Higher National Unit Specification

General information

Unit title: Data Security (SCQF level 7)

Unit code: J0H9 34

Superclass: CC

Publication date: June 2018

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this unit is to introduce learners to the principles and practice of data security, in the context of both personal and corporate data, where knowledge of preserving the integrity of digital data is of importance.

This is a **non-specialist** unit, intended for learners with an interest in this area. It is particularly suitable for learners who are undertaking an HN in Cyber Security, Computer Science or Computing Networking. However, it may also be appropriate for delivery within other group awards where there is a requirement to create, store, access and process digital data.

The unit covers the practical implications of data security and the requirements to maintain the confidentiality, integrity and availability of digital data that is created and manipulated by an organisation or entity. The unit is intended to be non-complex and involve a wide, shallow range of knowledge, which will make it appropriate for a number of group awards.

On completion of this unit, learners will be able to use their knowledge to identify potential threats and risks to digital data, and describe suitable solutions.

Outcomes

On successful completion of the unit, the learner will be able to:

1 Explain the causes and effects of data security breaches.
2 Use data security tools for personal devices.
3 Implement security measures to protect corporate data.
4 Deliver an appropriate security strategy to improve corporate data security.

Higher National Unit Specification: General information

Unit title: Data Security (SCQF level 7)

Credit points and level

1 Higher National unit credit at SCQF level 7: (8 SCQF credit points at SCQF level 7)

Recommended entry to the unit

Access to this unit will be at the discretion of the centre. This unit has been designed as a progression from *Data Security* units at SCQF levels 5 and 6, and while achievement of these would be beneficial, it is not essential.

However, it would be beneficial if learners possessed a basic understanding of IT, numeracy skills, computer security concepts, and basic browser search abilities.

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

There is no automatic certification of Core Skills or Core Skill components in this unit.

Context for delivery

This unit may be offered as standalone or as part of a group award. If the unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

The Assessment Support Pack (ASP) for this unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

Higher National Unit Specification: Statement of standards

Unit title: Data Security (SCQF level 7)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Explain the causes and effects of data security breaches.

Knowledge and/or skills

- Definition of data security breach
- Contemporary real-life examples of a data security breach
- Common causes of data security breaches
- Implications of a data security breach on both corporations and individuals

Outcome 2

Use data security tools for personal devices.

Knowledge and/or skills

- Use and importance of a robust password
- Use of encrypted e-mail
- Purpose and use of personal firewalls
- Purpose and use of an IDS (Intrusion Detection System), including the distinction between HIDS (Host-based IDS) and NIDS (Network-based IDS)
- Access Control List and typical permissions

Outcome 3

Implement security measures to protect corporate data.

Knowledge and/or skills

- Hardware security protection of host systems
- Configuration of firewalls to allow/disallow certain types of traffic
- Backup strategy and rules for storing and testing backups
- Data recovery
- Damage mitigation
- Access control list/whitelist
- Physical access protection of sensitive premises
- Biometric access measures

Higher National Unit Specification: Statement of standards

Unit title: Data Security (SCQF level 7)

Outcome 4

Deliver an appropriate security strategy to improve corporate data security.

Knowledge and/or skills

- Evaluation of security measures
- Identification of shortfalls in security measures
- Recommendations of desirable security measures
- Importance of a sound security strategy
- Pitch security strategy to a target group

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms.

1 Knowledge evidence (Outcomes 1, 2 and 3)
2 Product evidence (Outcomes 2, 3 and 4)

The **knowledge evidence** will relate to Outcomes 1, 2 and 3. This evidence is required to demonstrate that the learner can:

- Describe what a data security breach is
- Describe real-life examples of a data security breach
- Describe common causes of data security breaches
- Explain the implications of a data security breach on both corporations and individuals
- Recognise the importance of robust passwords and password policies
- Recognise the importance of secure, properly configured firewalls for personal devices
- Describe the concept of encryption for e-mails containing sensitive data
- Explain the importance of hardware security protection for personal devices, host systems and premises
- Identify the importance of a corporate firewall (network intrusion protection)
- Explain the importance of an appropriate backup strategy for critical data

This evidence may be produced over the life of the unit under loosely controlled conditions (including access to resources and reference materials). The knowledge evidence may be sampled when testing is used. When testing is used, it must be controlled in terms of location, timing and access to reference materials (not permitted). Learners are expected to demonstrate a breadth of understanding across all the knowledge statements; as a result, sampling need not be of a detailed nature.

When re-assessment is required a different test must be used on each occasion.

Evidence may be written, oral or a combination of both. Evidence may be captured and stored across a variety of media, including both audio and video. Particular consideration should be given to digital formats and the use of multimedia.

Higher National Unit Specification: Statement of standards

Unit title: Data Security (SCQF level 7)

The **product evidence** will relate to Outcomes 2, 3 and 4. Learners will be required to carry out the practical tasks outlined in Outcomes 2 and 3. They will use the knowledge and skills gained from these two outcomes to deliver a sound security strategy to improve data security for a client, in a real or simulated scenario in Outcome 4. They will be able to evaluate the current security measures and identify shortfalls from a given brief, and then provide a pitch to a target client with recommendations for an appropriate strategy to improve the corporate data security.

The product evidence will be produced over the life of the unit, under supervised conditions, and access to reference materials will be permitted. Authentication may be required (*see below*).

Assessors will use their professional judgement, subject knowledge and experience, with reference to the support notes, and understanding of their learners to establish the most appropriate ways to generate credible evidence. This may vary depending on the conditions and context in which this unit is delivered.

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. Appropriate level descriptors should be used when making judgements about the evidence.

When evidence is produced in uncontrolled or loosely controlled conditions it must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The support notes section of this specification provides specific examples of instruments of assessment that will generate the required evidence.

Higher National Unit Support Notes

Unit title: Data Security (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this unit

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the teacher. It seeks to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

Outcome 1

Outcome 1 introduces learners to the subject of data security and why it is relevant at both personal and corporate level. Learners will investigate contemporary data breaches including the causes and effects, from both the point of view of the client and the organisation, in terms of their reputation and financial penalty. Learners should be encouraged to source their own case studies to help develop their research skills. It may also be desirable to introduce the implications of the General Data Protection Regulation, effective from May 2018, and how this will affect organisations in the event of a data breach. This knowledge will then be applied to the recommendation report for Outcome 4.

Outcome 2

Outcome 2 relates to data security on a personal level. Learners will demonstrate the creation of robust passwords, and this understanding will help formulate a password policy for inclusion in Outcome 4. Password attacks, such as brute-force and dictionary attacks, can be introduced. Created passwords may be tested for robustness on password-checker websites, such as **https://www2.open.ac.uk/openlearn/password_check/**.

Learners will also install and configure a simple firewall on a personal device, for example a laptop, desktop PC or mobile phone. The importance of secure, properly configured firewalls should be emphasised, as this is included at a more advanced level in Outcome 3. Learners should also be introduced to the concept of encryption for e-mails containing sensitive data, and this can be accomplished by the creation of free webmail accounts with providers, such as **https://protonmail.com/**, or appropriate plugins for existing accounts, using providers such as Gmail.

Completion of these practical tasks may be evidenced with screenshots that can be included in the recommendation report produced for Outcome 4.

Higher National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 7)

Outcome 3

Outcome 3 follows on from Outcome 2, in that it takes security measures from a personal level to an organisational level. Learners will be introduced to various forms of hardware security protection for both personal devices (cable locks, password protection, screen lock) up to host systems (security slots, backups kept offsite) and the buildings and premises themselves (security guards, motion detection sensors, physical barriers, mantraps, biometric access to sensitive premises (eg, retina scan, fingerprint scan)).

Learners will be introduced to the concept of a corporate firewall (network intrusion protection) following on from the personal firewall (host intrusion protection). Depending on the environment in which this unit is delivered, and the type of group, it may not be possible for learners to configure a corporate firewall with an access control list, in which case a Whitelist on the personal firewall in Outcome 2 may be used. Certainly, the concept of allowing/denying certain types of traffic, whitelisted and blacklisted traffic, should be introduced, and either the configuration of a network firewall or the creation/customisation of a whitelist on a personal firewall could be used as evidence of this knowledge.

Finally, learners should develop an appropriate backup strategy regarding the type of media used, frequency, and appropriate storage and testing.

Outcome 4

Outcome 4 gives the learner the opportunity to demonstrate the knowledge and skills acquired in Outcomes 1–3 in the form of a recommendation report. The learner will be provided with a case study, in which all of the points covered in Outcomes 1–3 should be addressed. Learners will be required to pitch their security strategy to a target group; they will be required to identify shortfalls in security measures and put together a sound security strategy.

Guidance on approaches to delivery of this unit

It is highly recommended that the outcomes are delivered in sequence, as the later outcomes are dependent on knowledge gained in the earlier ones.

A suggested distribution of time, across the outcomes, is:

Outcome 1: 8 hours
Outcome 2: 8 hours
Outcome 3: 12 hours
Outcome 4: 12 hours

Delivery could be by short presentations, followed by group work, classroom discussions, research tasks and practical exercises. There should also be guidance in relation to collation of evidence and research methodology.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide educators with an opportunity to diagnose misconceptions, and intervene to remedy them before progressing to the next outcome.

Formative assessment may, therefore, be carried out after the delivery of Outcomes 1, 2 and 3. The case study can be introduced at the beginning of the unit and evidence collected as the unit progresses; when reaching Outcome 4, learners will have already collected much of the material for the report. This will spread the burden of assessment across the period of delivery.

It is recommended that any resources used, for example the encrypted e-mail task in Outcome 2, be web-based or capable of being run from a USB drive. Some centres may have limitations on software that can be installed on their machines, but this unit is intended to be as accessible as possible. The use of web-based or portable resources also enables learners to practise their skills out with the centre. Suitable versions of personal firewalls may be obtained as freeware or trialware (for example Zone Alarm or Comodo).

Summative assessment, by the nature of the unit, may be carried out towards the end of the unit (but with sufficient time for remediation and re-assessment). As already stated, continuous formative assessment could commence early in the life of the unit and be carried out throughout the duration of the unit.

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Suggestions for the **knowledge evidence** covering all Outcomes (1–3) could be:

1 Questioning using a variety of response types, for which the overall pass mark could be 60%. The test could be split into sections with, for example, 20 selected response questions. The test could last an hour and sample all of the knowledge. In addition, as parts of the evidence require a description, extended response questions may be a better format to allow this opportunity. This test would be taken sight-unseen, in controlled and timed conditions without reference to teaching materials.

Or

2 A constructed response test comprising a number of short answer questions, marked and assessed traditionally. For example, the test may comprise of 10 questions, requiring a response comprising no more than one or two paragraphs, selected across all three outcomes, each worth five marks, with the learner responses marked out of 50 and a pass mark of 25. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across outcomes. This test would be taken sight-unseen, in controlled and timed conditions without reference to teaching materials. A suitable duration could be 60 minutes;

A more contemporary approach to assessment would involve the use of a web log (blog) to record learning and researched case study examples throughout the life of the unit. The blog would provide knowledge evidence in the descriptions and explanations. The blog should be assessed using defined criteria to permit a correct judgement about the quality of the evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate.

The **product evidence** could take the form of a report with appendices. A suitable length for the report would be 1000 words. This report could generate evidence for all outcomes (2, 3 and 4). Learners should be able to evaluate the current security measures and identify shortfalls from a given brief, and then provide a pitch to a target client with recommendations for an appropriate strategy to improve the corporate data security. The report should address the given case study. However, where alternative assessment arrangements may be required, the product evidence could be generated in any of the following:

- Video testimony
- Web page information
- Advice disseminated in an e-mail
- Advice given in a poster
- Advice given in a leaflet
- Oral presentation
- Visual presentation using any suitable means
- Interactive application
- Animation
- Discussion forum or blog
- FAQ formatted web page or interactive presentation
- Social media page designed to give informative advice only

The report should take the form of a recommendation report commonly used in industry (a sample report can be shown) and should be properly formatted and referenced, as appropriate for a level 7 unit. The report should also include screenshots of the practical tasks undertaken in Outcomes 2 and 3, either in the body of the report, or as an appendix. The learner should also emphasise to the ‘client’ the value of a robust security strategy. The final recommendation in the report could also provide evidence for some of the **knowledge** requirements (eg, explanations of the importance of hardware security protection, corporate firewalls, backup strategies, etc).

The evidence should be generated under supervised conditions and work can be authenticated by continual observation or by individual questioning to ensure that it is the learner's own work.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide assessors with an opportunity to diagnose misconceptions, and intervene to remedy them before progressing to the next outcome. Diagnostic feedback can be provided to learners on an ongoing basis.

Higher National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 7)

Summative assessment, by the nature of the unit, should take place towards the end of the unit. When continuous formative assessment is used, this could commence early in the life of the unit and be carried out throughout the duration of the unit.

Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software.

Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

There are opportunities to develop the Core Skill of *Problem Solving* at SCQF level 5 in this unit.

Learners will develop skills in computational thinking in the form of recognition of threats to IT systems, which often follow similar patterns. They will initiate appropriate solutions by suggesting methods to implement security measures, which will reduce the risk of data breaches.

Learners will also have an opportunity to develop skills in report writing and employability.

History of changes to unit

Version	Description of change	Date

General information for learners

Unit title: Data Security (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit will introduce you to Data Security at both a personal and a corporate level, including potential threats to data, and how to mitigate such threats and reduce the risk of data breaches.

You will learn and research different ways in which systems can be breached and data stolen, and the potential implications for both individuals and organisations. You will learn to recognise potential vulnerabilities and be able to formulate solutions or devise preventative measures to counteract the possibility of a data breach, and you will learn to make recommendations to your client on how to protect and safeguard their valuable data.

This unit will be of benefit to anyone who stores or processes any sort of data in digital form, at a personal as well as a corporate level. This unit can also be contextualised, depending on the framework of the award that you are pursuing, as data security affects every type of organisation that stores or processes digital data.

You will be assessed in a variety of ways. There will be various practical tasks to complete as part of your assessment. You will, most likely, be required to produce a recommendation report based on a case study, to disseminate advice to your client.

As part of this unit, you will have opportunities to develop the Core Skill in *Problem Solving* as well as skills in computational thinking, citizenship, researching, report writing and employability.

At the completion of this unit, you may progress to further study in this topic or similar security topics at a diploma or degree level. The knowledge and skills gained in this unit are also extremely relevant to future employment in any business or computing capacity.