

## 網絡基建及營運之能力單元

1.名稱	釐定網絡安全政策
2.編號	ITCSNO529A
3.應用範圍	在沒有安全政策的情況下，網絡可能被駭客，欺詐用戶，低劣工藝(如路由器和交換設備配置錯誤)所危害。這些都會給網絡支援團隊帶來各種問題，同時業務也一定會受到影響。安全政策應從網絡的風險評估做起，成立團隊以便應對。本能力單元說明釐定網絡安全政策的能力。
4.級別	4
5.學分	3
6.能力	<p style="text-align: center;"><u>能力單元</u></p> <p>6.1 具備有關知識</p> <ul style="list-style-type: none"> <li>● 在公司政策的制定機制和業務需求上，具備廣博的知識</li> <li>● 具備公司安全政策的知識</li> <li>● 在電訊監管的要求，特別是有關安全方面，具備廣博的知識</li> <li>● 在網絡基建及其支援的所有服務上，具備經驗</li> <li>● 在安全原則和最佳做法上，具備廣博的知識</li> <li>● 在分析和確認各種安全風險上具備專家水平，包括可能的攻擊方法，如針對訊號層、用戶資料庫、網絡元素、網關、詐騙和服務中斷等</li> <li>● 在健康和安全的規例和危害上，具備知識</li> </ul> <p>6.2 釐定網絡安全政策</p> <p>能夠：</p> <ul style="list-style-type: none"> <li>● 透過確認網絡基建及其組成部分的資產，威脅和漏洞，來分析網絡的安全風險</li> <li>● 按照對業務的重要性，排列資產的先後次序</li> <li>● 確認公司資產會面臨的威脅和風險，如：未經授權的存取/資源的運用（身份驗證）、拒絕服務（可用性）、資料洩漏（保密性）、數據毀壞/未經授權擅自對數據作出改動（完整性）、自然災害等</li> <li>● 評估不同的風險處理方法</li> <li>● 按照下列因素將風險分類：必須盡量減少/消除，應盡量減少/消除或可接受</li> <li>● 為3類風險計劃合適的安全機制（實行什麼措施，如何有效地進行監督），並確保其符合公司的政策</li> <li>● 記錄安全政策，包括檢討時間表</li> <li>● 向適當的持份者分發政策文檔，以便實施和執行，如：保安主任、NOC(網絡操作中心)、網絡工程師、服務台等</li> </ul> <p>6.3 展示專業能力</p> <ul style="list-style-type: none"> <li>● 確保政策以非技術人員可以理解的方式編寫，並符合公司的標準</li> <li>● 時刻注意各相關的技術，政治，社會，環境和法律因素，並從中取得適當的平衡</li> </ul>
7.評核指引	<p>此能力單元的綜合成效要求為：</p> <ol style="list-style-type: none"> <li>i. 理解公司的安全政策，並把這些安全上的需求納入制定的網絡安全政策中</li> <li>ii. 確認風險，並把與網絡有關的風險分類</li> <li>iii. 制定合適的風險緩解程序，以處理不同類別的風險</li> <li>iv. 把緩解程序有效地轉化成網絡安全政策</li> <li>v. 向持份者傳達政策，讓他們理解，並採取適當的措施，如：審批、簽收、實施</li> </ol>

	和執行
備註	