Functional Area: Network Infrastructure & Operation (Security)

1. Title	Implementing controls to prevent cable tampering	
2. Code	ITCSNO335A	
3. Range	Cable tempering is not just concern with physical tampering to gain access or creating disruption to networks. In today's environment, with VOIP, operators are also concern on protecting data/information that transmitted on the cable. This UoC describes the competencies for implementing appropriate controls to prevent cable tampering. The type of controls implemented depends on type of cable (copper or fibre) selected and level of protection required. It could be just a simple label seal at the cable closet or a sophisticated monitoring sensor device.	
4. Level	3	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Possess the knowledge in the subject area	• Possess extensive experience with data communication concepts and how data is transmitted on cables • Possess extensive knowledge of cable and cabling standards like EIA/TIA 568, 569, etc • Possess extensive experience with network cable security principles and types of risks exist • Comprehend network plans • Experienced with cabling tools and use of cable marking systems • Possess extensive knowledge of new cable technologies and security controls to mitigate risks, such as sensors, fibre vibration detectors, etc • Knowledgeable of the organisation security policies
	6.2 Implementing controls to prevent cable tampering	Be able to: • Determine from work orders or supervisors the cabling job requirements • Study site plans or carry out site visits to evaluate where cables would be suspected to tampering, including cable box, closet, the cable, etc • Evaluate various options and identify the most suitable control to use, such as label seals on cable box, cables with built in sensors that detect tampering, cables completely protected within conduits, deep conduits, etc • Install the controls as per required by the job order, vendor product instruction, or the organisation procedures • Fully document the implementation steps with network diagrams showing where controls are placed and how. For complex controls fuller details may be required such as: triggers start, end and the monitoring threshold, etc. Extra user procedures will be required for any internally developed monitoring equipment/software • Ensure various stakeholders receive copies of the document for approval and file in accordance with the organisation standards and procedures
	6.3 Exhibit professionalism	• Follow safety procedures at every step • Follow the security policies of the organisation to prevent unauthorised access of the network and comply with the industry and regulatory standards

7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: i. read job orders or follow supervisor's instructions to understand the set up of cabling control requirements ii. install the anti-tampering controls in accordance with the vendor or the organisation standard policies and procedures iii. fully document the installation work and seek work completion signoff from stakeholders
Remark	