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

Functional Area - Operations Management

Title	Observe information security
Code	108013L2
Description	This unit of competency applies to all Digital Media Technology (DMT) practitioners. Digital media personnel are no different to other digital information users. Hence, like other digital information users, they need to observe all rules and procedures layout by the organisation to safeguard all its systems, business information, and assets (digital assets).
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for observing information security: • Possess literacy skills that can understand technical and non-technical documents • Possess basic knowledge of information security concept • Possess good knowledge of the organisation's information security procedures and guideline • Possess knowledge of who and where to report security incidents 2. Observe information security: • Understand 3 pillars of information security: o Confidentiality: preventing someone from reading information they are not authorised to read. In addition, confidential information has to be protected from not just malicious people but also their agents, such as malicious software, compromised computer, or other compromised network components o Integrity: prevent information from being inappropriately modified through accidental events or malicious means such as: storage media problems, crashed or buggy programs, and noisy transmission environments can cause accidental data corruption. o Availability: ensure information is all way available which means, in case of temporary loss of information, it can be recovered from backups. Hence, backup or redundancy and speed of recovery are considered to ensure availability • Observe user identification and passwords policies, including the following : o Change password regularly o Never keep password visible to others o using only own passwords o log off applications/systems when appropriate • Observe guidelines for handling confidential data. It must be stored, transported, transmitted, handled, used, and disposed of in ways that protect the information from unauthorised access, alteration, destruction, disclosure, copying, theft, or physical damage, etc. • Observe policies to secure your device, including the following : o Install authorised software o Install anti-virus software o Install anti-spyware o Install personal firewall o Keep system updated and patches current • Observe Internet usage guidelines, including the following : o Disconnect from Internet when not needed o Real-time scan for all incoming files before opening them o Do not open emails from strangers

Functional Area - Operations Management

	○ Beware of popups, enable pop-up blockers ○ Beware of phishing • Report any or suspected Information Security incidents in accordance with the organisation procedures and guidelines 3. Exhibit professionalism • Always be updated with information security news and follow industry best practices and organisation guideline and procedures to ensure information security is maintained
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand the importance of information security and follow the organisation guidelines and procedures to safeguard the organisation business assets • Proactively report various suspected information security incidents in accordance with the organisation's procedures
Remark	1. For practitioners involved with information security responsibilities, there are a number of industry standards they should practise, such as: ISO 27000 series 2. For Hong Kong government guidelines to information security best practices, refer http://www.infosec.gov.hk