬機關資訊單位洽公之業務人員，均應簽署保密切結。</p> <p>(四) 資訊作業工作職責為可存取機密性與敏感性之資訊或系統者，於任務指派前應經適當安全評估程序，並應加強工作評估及考核。</p> <p>(五) 重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立管控機制，</p>	<p>為符合新版 ISO/IEC 27001:2013 標準本文 5.3 組織角色、責任及權限與 7.2 能力之要求，爰修正第一款規定。</p>

<p>於任務指派前應經過適當安全評估程序，並應加強工作評估及考核。</p> <p>(五) 重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立管控機制，實施人員輪調，建立人力備援制度。</p> <p>(六) 各級主管應督導所屬人員妥為辦理資訊作業，以確保資訊安全，防範不法及不當行為。</p> <p>(七) 資訊作業人員於調離職時應辦理資訊資產交接或歸還，並應立即辦理權限異動或帳號移除。</p>	<p>實施人員輪調，建立人力備援制度。</p> <p>(六) 各級主管應督導所屬人員妥為辦理資訊作業，以確保資訊安全，防範不法及不當行為。</p> <p>(七) 資訊作業人員於調離職時應辦理資訊資產交接或歸還，並應立即辦理權限異動或帳號移除。</p>	
---	---	--