National Unit specification

General information

Unit title: Data Security (SCQF level 5)

Unit code: H9E2 45

Superclass: CC

Publication date: July 2015

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this Unit is to introduce concepts around personal and corporate data security, including aspects of legal and ethical obligations. Learners will discuss examples of real-life data security breaches, and examine the reputational and financial damage caused by poor data security practice.

A specific aim of this Unit is to place data security within the context of the real world. This includes the legal and ethical considerations, and the practical methods to protect personal and corporate data.

On completion of this Unit, learners will be able to use their knowledge to discuss data security breaches and provide remedial solutions, within the context of legal and ethical obligations. Learners may progress to the *Data Security* Unit at SCQF level 6 or similar National Units.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF level 5.

Outcomes

On successful completion of the Unit the learner will be able to:

1 Describe the legal and ethical obligations around storing and sharing personal and business data.
2 Explain the causes and effects of data security breaches.
3 Protect data against security breaches.

National Unit specification: General information (cont)

Unit title: Data Security (SCQF level 5)

Credit points and level

1 National Unit credit at SCQF level 5: (6 SCQF credit points at SCQF level 5)

Recommended entry to the Unit

Entry is at the discretion of the centre. However it would be beneficial if learners have knowledge of basic digital literacy and understanding of the use of data.

Basic computer skills may be evidenced by possession of:

H3LJ 44 *Computer Basics* (SCQF level 4) or equivalent qualifications or experience.

With regards to an understanding of data, learners who have completed the *Data Security* Unit at SCQF level 4 will have the necessary background information.

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

If this 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**.

National Unit specification: Statement of standards

Unit title: Data Security (SCQF level 5)

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.

Outcome 1

Describe the legal and ethical obligations around storing and sharing personal and business data.

Performance Criteria

(a) Describe the laws that apply to the storing and sharing of data.
(b) Describe the ethical considerations of organisations when storing and sharing data.
(c) Describe real life examples of best practice in the application of ethics within organisations.

Outcome 2

Explain the causes and effects of data security breaches.

Performance Criteria

(a) Define a data security breach.
(b) Identify contemporary real life examples of data security breaches.
(c) Explain common causes of data security breaches.
(d) Explain the potential effects of a data security breach on individuals.
(e) Explain the potential effects of a data security breach on organisations.

Outcome 3

Protect data against security breaches.

Performance Criteria

(a) Identify software that can be used to enhance data security.
(b) Identify hardware that can be used to enhance data security.
(c) Identify workplace rules that can be used to enhance data security.
(d) Apply selected methods of enhancing data security to a specific situation.
(e) Create a data security solution for a recent data security breach.

National Unit specification: Statement of standards (cont)

Unit title: Data Security (SCQF level 5)

Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge and experience, and understanding of their learners to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used.

Evidence is required to demonstrate that learners have achieved all Outcomes and Performance Criteria. However, sampling may be used in certain circumstances (see below).

The evidence for this Unit may be written or oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital). Particular consideration should be given to digital formats and the use of multimedia.

Evidence is required for two types of competence: evidence of **cognitive competence** (knowledge and understanding) and evidence of **practical competence** (practical abilities).

The evidence of cognitive competence for this Unit will relate to Outcome 1 (all Performance Criteria), Outcome 2 (all Performance Criteria) and Outcome 3 (PC (a), (b) and (c)).

In Outcome 1, the evidence generated should demonstrate:

- knowledge of at least **two** relevant laws relating to data security.
- at least **two** examples of ethical considerations organisations should undertake.
- at least **two** examples of best practice in the application of ethics within organisations.

In Outcome 2, the evidence generated should demonstrate:

- a clear meaning of the term 'security breach' and at least **two** common causes of data breaches.
- at least **two** contemporary real life examples of security breaches.
- at least **two** potential effects on individuals who are affected by a data security breach.
- at least **two** potential effects on an organisation when a data security breach takes place.

In Outcome 3 (PC a-c), the evidence generated should demonstrate:

- at least **two** types of software, hardware and workplace rules used to enhance data security are identified.

Evidence for cognitive evidence may be sampled across the knowledge domain defined by this Unit specification, so long as the sample is unknown, and unpredictable, to the learner. Where sampling is used to assess the learner's knowledge and understanding, an appropriate pass mark should be set.

National Unit specification: Statement of standards (cont)

Unit title: Data Security (SCQF level 5)

The evidence of practical competence for this Unit will relate to Outcome 3 (PC d and e). Evidence of practical competence may be produced over an extended period of time; but where it is generated without supervision some means of authentication must be carried out. The Guide to Assessment provides advice on methods of authentication.

For Outcome 3 (PC d–e) requiring evidence of practical competence, the evidence generated should demonstrate:

- at least **one** method of enhancing data security to a specific situation is selected.
- at least **one** data security solution is produced for a recent data security breach.

A data security solution is an end-product that should demonstrate understanding of all Performance Criteria in Outcome 3. The solution should indicate the use of hardware and software. It may be necessary to supplement evidence created in the data security solution with further questions, in the event that it does not provide a full demonstration of competence.

The Guidelines on Approaches to Assessment (see the Support Notes section of this specification) provide specific examples of instruments of assessment.

National Unit Support Notes

Unit title: Data Security (SCQF level 5)

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

The content of this Unit aims to introduce the standards, laws and ethical considerations of data security, and, using this knowledge, explore examples of breaches in data security and look for solutions to such breaches. This Unit can be used as a platform for discussion on the wider effects of poor data security, whilst looking at the legal protection for data subjects.

Data security, and understanding the place of data security in the personal and corporate spheres, allows learners to work towards building the skills to provide data security solutions. In this way, the focus of this Unit is very much towards the final product — applying knowledge of the legal and ethical aspects of data security to a situation, to provide a data security solution.

Throughout this Unit learners must adhere to ethical standards of practice.

Outcome 1

This Outcome aims to inform learners of the laws and ethical considerations of data security, to provide enough knowledge to come to an informed opinion on matters of data security in the subsequent Outcomes within this Unit.

Learners will be able to discuss and research the laws that apply to the storing and sharing of sensitive data. The laws regarding data security may be updated and amended, and could be affected at Scottish, UK and EU legislations.

It may be important to highlight data security and data protection as part of a larger legal and ethical framework, including the following laws and conventions:

- The European Convention on Human Rights. Article 8 of the ECHR provides a right to respect for one's 'private and family life, his home and his correspondence', subject to certain restrictions.
- The European Data Protection Directive, which gives guidelines on data protection
- The Data Protection Act (UK law)
- Freedom of Information Act (Scotland)

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 5)

Particular attention would be applied to the Data Protection Act. Learners should be able to name and describe this law, in the context of data security. This would include a brief description of the rights of individuals and the responsibilities of companies.

It would be useful to look at the 'not in the UK' issue regarding cloud storage — where data is held can determine its security, in accordance with the laws of the country.

Ethical considerations can be discussed in the context of the Data Protection Act, or discussed in wider terms. A debate on the topic of 'just because an organisation can piece together a customer's life from their data trail does not mean it always should', for example, would provide time for discussion on how companies and governments should use data.

Real life examples of best practice in the application of ethics within organisations will help learners develop views on what level of data storage is appropriate in a particular circumstance, and how it relates to the legal aspects of data security and storage.

The links below give some further information relating to Outcome 1.

- http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you
- https://ico.org.uk/for-the-public/
- https://ico.org.uk/media/for-organisations/documents/1607/the_guide_to_data_protection.pdf
- http://www.computerweekly.com/news/2240162744/Data-ethics-Author-warns-of-ethical-pitfalls-of-data-collection
- http://www.scu.edu/ethics/practicing/focusareas/cases.cfm?fam=TECH
- http://en.wikipedia.org/wiki/Ethics_of_technology
- http://www.forbes.com/sites/privacynotice/2014/02/03/inside-googles-mysterious-ethics-board/
- https://www.microsoft.com/online/legal/v2/?docid=25
- http://www.computerworld.com/article/2557944/security0/ethical-issues-for-it-security-professionals.html

Outcome 2

In Outcome 2, learners will begin to understand the nature and effect of security breaches.

Using popular examples (see Information is Beautiful link below), learners should be able to appreciate the scale and severity of corporate data breaches, and what kind of information is lost in a data breach.

When looking at the causes of data security breaches, learners can identify a variety of methods and the prevalence of types of attack used in data breaches. Types of attack that may be mentioned in other Units within this Group Award may be investigated here, including stealing credentials, default passwords, keylogging and spyware, phishing, exploits and RAM scraping.

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 5)

Learners will be required to appreciate the inherent risks associated with any networked device, and understand the potential threats posed by public and private IP addresses and TCP ports.

The potential effects of data security breaches can be observed in case studies — learners can benefit from seeing the difference in effect on an organisation and an individual.

- Information is Beautiful — Worlds Biggest Data Breaches — http://goo.gl/y4XCwh
- Forbes — Chart of the Biggest Data Breaches in U.S. History — http://goo.gl/flZG4m
- Target — Data Breach FAQ — http://goo.gl/4RHFb0
- Gartner — How PCI failed Target and U.S. Consumers — http://goo.gl/WDyCtP
- Krebs on Security — Home Depot Hit By Same Malware as Target — http://goo.gl/fFHlW9
- The Week — eBay Hack — http://goo.gl/jchRFI
- PC Mag — Adobe Hacked, Data for Millions of Customers Stolen — http://goo.gl/1B5CYL
- PC Mag — Experian Confirms Subsidiary's Data Sold to ID Theft Operation — http://goo.gl/PYEgPM
- https://www.youtube.com/watch?v=jukNor0-fOw (Russia Today data breach report)
- http://www.pcworld.com/article/2909952/web-app-attacks-pos-intrusions-and-cyberespionage-leading-causes-of-data-breaches.html
- http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf
- http://www.networkworld.com/article/2905953/under-one-percent-of-android-devices-affected-by-potentially-harmful-applications.html

Outcome 3

The purpose of this Outcome is to give learners a chance to create a solution that could prevent a data security breach. By this point, the learner will be aware of the legal and ethical requirements and considerations that an organisation will have regarding data security, and will be aware of how data breaches can happen and the potential effects the breach can have on the individuals and organisations involved. With all this in mind, a data security plan can be created.

In relation to software, learners should look at the growing variety of software techniques used to secure data, from authentication to encryption. This could include two-phase authentication, facial recognition, fingerprint scanning, automatic log-out, updating software to the latest versions, file encryption, encryption of connections, RSA ID tokens, user level filtering and monitoring, firewalls and anti-virus/spyware/malware.

In relation to hardware, learners should be aware of the physical nature of some data security methods, including access PINs, hardware keys and protective networking devices such as firewalls. If learners are aware of networking hardware, looking at the logistical nature of port access, disabling ports, identifying devices by MAC address and other network security techniques can be investigated.

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 5)

Workplace rules can include backing up files, ethical rules and training, strict access control and any other relevant technique.

When forming a plan for data security, learners can apply a selected method of enhancing security to a specific situation. This could work well as a scenario-based task, where learners must use sound and informed reasoning to pick the best tool.

The summary exercise of creating a data security solution should be informed by all Outcomes and Performance Criteria that precede it. The learner should talk about relevant hardware, software and workplace rules that would help to prevent a data security breach.

Examples of real-life scenarios that could be used to apply enhanced security could be a:

- default install of an operating system with no authentication
- user with a simple or default password
- computer visible publicly on a network
- device that can be switched for an unrestricted device on a network
- login system that is accessed from public computers
- system that must uniquely identify a person for physical access (biometrics)
- hard drive that is accessible by a large group of people
- file being sent over a network to another computer

Examples of data security solutions should take into account the nature of a breach and suggest relevant actions. Below are some suggestions of example breaches, and some relevant actions that could be taken.

Breach	Relevant Action
USB flash drive of sensitive data is lost on the subway	Encryption, authentication method built into USB flash drive. Banning use of USB flash drives for file transfer.
An employee is fired and downloads sensitive data to take with them when they leave	User-level access monitoring, separate encryption for groups of files, time-restricted accounts.
Hackers gain access to a server and download files	Update patches are applied at all times to prevent vulnerabilities, firewall to prevent access, removal of all default passwords, password rotation, password strength checks, two-phase authentication, ID tokens, restriction of important files to small number of accounts, encrypted files.
Employee leaves computer on and another member of staff uses their account to steal data	Automatic logout on all machines, user-level monitoring to record actions, fingerprint authentication.

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 5)

Links to further information:

- http://www.pcs.org.uk/en/resources/imembership/guide-to-data-protection.cfm
- https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf
- http://www.itdonut.co.uk/it/staff-and-it-training/your-it-policies/sample-data-protection-policy-template
- http://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy

Guidance on approaches to delivery of this Unit

This Unit relies on some studying and research to build knowledge of data security. It may be best to use online resources in combination with co-operative learning strategies to encourage learners to foster an approach that leads to deep understanding.

There are a large number of online resources in relation to data security, including a number of easy to access videos on data breaches, the law and data security policy.

It would be appropriate for teacher-led tasks to be used to guide progress.

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 that 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.

The evidence for cognitive competence in Outcomes 1, 2 and 3 (PC a, b and c) can be captured in various ways, such as reports, presentation, videos, podcasts or summaries of the learning. A traditional test which appropriately samples knowledge is also acceptable.

It is also possible that the security plan produced in Outcome 3 could adequately cover all Performance Criteria for all Outcomes, if significant background information was given before the solution was provided.

The evidence for **Outcome 1** could take the form of a set of written or presented case study. All Performance Criteria should be covered explicitly in the content of the case study. The topics covered could include:

- The names and descriptions of two UK laws relating to data security, such as the Data Protection Act

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 5)

- The descriptions of two ethical considerations companies should consider when storing data. This could include the decision on which data was relevant to the company's work, if it would be right to use identified patterns of behaviour gleaned from data to guide company policy, if companies should read the emails of their employees to guarantee network security or if it would be right to monitor internet usage in work.
- Two examples of best practice in the application of ethics or guidelines used by organisations. These could be specific to data security or wider guidelines that incorporate data security.

The evidence for **Outcome 2** may take the form of a written set of questions, or a report. Questions should cover all of the Performance Criteria, and should demonstrate understanding of the meaning, causes and effects of data security breaches. A report should cover all Performance Criteria, and could be presented in a number of ways, such as a web page, audio report or written report.

The evidence for **Outcome 3** may take the form of a report or presentation detailing a solution to a recent data security breach. The report should incorporate the Performance Criteria (a) to (d), informing the creation of the solution itself (Performance Criterion (e)). Performance Criteria (d) and (e) may be treated as separate tasks, with (d) focussing on a single practical activity to fix a specific problem, and (e) looking at a problem in context. It could be in the form of an observation checklist completed and signed by the assessor after observing candidates carry out practical tasks.

Another approach to assessment would be the creation and maintenance of a web log, which would record candidate activity throughout the Unit. This would log, on a daily or weekly basis, what candidates learn and what they do. However, their posts would have to satisfy the relevant Performance Criteria. Practical activities could also be recorded via the blog. When practical activity is recorded on a blog (narratively), authentication could involve a photograph or video of candidate activity (this could be included as part of their post). Not every practical task would require authentication; at this level it is acceptable for some posts to be a simple description of appropriate practical activities. When necessary, separate authentication (such as oral questioning) could be used for verification purposes.

The critical aspect is that the blog is an overall accurate reflection of the practical activities (and, therefore, the associated skills) carried out by the learner during the life of the Unit.

Another approach would involve the creation and maintenance of an e-portfolio. The e-portfolio would include all of the statements, identifications, descriptions and selections necessary to satisfy the criteria relating to cognitive competencies, together with digital artefacts that provide evidence of their practical abilities. Digital artefacts would include screenshots, digital photographs, audio and video recordings, etc that collectively evidence candidates' competencies. Some form of authentication would be required. This could be as simple as a statement of originality, signed by the candidate and the assessor.

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 5)

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

In this Unit, learners will have the opportunity to develop the following Core Skill:

Information and Communication Technology (ICT) (SCQF level 5)

Learners will be required to investigate aspects of technology, and report of their effectiveness. They will be expected to experience a range of data security software and hardware. *ICT* skills are crucial for developing solutions to data security concerns. In particular, the investigation of data security products would involve processing and presenting information and accessing information using *ICT*, two Core Skill components in *ICT* at SCQF level 5.

The data security concerns of business and the legal/ethical framework that are used to discuss such concerns can develop skills in the areas of enterprise and employability. The area of citizenship may be developed through an understanding of the responsibilities of organisations to use data correctly.

History of changes to Unit

Version	Description of change	Date

General information for learners

Unit title: Data Security (SCQF level 5)

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 aims to provide you with knowledge about data security and how it is handled by organisations, and skills to provide practical solutions to data security problems.

All the learning in this Unit is aimed at informing you of current practices in data security. This will make it possible for you to complete the final Outcome, in which you are expected to create a data security solution to deal with a recent data breach.

This Unit is designed for those with a basic understanding of data security. This may have been developed in the *Data Security* Unit at SCQF level 4, which introduces the idea of data, how data is stored and how it can be used, as well as preparing learners with the skills to secure a computer's data.

In this Unit, you will begin by investigating the laws surrounding data security, such as the Data Protection Act. The laws are important — without them, we would have no rights, and organisations would have no responsibilities. We will further discuss the ethical considerations that companies need to think about when storing lots of your data.

You will also look at data breaches — a growing cause of financial and emotional damage as more and more data is stored online.

Finally, you will look at how work-related practices, hardware and software can all help to prevent data breaches and keep data secure. You will finish this Unit by providing a solution to protect a company after a data security breach. This practical know-how and ability to pick a solution that could protect a computer system is the essence of cyber security.

Assessment for this Unit can take various forms. It should be part of your ongoing work and you will find your focus will be on learning and practical work. You should take a responsible attitude to recording your work throughout the year, as anything you do can help provide evidence of your learning.

This Unit is part of a series of Units on data security. You may progress to the next Unit in the series (the *Data Security* Unit at SCQF level 6) on completion of this Unit if you wish to improve your knowledge and skills in this area.