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

Functional Area - Content Security

Title	Develop content security practices and procedures
Code	108067L3
Description	This unit of competency applies to all Digital Media Technology (DMT) practitioners involved with implementation of content security. Content can be captured/created in multiple ways and published via multiple avenues. It can be dynamically repurposed, tailored to individual consumers/users. Good content management practices that can balance access and risk are needed to ensure digital contents are well controlled and protected.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for developing content security practices and procedures
	• Possess good project management and technical writing skills
	• Possess in-depth knowledge of developing security and operating procedures
	• Possess in-depth knowledge of different types of content protection systems, such as:
	  o DRM (Digital Rights Management)
	  o DAM (Digital Asset Management)
	  o Encrypted Media Extension
	  o Content Distribution Systems
	• Possess good knowledge of content management methodologies
	• Possess good knowledge of content security and Intellectual Property (IP) laws of Hong Kong
	• Possess good knowledge of the organisation documentation standards
	
	2. Develop content security practices and procedures
	• Comprehend the organisation's content protecting and security strategy to form a protection mapping of different categories of contents
	• Review the content protection systems and technologies that currently operating in the organisation, including but not limited to the following:
	  o DRM and DAM systems
	  o SSL (Secure Socket Layer), SHA (Secure Hash Algorithms), TLS (Transport Layer Security) security
	  o Watermarking
	  o Dynamic adaptive streaming over HTTP (DASH)
	• Define the scope/objectives of the procedure and target reader, for example:
	  o Defining access control
	  o Defining basic encryption protection
	  o Configuring content security management systems
	  o Handling infringements
	• Define actions for the procedure. For Example:
	  o Defining video access control
	  ▪ Allow viewing by tokens generated by certain defined players
	  ▪ Accept tokens from defined geographical area
	  ▪ Deny access, even with valid token, where IP address is anonymised
	• Define registration and enrollment requirements, setting and configurations for security systems, such as:
	  o User ID - minimal length
	  o Password - minimal length, validation characters

Functional Area - Content Security

	○ Double validate - Use of CAPTCHA check (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) ○ Email address - to confirm registration • Define actions to take when security system flags illegal content access or infringements/security breaches are detected. Also, define escalation structure with roles and responsibilities • Organise briefing sessions to introduce and test the procedure with stakeholders and receive comments to enhance procedure, if appropriate 3. Exhibit professionalism • Committed to develop procedure that can provide precise instructions to reader at the correct level without any miscommunication
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Develop a procedure at the correct level that can give precise and concise details and required actions to stakeholders to protect the organisation's contents • Develop the procedure that reflects the scope of the procedure and achieve its objective • Develop the procedure that complied with the organisation's format and documentation standards
Remark	