Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

Functional Area - Information Security

Title	Develop information security standard, policies and guidelines for the organization
Code	111164L6
Range	This UoC applies to the arrangements and procedures relating to the establishment of information security policies for the organization. This step is to ensure that all staff members have standards to follow and protect the organization from cyber attack, unauthorized access, alteration, unauthorized disclosure, etc.
Level	6
Credit	6 （For Reference Only）
Competency	Performance Requirements 1. Possess the knowledge in the information security area • Realise the necessity in the establishment of a set of information security policies to be embedded into the organization • Recognise the changes in cyber technology in the organization’s related industries, and apply the knowledge to analyse future trends and developments in information security threats and measures based on incomplete information collected from different sources • Understand the compliance requirements and based on that to determine regulatory requirements and obligation under different jurisdictions • Understand the business requirements of key stakeholders and analyse views collected from different business and operation units accurately to discern their needs in IT control or security 2. Develop relevant standard, policies and guidelines • Establish strategic objectives and compliance position for information security of the organization to provide protection with an outlook of future perspective • Establish IT control or security (e.g. network) policies with respect to the organizations business strategies and security needs • Ensure the information security policies and guidelines are established correctly, positioned at the appropriate level, and comprehensive enough for employee to follow 3. Develop professional behaviour and attitude • Direct communication and training programs on information security measures; ensure all levels of staff are aware of their importance and participate in the protection of information security • Ensure all information security policies established comply to all existing legal and regulatory requirements as well as social concerns • Design monitoring measures to ensure compliance with established security policies
Assessment Criteria	The integral outcome requirements of this UoC are: • Formulation of security policies. The policies should be based on critical analysis of a broad range of data and incomplete information with the aim to provide enough protection to organizations’ IT systems and meet the regulatory requirements without hampering operational efficiency • Production of supporting measures on enforcing security policies. Comparison of different types of security measures should be provided to support the design.
Remark	