Unit title	Investigating Information Security Incidents 1
SQA code	H7CX 04
SCQF level	6
SCQF credit points	10
SSC ref	SECINCI1

History of changes

Publication date: July 2014

Version: 01

Version number	Date	Description	Authorised by

Title	Investigating Information Security Incidents 1
Learning Outcomes **The learner will:**	**Assessment Criteria** **The learner can:**
1 Be able to gather information to investigate Information Security Incidents.	1.1 Identify the information assets and system components that may be impacted by detected incidents. 1.2 Verify the scope of detected incidents with relevant persons. 1.3 Obtain and preserve evidence relating to detected incidents.
2 Be able to investigate Information Security incidents.	2.1 Undertake agreed investigative actions. 2.2 Examine how access to the affected information assets and system components was obtained. 2.3 Report to the relevant persons any incidents for which the mode of access cannot be identified. 2.4 Make recommendations on the need for detailed forensic examinations. 2.5 Report on incident investigation activities using standard documentation. 2.6 Follow organisational procedures for investigation activities.

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 Unit 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.