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

Functional Area - Content Security

Title	Establish content security policies
Code	108063L5
Description	This unit of competency applies to all Digital Media Technology (DMT) practitioners responsible for digital content security. For digital media publishers, organisation contents is their bread and butter; they would make sure those content's intellectual property is not stolen or illegally reproduced. But with the volume of content, the speed of creation and the reach of collaboration, accidental content exposure, purposeful content leakage and piracy are creating challenges. A clear policy is needed for the organisation to how the contents can be shared, accessed with minimal risk of security.
Level	5
Credit	5
Competency	Performance Requirements 1. Knowledge for establishing content security policies • Possess good project management and policy formulation skills • Possess in-depth knowledge of information and cyber security • Possess good knowledge of digital media security • Possess in-depth knowledge of Digital Rights Management (DRM) • Possess good knowledge of laws and regulations related to information and cyber security, especially Internet laws of Mainland China when operating in the Mainland • Possess good knowledge of content security and content development lifecycle 2. Establish content security policies • Study and identify best approach in content security that is suited to the organisation: o Network-centric approach to content security concerns mainly: ▪ Authentication and authorization ▪ Firewalls (perimeter security) ▪ Servers ▪ Networks ▪ Operating systems o Object(Document)-centric approach to content security concerns: ▪ Metadata associated with each content object ▪ Versioning and changes are tracked • Conduct a content review, how the contents are handled, transported, internally and externally, etc. • Categorise contents, evaluate risks and develop policies and procedures across all content, at any level, in context: o Document management o Web content management o Workflow/BPM (Business Process Management) o Enterprise rights management/Digital rights management o Identity management/User authentication o Policy-based encryption o Content authentication o Content addressed storage o Trusted time stamps o Data loss/Leak prevention o Public key infrastructure (PKI) o Digital signatures and Hierarchical storage management

Functional Area - Content Security

	• Formulate guideline for implementing tools and systems
	  ○ Metadata requirements
	  ○ Define rules and policies for access control
	  ○ Types of tools and systems to be considered, such as: DRM systems, Asset Management Systems (AMS), etc.
	  ○ Monitoring and reporting requirements
	• Human aspects
	  ○ Create and build security culture
	  ○ Develop procedures/guidelines for staff to follow and enforce training
	  ○ Ensure guidelines are easily reachable by all shareholders
	  ○ Assign responsibilities
	• Define monitoring mechanism and appropriate action to take to ensure the security policy is kept aligned with business and technology trends
	
	3. Exhibit professionalism
	• Apply industry standards and best practices when formulating and establishing security polices, such as ISO 27000 standards family
	• Always take into consideration and strike a proper balance among all related technological, political, social, environmental, business and legal factors

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Analyse and determine the most applicable content approach that matches the organisation business • Define a complete set of metadata for the organisation contents that can be used by content management tools • Develop a concise and precise content security policy that can protect the organisation asset (contents) with complete sets of guidelines for implementation which all stakeholders can adhere to
Remark	