

資訊科技及通訊業標準說明  
能力單元

1. 名稱	訂定保安操作上的保護程序
2. 編號	ITSWOS522A
3. 應用範圍	為機構的資訊科技操作提供保安管理服務時，按照保安控制政策，訂定保安控制的程序，以保護系統免受安全威脅 [營運與支援 - 保安管理服務]
4. 級別	5
5. 學分	2
6. 能力	<p style="text-align: right;"><u>表現要求</u></p> <p>6.1 瞭解保安控制的要求和安全威脅的種類</p> <p style="padding-left: 20px;">有能力的</p> <ul style="list-style-type: none"> <li>▪ 領悟保安政策和管理層的指引</li> <li>▪ 理解保安控制計劃</li> <li>▪ 確定對業務程序的各種安全威脅</li> </ul> <p>6.2 訂定程序以保護基礎建設免受安全威脅</p> <p style="padding-left: 20px;">有能力的</p> <ul style="list-style-type: none"> <li>▪ 訂定程序和措施以保護基礎建設免受安全威脅</li> <li>▪ 推薦適當防毒軟件(識別標誌)和保安修補檔</li> </ul> <p>6.3 按照保安控制政策，監督、調查和執行糾正行動</p> <p style="padding-left: 20px;">有能力的</p> <ul style="list-style-type: none"> <li>▪ 監督警報和異常回報</li> <li>▪ 調查警報以決定根由</li> <li>▪ 按照保安控制政策，實行糾正行動</li> </ul> <p>6.4 以專業方式按照保安控制政策，訂定保安控制程序</p> <p style="padding-left: 20px;">有能力的</p> <ul style="list-style-type: none"> <li>▪ 以現有安全威脅的資訊，尋找可靠的支援資源，以協作和互相支援</li> <li>▪ 運用行內最佳做法，並緊貼本地及國際標準</li> <li>▪ 依從機構內部指引和程序以及任何適用的(包括本地及國際)法律和監管要求</li> </ul>
7. 評核指引	上述能力單元之綜合能力要求為 (i) 訂定程序以保護基礎建設免受安全威脅，並且 (ii) 按照保安控制政策監督、調查和執行糾正行動
備註	1. 安全威脅的例子包括，但不限於，病毒突襲，未經批准的闖入和保安缺口。

2. 假設參與者具備廣泛的資訊科技及其應用知識.
3. 上述能力單元包含 ITIL®保安管理服務的計劃和操作基礎建環境的保安服務