**Functional Area: Network Infrastructure & Operation (Security)**

| | | |
|---|---|---|
| 1. Title | Define requirements to ensure data is transmitted confidentially and with integrity | |
| 2. Code | ITCSNO434A | |
| 3. Range | One of the network security considerations is to ensure data is transmitted without loss of security. This UoC describes the competencies for defining requirements to ensure data is transmitted securely. “Securely” implies confidentiality and integrity. Data transmission security can be implemented at all layers of the OSI (Open Systems Interconnect) reference model, but this UoC limits security at above layer 3 of the model. | |
| 4. Level | 4 | |
| 5. Credit | 3 | |
| 6. Competency | | Performance Requirement |
| | 6.1 Possess the knowledge in the subject area | • Possess extensive knowledge of the organisation security policy<br>• Possess extensive experience with the network infrastructure, data transmission techniques and security implementation at different layers of the OSI reference model<br>• Possess extensive knowledge of security principles, security trends, mitigation techniques, implementation of controls and best practices<br>• Expert in various data security risks, such as packet spoofing, snooping, network intrusion, etc<br>• Expert in network vulnerability analysis, such as penetration testing, Nmap, snort, etc<br>• Possess extensive experience with various network and data protection technologies, such as IPsec, Firewall, IPS/IDS (Intrusion Protection Systems/ Intrusion Detection Systems), VPN, etc.<br>• Knowledgeable of various data encryption techniques<br>• Knowledgeable of health and safety rules and hazards. |
| | 6.2 Define requirements to ensure data is transmitted confidentially and with integrity | Be able to:<br>• Work with stakeholders (internal or external customers) to identify the level of data transmission security required.<br>• Analyse the network infrastructure, the operation centre to identify the possible type of risks which the stakeholders are exposed to<br>• Group and map the risks to the OSI reference model<br>• Define the types of security protection to be applied for each layer while transmitting the data such as: set on IPsec at network layer, use of data encryption application at application layer, etc<br>• Identify what equipment can be used to monitor and alert security breach relating to data integrity and confidentiality to meet the protection required by the stakeholders. Such as anti-spyware, intrusion detection/prevention devices, etc<br>• Document the protection requirements with the type of protection to apply and distribute to the stakeholders<br>• Present the proposal to stakeholders for acceptance and implementation |
| | 6.3 Exhibit professionalism | • Ensure the defined protections are inline with the organisation’s security policy<br>• Always take into consideration and strike a proper balance among all related technological, environmental and legal factors |

| | |
|---|---|
| 7. Assessment Criteria | The integrated outcome requirements of this UoC are the abilities to:<br>i. communicate and work effectively with stakeholders to determine the different types and levels of transmission security requirements<br>ii. differentiate and associate the security requirements with the OSI reference model so that appropriate security protection can be determined such as application security, network security, physical security, etc<br>iii. formulate the type of applications, equipment, or tools used to enable transmission is performed securely and monitoring of the transmission security is not breached<br>iv. effectively document and present the protection proposal to stakeholders and seek approval for implementation |
| Remark | |