Unit title	Investigating Information Security Incidents 2
SQA code	H7CY 04
SCQF level	8
SCQF credit points	15
SSC ref	SECINC2

History of changes

Publication date: July 2014

Version: 01

Version number	Date	Description	Authorised by

Title	Investigating Information Security Incidents 2	
Learning Outcomes **The learner will:**		**Assessment Criteria** **The learner can:**
1	Be able to prepare for Information Security incident investigations.	1.1 Interpret given incident investigation briefs to identify the scope of the incidents to be investigated. 1.2 Verify the scope of identified incidents with relevant persons. 1.3 Evaluate sources of evidence relating to identified incidents.
2	Be able to investigate Information Security incidents.	2.1 Obtain evidence relating to identified incidents, following organisational procedures. 2.2 Critically review evidence to determine appropriate investigative actions. 2.3 Make justified recommendations for investigative actions to relevant persons using media, format and structures which meet the needs of the intended audience. 2.4 Report on incident investigation following organisational procedures. 2.5 Critically evaluate organisational procedures for Incident Investigation.

Additional information about the Unit
Unit purpose and aim(s)
The conduct of information security incident investigation, following incident investigation processes. This involves undertaking investigations into information security breaches and assessing the nature of the incident and the access breach that occurred.
Details of the relationship between the Unit and relevant national occupational standards (if appropriate)
This Unit is based on the e-skills UK NOS for Information Security.
Details of the relationship between the Unit and other standards or curricula (if appropriate)
N/A
Assessment requirements specified by a sector or regulatory body (if appropriate)
This must be assessed using evidence derived from real work activities.

Assessment (evidence) Requirements
The Unit may be assessed using any appropriate methods, or combination of methods, which clearly demonstrate the learning outcomes.
Guidance on Instruments of Assessment
Learners must complete real work activities in order to produce evidence to demonstrate they are occupationally competent. An e-portfolio approach is encouraged. Simulation is allowed for aspects of the Unit specified when: • a learner is required to complete a work activity that does not occur on a regular basis and therefore opportunities to complete a particular work activity do not easily arise • a learner is required to respond to a situation that rarely occurs, such as responding to an emergency situation • the safety of a learner, other individuals and/or resources will be put at risk. Simulation must replicate the workplace to such an extent that learners will be able to fully transfer their occupational competence to the workplace and real situations.