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

Functional Area - Content Security

Title	Maintain content security
Code	108066L3
Description	This unit of competency applies to all Digital Media Technology (DMT) practitioners involved with implementation of content security. To most organisation, content security is all about rights and Intellectual Property (IP) protection. This is correct. But there are many other security aspects, in-addition to Digital Rights Management (DRM), needed to be considered and be validated to maintain content security. Content security is a part of information security. Hence, this UoC will not distinguish "Pure Content" or "Pure information" security; but covers only security elements associated with protecting an organisation's digital media contents.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for maintaining content security • Possess good project management and technical writing skills • Possess in-depth knowledge of planning and implementing content security • Possess good knowledge of different types of content security and information security technology • Possess good knowledge of content security implementation methodologies • Possess good knowledge of networking and infrastructure security • Possess good knowledge of content security and IP laws of Hong Kong • Possess good knowledge of the organisation security policies 2. Maintain content security: • Evaluate the organisation's current content protect plan/design and determine areas which have or may have security exposures. Areas include but not limited to the following: o Firewall protection rules o Physical storage systems (Servers, Storage Area Network (SAN), etc.) o Network security including Virtual Private Network (VPN), transport layer security, etc. o Cyber-attack protections • Review user's credential/authentication and registration system on website and web applications to ensure all the required authentication elements are properly implemented and functioning as stipulated by the security policy. Examples of elements include: o Username, password o Personal identifiable information o Answers to security questions/challenges o CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) o Server scripting cannot be compromised by Structured Query Language (SQL) injection • Review on contents protection mechanisms which are being applied during the production stage, such as: o Watermarking o Encryption o Rights/geo-location access have been set • Review the organisation's hybrid cloud security when storing contents in the cloud and ensure the following:

Functional Area - Content Security

	○ Sensitive contents/documents held on mobile devices are encrypted ○ Contents on cloud store are encrypted ○ Contents transmitted across networks are encrypted. For example: delivery systems • Review the DRM/Digital Asset Management (DAM) system, certificate systems, delivery systems to ensure they are properly configured and all contents are handled encrypted, and are delivered to the correct stakeholder (user, customer, staff, etc.) • Review backup and recovery mechanisms and procedures; ensuring they are in place and well setup. Staff are well rehearsed and prepared for emergencies • Review security monitoring, ensuring that it can alert/highlight any security abnormalities. e.g. web page • Review security escalation, handling and other contents security procedures to determine if they are current and effective • Document the findings and areas for probable enhancement. If necessary, present to management. Also schedule future reviews 3. Exhibit professionalism • Apply industry best practices to protect the organisation's digital contents either on premise or at the cloud. Example of best practices: ISO 27000 standards family
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Identify and review security components that are associated with protecting digital contents • Perform review of the content security to ensure it is systematically and methodically in layered or onion manner • Perform a complete review of all the organisation's content security and able to deliver a complete report of any security exposures that needed to be reinforced
Remark	