Unit of Competency

Functional Area: Security Support

Title	Administer basic website security
Code	107889L3
Range	This unit of competency applies to support personnel who are responsible to administer security of the organisation’s website under the direction of supervisor. The server on which the website resides on, either locally or remote hosted should be protected from hackers, virus, unauthorised access, hijacked. Monitor and validate the web page, scripts, SQL commands used does not have vulnerabilities for malicious attacks which can affect the organisation’s network or systems or theft of the organisation’s business data.
Level	3
Credit	6
Competency	Performance Requirements 1. Knowledge for administer basic website security • Knowledge of different website security risks and the importance of website security protection • Understand the use of website security audit tools • Possess a broad knowledge of server and network security • Possess good knowledge of the organisation’s security requirements and policies • Possess good knowledge of website protection technologies and trends • Possess good knowledge of installing and configuring hardware and software 2. Administer basic website security • Work with the supervisor to identify the security needs of the organisation’s website, including but not limited to the following: • Website functionality • Access requirement of transactions, visitors and users • Operating Systems weaknesses • Secure the server of the website with installation of site certificate, regular system patches and updates, antivirus, anti-spyware protection and updates • Configure web server securely with required functionality and features only • Secure website transactions with encryptions • Set access control of server and database to those needed access only • Work with website content development team to ensure scripts and web applications are vulnerabilities free • Regularly use monitoring and audit tools to test and monitor vulnerabilities of the website • Perform regular offline backup of the website • Continue to develop or help to secure procedure to secure the organisation’s website that comply with the organisation security requirements 3. Exhibit professionalism • Committed to protect the organisation’s assets • Exhibit security attitude but balance the business needs against the security need when administering the website security • Well versed with industry network security best practices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Secure the organisation’s website that complied with the organisation’s requirement • Use audit and monitoring tools to reduce the website vulnerabilities • Set the correct level of network access for users in accordance with the organisation procedure
Remark	