UNIT 7 - IT Systems Security and Encryption (Mandatory Unit) Coursework Unit						
Lesson No	**Topic & Objectives**	**Big Question – What will students learn?**	**Key Activities & Specialist Terminology** **(Do Now Task / Starter/Tasks/Plenary**	**Planned Assessment**	**Homework or flipped learning resources** **DODDLE resources**	**Lit Num** **SMSC Codes**
1	**A1 Threat types*** Internal threats.	**Why is 'Bringing Your Own Device' a security threat?**	• **Lead-in:** Discuss the relevance and importance of IT security. See link: The three greatest insider threats to your organisation, and how to beat them in the following link www.itproportal.com/2014/05/30/the-three-greatest-insider-threats-to-your-organisation-and-how-to-beat-them/ • **Tutor-led discussion:** Discuss learners' experience and knowledge of security threats. • **Paired activity**: Learners discuss what they consider to be an 'internal' threat and research the types of threats posed by staff within a company. Each pair presents findings to the whole class. • **Independent learning activity:** Learners complete a short report on why Bring Your Own Device (BYOD) is a security threat and how it can be dealt with.	A.P1 Explain the different security threats that can affect the IT systems of organisations. Completed report on the security issues with BYOD	Cybersecurity issues are often in news. Check out news websites such as the technology section of the BBC news website for the latest IT security issues – Write up notes from news stories that they find.	Lit Social So8 C3 Sp2 Sp5

			• **Plenary:** Give feedback on activities. Sum up the lesson and hold a quick Q&A session on the internal threats that exist in different environments			
2	**A1 Threat types** External threats.	What security threats could affect the students at school	• **Lead-in:** As a whole class, thought shower ideas about the meaning of 'external' threats. **Paired activity**: Learners research recent examples of cyber-attacks from a variety of external resources and present findings. See links: Massive cyber-attack could trigger NATO response (June 2016), Second bank cyber-attack detected (May 2016), Cyber-attacks: Two-thirds of big UK businesses targeted (May 2016), DDoS: Website-crippling cyber-attacks to rise in 2016 (January 2016) and Cyber-attack news (multiple articles) in the following links: Massive cyber attack could trigger NATO response (June 2016) www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE Second bank cyber attack detected (May 2016) www.bbc.co.uk/news/technology-36284446 Cyber attacks: Two-thirds of big UK businesses targeted (May 2016) www.bbc.co.uk/news/uk-36239805	A.P1 Explain the different security threats that can affect the IT systems of organisations.	Q&A on the external threats that exist in different environments.	Lit Social So8 C3 Sp2 Sp5

			DDoS: Website-crippling cyber-attacks to rise in 2016 (January 2016) www.bbc.co.uk/news/technology-35376327 Cyber attack news (multiple articles) www.cyberattack.news/ • **Independent learning activity:** Learners complete a short report on the types of external threats that could affect them at college/school or at home. They should retain their research notes and reports for future use.			
3	**A1 Threat types** Social engineering and software-driven threats.	**'What is a computer virus?'**	• **Lead-in:** As a whole class, thought shower ideas about software-driven threats. Discuss 'What is a computer virus?' See video link: Difference Between Viruses, Worms and Trojans (3 minutes) in the following link: www.youtube.com/watch?v=y8a3QoTg4VQ • **Tutor-led discussion:** Discuss experience and knowledge of virus infections. • **Tutor presentation:** Introduce learners to the different types of software-driven threats. • **Paired activity:** Learners research recent examples of malware including virus attacks, ransomware etc and present their findings to the whole class. They should retain their research notes and reports for future use.	A.P1 Explain the different security threats that can affect the IT systems of organisations.	Learners should find out about viruses. See video link: Top 30 Dangerous Computer Viruses (27 minutes) in the following link: www.youtube.com/watch?v=QIqA66eYpC0	Lit Social So8 C3 Sp2 Sp5

			• **Tutor-led discussion:** Discuss the meaning of 'social engineering' and how it works. • **Plenary:** Q&A on malware.			
4	**A2 Computer network-based threats*** Passive threats.	**'Why might people want to find a way into your computer?'**	• **Lead-in:** Discussion, 'Why might people want to find a way into your computer?' • **Tutor presentation:** Introduce learners to the different types of passive threats. See link: Passive attack in the following link: http://whatis.techtarget.com/definition/passive-attack • **Paired activity:** Learners research the nature and effects of various types of passive threats. • **Tutor-led discussion:** Feedback on the activity. • **Plenary:** Discussion, should the government or police be allowed to eavesdrop on your electronic data?	A.P2 Explain the principles of information security when protecting the IT systems of organisations	Research news websites such as the technology section of the BBC news website for the latest IT security issues	Lit Social So8 C3 Sp2 Sp5
5	**A2 Computer network-based threats** • Active threats. • Cloud computing risks.	**How secure is cloud computing secure?**	• **Lead-in:** Discussion on cloud computing – is it secure? • **Tutor presentation:** Introduce learners to the different types of active threats. See link: Active attack in the following link http://whatis.techtarget.com/definition/active-attack • **Small group activity:** Each group researches a different active threat and prepares to present their findings to the class. • **Tutor-led discussion:** Learners present their ideas from the group activity to the whole class.	A.P3 Explain why organisations must adhere to legal requirements when considering IT system security	The Stuxnet computer worm is said to have been developed by the US and Israeli governments to attack the Iranian nuclear programme, although they have never admitted this. Research what Stuxnet does	Lit Social So8 C3 Sp2 Sp5

			• **Plenary:** Feedback on activity. Test learners understanding with Q&A on network threats.		and how it has been used.	
6	**A3 Information security***	**How do they think the principles of information security apply to this information?**	• **Lead-in:** Ask learners to think about what information security is and why it is important. Learners thought shower ideas and feed back to the whole group. • **Paired activity**: In pairs, learners discuss what sort of information about them is held electronically. How do they think the principles of information security apply to this information? How might this data be misused? Learners write up their notes and keep them for future reference. • **Tutor-led discussion:** Learners present their ideas from the paired activity to the whole class. • **Independent learning activity:** Learners research a number of given scenarios about their personal information. In each case, learners research who holds the information, who it is shared with and any privacy issues associated with it. Learners keep their research notes for future use. • **Plenary:** Feedback on individual activity. Test learners' understanding with a Q&A session on information security.	A.M1 Assess the impact that IT security threats can have on organisations' IT systems and business whilst taking account of the principles of information security and legal requirements.	Find out how to request your personal information – see link https://ico.org.uk/for-the-public/personal-information/	Lit Social So8 C3 Sp2 Sp5
7	**A4 Legal requirements**	**What are the legal requirement**	• **Lead-in:** Discuss the main legal requirements of IT security and which	A.D1 Evaluate the effectiveness of the techniques	CryptoLocker is a well-know example of ransom for their	Lit

	• Data Protection Act 1998. • Computer Misuse Act 1990. • Copyright, Designs and Patents Act 1988. • Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. • Fraud Act 2006. • Legal liability and contractual obligations.	**s of IT security**	laws apply to IT security. See link: Guide to data protection: • Information relating to: • Data Protection Act (1998) • Computer Misuse Act (1990) • Copyright, Designs and Patents Act (1988) • Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000) • Fraud Act (2006). • Computers with internet connection for research. • Link for lead-in: • www.pcs.org.uk/en/resources/imembership/guide-to-data-protection.cfm • **Small group activity:** Learners research prosecutions under the different laws listed in the specification. Learners write up their notes and keep them for future reference. • **Tutor-led discussion:** Discuss how the legislation was applied, and the consequences. • **Independent learning activity:** Learners are given examples of situations where laws may have been broken and then identify which laws might apply. • **Plenary:** Prepare for next lesson's guest speaker. • **Independent learning activity:** Learners devise a given number of suitable questions for the guest	used to protect organisations from security threats whilst taking account of the principles of information security and legal requirements.	decryption. Research how CryptoLocker works, what effects it had on infected computers and how it was eventually disrupted.	Social So8 C3 Sp2 Sp5

			speaker. If necessary, this task could be set as homework.			
8	**A5 Impact of security breaches*** **C7 Skills, knowledge and behaviours**	**What impact could a security breach have on an individual?**	• **Lead-in:** Discuss the impact of security breaches. • **Guest speaker:** IT manager from a local business talks about the importance of IT security, some of the threats that their business faces and the potential impact of security breaches. Learners ask the speaker their prepared questions. • **Small group activity:** Learners investigate examples of security breaches and consider the impact that they could have. Groups feed back their findings to the whole class. • **Plenary:** Discuss and ask learners questions about what sort of impact a security breach could have on them as individuals.	A.D1 Evaluate the effectiveness of the techniques used to protect organisations from security threats whilst taking account of the principles of information security and legal requirements.	Students to research and make notes on the UK's 11 most infamous data breaches – see link www.techworld.com/security/uks-11-most-infamous-data-breaches-2015-3604586/	Lit Social So8 C3 Sp2 Sp5
9	**Summary of learning aim A and mock assessment** **C7 Skills, knowledge and behaviours***	**Overview of Learning Aim A**	• **Lead-in:** Recap what has been covered in this learning aim. • **Knowledge quiz:** Learners take a self-marked informal quiz covering the topics in learning aim A. • **Tutor presentation:** Introduce the mock assessment. • **Individual activity:** Learners work on the mock assessment. • **Plenary:** Q&A on the mock assessment. • **Individual activity:** Learners complete the mock assessment as homework.	A.D1 Evaluate the effectiveness of the techniques used to protect organisations from security threats whilst taking account of the principles of information security and legal requirements.	Research and make notes on ICMP is not used to send messages between computers. Instead it is used for diagnostic tool that uses ICMP is a program called Ping. Find out what Ping is for and how it can be used.	Lit Social So8 C3 Sp2 Sp5

10	**B1 Cryptographic principles***	**What are the cryptographic principles?**	• **Lead-in:** Introduction to learning aim B and cryptography. **Tutor presentation:** Introduction to cryptographic principles. See video link: Introduction to Cryptography (4.5 minutes) in the following link www.youtube.com/watch?v=68Pqir_moqA • **Paired practical activity:** Learners use various cryptographic principles to try out simple cyphers. • **Tutor-led discussion:** Feedback on activity.	B.P4 Explain the principles and uses of cryptography to secure and protect data	Students need to research and write about 'Can encryption be used to hide illegal activity? Should access to encryption be restricted?'	Lit Social So8 C3 Sp2 Sp5
11	**B2 Cryptographic methods** Key cryptography methods.*	**Should the government or police be able to eavesdrop on a person's electronic data?**	• **Lead-in:** Discussion around the computational hardness assumption. Will computers become too powerful for current encryption methods? • **Tutor presentation:** Introduce learners to the different cryptographic methods. • **Paired activity:** Learners research the way different cryptographic methods work. • **Tutor-led discussion:** Feedback on the activity, recap on the various methods. • **Plenary:** Discussion 'Should the government or police be allowed to eavesdrop on your electronic data?'	B.P4 Explain the principles and uses of cryptography to secure and protect data	Carry out research to find out what the most common threats are to computer systems. There are a number of places you can go to research this question. The Open Web Application Security Project (OWASP) publishes a list of the 'top 10' web security risks from time to time. Companies that produce anit-malware software, such as Norton™,	Lit Social So8 C3 Sp2 Sp5

					McAfee and Kaspersky™, also publish lists of the most destructive malware	
12	**B3 Applications of cryptography** **The types and applications of cryptography.***	**What are the different types of encryption methods?**	• **Lead-in:** Recap of cryptographic methods followed by Q&A session to check learners' understanding. • **Tutor presentation:** Explanation of symmetric and public/private key encryption methods. See video link: Symmetric key and public key encryption (6.75 minutes) in the following link www.youtube.com/watch?v=ERp8420ucGs • **Small group activity:** Each group researches a different application of encryption • **Tutor-led discussion:** Groups feed back on their research. • **Plenary:** Q&A to check learners' understanding of encryption methods and applications.	B.M2 Analyse how the principles and uses of cryptography impact on the security and protection of data	Computer forensic is a complex and fascinating topic. Research the tools and techniques which are used	Lit Social So8 C3 Sp2 Sp5
13	**Summary of learning aim B and mock assessment** **C7 Skills, knowledge and behaviours**	**What are the different types of encryption methods?**	• **Lead-in:** Recap what has been covered in this learning aim. • **Knowledge quiz:** Learners take a self-marked informal quiz covering the topics in learning aim B. • **Tutor presentation:** Introduce the mock assessment. • **Individual activity:** Learners work on the mock assessment.	B.M2 Analyse how the principles and uses of cryptography impact on the security and protection of data	Research the use of the A5/1 cypher to encrypt mobile phone communications is interesting to look into. Why for example, was a relatively short key length of 54 bits used rather than a	Lit Social So8 C3

			• **Plenary:** Q&A session on the mock assessment. • **Individual activity:** Learners complete the mock assessment as homework.		more secure longer key? Are there other methods that can be used to protect mobile phone communications?	Sp2 Sp5
14	**Preparation for assessment** **C7 Skills, knowledge and behaviours***	**Assignment work**	• **Tutor-led discussion:** Give general group feedback on mock assessment for learning aim B. • **Revision session:** Recap learning aim A topics and any topics that learners struggled with on the learning aim A mock assessment. • **Tutor presentation:** Introduce the assignment for learning aims A and B. • **Independent learning activity:** Learners complete work schedule/plan for assessment, setting out when they plan to complete each part of the assignment. • **Plenary:** Q&A on assessment.	Completed coursework	Complete Case study on Page 317 on the BTEC Book	Lit Social So8 C3 Sp2 Sp5
15	**Assessment 1** (learning aims A and B)	**Assignment work**	**Assignment:** Learners work independently on the assignment for learning aims A and B. Learners complete this outside class time.	Completed coursework	Bluetooth is widely used for the short-range transmission of data between mobile devices. Although Bluetooth data packets are encrypted, there are a number of security issues when using	Lit Social So8 C3 Sp2

					Bluetooth. Find out how the data packets are encrypted and research the security issues involved when using Bluetooth	Sp5
16	**C1 Physical security*** Building and computer/network room security.	**What different physical security methods are there?**	• **Lead-in:** Introduce learning aim C. • **Tutor presentation:** Introduction to the types of physical security. See video link: Physical Security Techniques - CompTIA A+ (10 minutes) in the following link www.youtube.com/watch?v=-pTIo5lBuTc • **Small group activity:** Learners research different physical security methods and keep their notes for future reference. • **Tutor-led discussion:** Learners present their findings from the small group activity. • **Tutor-led discussion:** Give general group feedback on mock assessments for learning aims A and B. • **Plenary:** Q&A session on types of physical security.	C.P5 Explain how protection techniques can help defend an organisation from security threats.	Firewalls and IDS are a complex topic with many different technologies and configurations is use. Research the topic to find out the latest information about their features and use.	Lit Social So8 C3 Sp2 Sp5
17	**C1 Physical security*** Backing up data.	**What is the importance of backing up files?**	• **Lead-in:** Discuss the importance of backing up data. See link on backing up data in the following link www.data-archive.ac.uk/create-manage/storage/back-up	C.P6 Produce a plan to protect an IT system which meets organisational	What is Kerberos? Where des the name come from? Who developed the system and how does it work?	Lit Social

			• **Tutor presentation:** Introduce the different types of data backup and their relative advantages. • **Paired practical activity:** Learners practise data backup with their own files (using multiple methods). • **Plenary:** Q&A session on backup procedures.	and legislative requirements		So8 C3 Sp2 Sp5
18	**C2 Policies and procedures*** Organisation policies and their application.	**What are Internet and email policies?**	• **Lead-in:** Though shower the purpose and importance of policies and procedures. • **Small group activity:** Learners look at different examples of internet and/or email usage policies and explain reasons for rules and identify any omissions. Learners should keep notes for future use. See links: Sample IT policies, disclaimers and notices, Sample Internet use policy and Sample email use policy in the following links: www.youtube.com/watch?v=kF4Xtq2rDno www.youtube.com/watch?v=en9n_W612sY • **Tutor-led discussion:** Groups feed-back on findings from activity. • **Tutor-led discussion:** What is the ideal content for IT use policies? What protection do they give?	C.P7 Perform tasks to protect the IT system which meets the requirements given in the plan.	Write a few paragraphs detailing whether Policies and procedures: useful or time-consuming?	Lit Social So8 C3 Sp2 Sp5
19	**C2 Policies and procedures*** • Security audits and their application.	**How do you monitor emails and spam coming in?**	• **Tutor presentation:** Introduce the purpose and nature of security audits, update management, email monitoring and data backup. See links: Network security audit case study, IT security auditing: Best practices for conducting	C.P8 Review the extent to which the organisation's IT system has been 'protected'.	Learners to research and answer the following question; If you use cloud storage do you	Lit Social

	• Update management. • Email monitoring and spam monitoring. • Backup of data.		audits and How to conduct a security audit in following links: • Links for presentation: Network security audit case study www.dionach.com/library/network-security-audit-case-study IT security auditing: Best practices for conducting audits http://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits How to conduct a security audit www.techsupportalert.com/pdf/t04123.pdf • **Paired practical activity:** Learners carry out a security audit on the college/school systems, keeping their notes for future use. • **Tutor-led discussion:** In pairs, learners present their conclusions from the paired activity to a whole class discussion.		need to do backups?	So8 C3 Sp2 Sp5
20	**C3 Software-based protection*** Anti-virus software and detection techniques. Firewalls.	**How does anti-virus and malware protect data?**	• **Lead-in:** Q&A session to recap on malware. • **Tutor presentation:** How does anti-virus and malware protection work? • **Individual activity:** Learners research common viruses and other forms of malware and their effects. • **Small group activity:** Learners contribute their discoveries to discussion about common viruses and other forms of malware.	C.M3 Justify the choice of protection techniques used to defend the IT systems of an organisation, showing how its IT system will be protected from security threats	Learners complete an informal self-marked quiz on wireless security and firewalls.	Lit Social So8 C3 Sp2

			• **Tutor presentation:** Introduce firewalls, explaining what they do and how they work. See links: 17 best antivirus and best free antivirus for PC and laptop UK 2016 and The Best Antivirus Utilities for 2016 in the following links: • Links for presentation: 17 best antivirus and best free antivirus for PC and laptop UK 2016 www.pcadvisor.co.uk/test-centre/security/best-antivirus-for-pc-laptop-2016-uk-free-summary-security-software-virus-3263332/ The Best Antivirus Utilities for 2016 http://uk.pcmag.com/antivirus-reviews/8141/guide/the-best-antivirus-utilities-for-2016			Sp5
21	**C3 Software-based protection*** User authentication.	**What methods of authentication are there?**	• **Lead-in:** Discuss passwords and other methods of user authentication. See link: Singapore banks adopt voice biometrics for user identification in the following link: www.computerweekly.com/news/4502982245/Singapore-banks-adopt-voice-biometrics-for-user-authentication • **Tutor presentation:** Introduce user authentication, issues associated with passwords, password best practice and alternative methods of authentication. • **Small group activity:** In small groups, learners develop a password scheme	C.M3 Justify the choice of protection techniques used to defend the IT systems of an organisation, showing how its IT system will be protected from security threats	Learners to research whether it is possible to have 100 per cent protection against viruses.	Lit Social So8 C3 Sp2 Sp5

			and write up notes which are retained for future use. • **Tutor-led discussion:** Feedback and discussion on conclusions from activity. • **Plenary:** Discuss passwords and the issues of security and usability (ie too hard to remember or too easy to guess).			
22	**C3 Software-based protection*** • Access controls and the methods they use to restrict authorised/ unauthorised users' access to resources. **D7 Skills, knowledge and behaviours***	**Why do we need access controls?**	• **Lead-in:** Discuss the need to control access to computer resources. • **Tutor presentation:** Introduce access controls, user groups and methods to allow levels of access to folders, files and resources. See link: User group access levels explained in simple terms in the following link https://docs.joomla.org/User_Group_Access_levels_explained_in_simple_terms • **Guest speaker:** IT manager from a local business talks about the how they control access to resources and access-related issues. Learners ask the guest speaker their prepared questions. • **Plenary:** Q&A on access control and user authentication with guest speaker.	D.M4 Enhance the protection of the IT system which to meet requirements given in the plan.	Passwords are an essential part of modern life. Every time you want to access an online resource or purchase something online you need to register and create an account with a password. This could mean that you have tens, if not hundreds, of accounts all of which require a password. Discuss the best way to keep track of all these passwords with a peer or in a small group. It may not be possible or wise to use the same password for	Lit Social So8 C3 Sp2 Sp5

					all accounts – why not? Students to research and write a couple of paragraphs.	
23	**C3 Software-based protection*** The principles of encryption.	**What is the history of encryption?**	• **Lead-in:** Discuss the use and history of encryption. See link: The best Encryption Software reviews 2016 in the following link http://encryption-software-review.toptenreviews.com/ • **Tutor presentation:** Introduce encryption techniques, such as public/private key encryption. • **Small group activity:** Within their groups, learners develop simple cyphers and send messages using these cyphers. They should then try to crack the other groups' cyphers. • **Tutor-led discussion:** Discuss where and when encryption is used. • **Plenary:** Discuss how effective encryption is and if increasing computer power will render it ineffective.	D.M4 Enhance the protection of the IT system which to meet requirements given in the plan	Students to complete, Cryptography brain teasers – see link in the following link www.braingle.com/Cryptography.html	Lit Social So8 C3 Sp2 Sp5
24	**C3 Software-based protection*** Precautions that can be taken to protect a Wireless LAN from	**What are the principles of wireless network?**	• **Lead-in:** Q and A on security for wireless networks. • **Tutor presentation:** Introduce the principles of wireless network, protections methods and potential issues with protecting a wireless network. **Small group activity:** Learners research given methods of wireless	D.M4 Enhance the protection of the IT system which to meet requirements given in the plan	Learners to write about wireless security, 'Do you need to take special precautions when using a WiFi network?'	Lit Social So8

	unauthorised access.		security. See links: Cain and Abel, Backtrack 5 and Demonstration of Man in the Middle attacks in the following links Cain and Abel www.oxid.it/cain.html Backtrack 5 www.backtrack-linux.org/ Demonstration of Man in the Middle attacks www.youtube.com/watch?v=YPAqvzGY0h0		Summarise the lesson.	C3 Sp2 Sp5
25	**Summary of learning aim C and mock assessment** **D7 Skills, knowledge and behaviours**	Recap of Learning Aim C	• **Lead-in:** Recap what has been covered in learning aim C. • **Knowledge quiz:** Learners complete a self-marked informal quiz on topics covered in learning aim C. • **Tutor presentation:** Introduce the mock assessment. • **Individual activity:** Learners work the on mock assessment. • **Plenary:** Q&A on the mock assessment. • **Individual activity:** Learners complete the mock assessment as homework.	CD.D2 Evaluate the plan and the effectiveness of the protected IT system against requirements	Learners devise a given number of suitable questions for the guest speaker in the next session.	Lit Social So8 C3 Sp2 Sp5
26	**D1 Group policies** Tools for managing a set of IT systems.	**What tools are there for managing a set of IT systems?**	• **Lead-in:** Introduction to learning aim D. • **Tutor presentation:** Introduce the workshop session, ensuring that you cover any health and safety requirements. • **Tutor-led practical demonstration:** Demonstrate how to create user groups and user accounts and how to configure group policies. See links: Step-by-step	D.P7 Perform tasks to protect the IT system which meets the requirements given in the plan.	Students to answer questions on the practical tasks.	Lit Social So8

			Guide to Understanding the Group Policy Feature Set, Group Policy for Beginners and The 10 Windows group policy settings you need to get right in the following links: Step-by-step Guide to Understanding the Group Policy Feature Set https://msdn.microsoft.com/en-us/library/bb742376.aspx Group Policy for Beginners https://technet.microsoft.com/en-gb/library/hh147307(v=ws.10).aspx The 10 Windows group policy settings you need to get right www.infoworld.com/article/3044614/security/the-10-windows-group-policy-settings-you-need-to-get-right.html • **Individual practical activity:** Learners practise creating user groups and user accounts and configuring group policies, following the procedures outlined in the demonstration.			C3 Sp2 Sp5
27	**D2 Anti-malware protection** Installation of anti-malware software, configuration of anti-malware scanning schedules.	**How to install anti-malware software and configure schedules?**	• **Lead-in:** Recap on anti-virus software. **Tutor-led practical demonstration:** Demonstrate how to install anti-virus software and configure scanning schedules. See video links: How to install Avast Free Antivirus and How to: Schedule automatic scan in Avast Antivirus 2016 in the following links; www.youtube.com/watch?v=dpCj2A-DNdQ How to: Schedule automatic scan in Avast Antivirus 2016	D.P7 Perform tasks to protect the IT system which meets the requirements given in the plan.	Students to answer a range of questions on the practical tasks they have viewed.	Lit Social So8 C3 Sp2

			www.youtube.com/watch?v=vg3OHDIk7Nk • **Individual practical activity:** Learners practise installing anti-virus software and configuring scanning schedules.			Sp5
28	**D3 Firewall configuration** Hardware and/or operating system-embedded firewalls, including configuration of: • inbound and outbound rules to control network connections that are allowed and prevent all other unauthorised connections • firewall events and interpretation of log entries.	**How to configure firewalls?**	• **Lead-in:** Recap on firewalls. • **Tutor-led practical demonstration:** Demonstrate how to configure a firewall. See links: Firewall Configuration, Configuring a simple firewall and Understanding Windows firewall settings in the following links: http://computer.howstuffworks.com/firewall2.htm Configuring a simple firewall: www.cisco.com/c/en/us/td/docs/routers/access/1800/1801/software/configuration/guide/scg/firewall.html Understanding Windows firewall settings: http://windows.microsoft.com/en-gb/windows/understanding-firewall-settings#1TC=windows-7 • **Individual practical activity**: Learners practise configuring a firewall (either built-in or separate firewall software).	D.P7 Perform tasks to protect the IT system which meets the requirements given in the plan.	Students to answer a range of questions on the practical tasks they have viewed.	Lit Social So8 C3 Sp2 Sp5
29	**D4 Wireless security** • Wireless encryption methods, e.g.	**What are some wireless**	• **Lead-in:** Recap on wireless security. • **Tutor presentation:** Talk through wireless security issues, different types of encryption and how to configure security settings.	D.P8 Review the extent to which the organisation's	Students to answer a range of questions on the	Lit Social

	Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), WPA2. • Configuration of wireless router security settings.	**security issues?**	• **Tutor-led practical demonstration:** Demonstrate how to configure a WiFi router. • **Individual practical activity:** Learners practise setting up and configuring a WiFi router.	IT system has been 'protected'.	practical tasks they have viewed.	So8 C3 Sp2 Sp5
30	**D5 Access control** • Design and implementation of hardware and software access control regimes. • Defining legitimate users, groups and the resources they need to access and the levels of access they need.	**How do you set up file permissions on folders?**	• **Lead-in:** Recap on access control and user accounts and groups. • **Tutor presentation:** Explain user and group permissions, and access rights to resources, folders, files. • **Tutor-led practical demonstration:** Demonstrate how to set up file and folder permissions. • **Individual practical activity:** Learners practise setting up file and folder permissions following the demonstrated procedures.	D.P8 Review the extent to which the organisation's IT system has been 'protected'.	Students to answer a range of questions on the practical tasks they have viewed.	Lit Social So8 C3 Sp2 Sp5
31	**D5 Access control**	**How to define a Password?**	• **Lead-in:** Recap on passwords. **Tutor-led practical demonstration:** Demonstrate how to define password policies and white list applications. See	D.P8 Review the extent to which the organisation's	Students to answer a range of questions on the	Lit

	• Defining password policies. White listing of applications trusted signed binaries.		links: Securing OpenSSH and The Password Meter (testing passwords) in the following link https://wiki.centos.org/HowTos/Network/SecuringSSH www.passwordmeter.com/ • **Individual practical activity:** Learners practise defining password policies and white list applications following demonstrated procedures.	IT system has been 'protected'.	practical tasks they have viewed.	Social So8 C3 Sp2 Sp5
32	**D5 Access control** • Data hiding when viewing logs and visibility of sensitive data. Defining users with special privileges.	**How to adjust user privileges?**	• **Lead-in:** Discuss user privileges and data logs. **Tutor-led practical demonstration:** Demonstrate adjusting user privileges, data hiding and use of logs. See links: User Rights and Configuring privilege and role authorisation in the following link User Rights https://technet.microsoft.com/en-us/library/bb457125.aspx Configuring privilege and role authorisation https://docs.oracle.com/cd/B28359_01/network.111/b28531/authorization.htm • **Individual practical activity:** Learners practise adjusting user privileges, data hiding and using logs following demonstrated procedures. • **Plenary:** Q&A on the practical tasks.	D.M4 Enhance the protection of the IT system which to meet requirements given in the plan.	Students to answer a range of questions on the practical tasks they have viewed.	Lit Social So8 C3 Sp2 Sp5
32	**D6 Testing and reviewing protection applied to an IT system**	**How would you test the protection required in**	• **Lead-in:** Thought shower what would be required to test, review and evaluate the protection applied to an IT system. • **Tutor presentation:** Explain how to create and use a test plan.	D.M4 Enhance the protection of the IT system which to meet	Students to answer a range of questions on the	Lit Social

	Ensuring rules created do not prevent users from accessing resources required to do their job.	**an IT system?**	• **Individual practical activity:** Practise creating and using test plans. • **Plenary:** Q&A on the practical tasks.	requirements given in the plan.	practical tasks they have viewed.	So8 C3 Sp2 Sp5
33	**D6 Testing and reviewing protection applied to an IT system** • Firewall testing to check the firewall blocks unauthorised traffic and allows legitimate traffic through. • Viewing and interpreting activity logs. Judging the effectiveness of protection and making recommendations for further improvements.	**How to test a firewall and interpret the logged data?**	• **Lead-in:** How to test that the protection applied is effective. • **Tutor presentation:** Methods of firewall testing and how to interpret logged data. See links: How to test a firewall: A three-step guide for testing firewalls and How to test your antivirus, firewall, browser and software security in the following links: How to test a firewall: A three-step guide for testing firewalls http://searchsecurity.techtarget.com/tip/How-to-test-a-firewall-A-three-step-guide-for-testing-firewalls How to test your antivirus, firewall, browser and software security www.howtogeek.com/143263/how-to-test-your-antivirus-firewall-browser-and-software-security/ • **Individual practical activity:** Practise testing firewall settings. Viewing and interpreting log entries	D.M4 Enhance the protection of the IT system which to meet requirements given in the plan.	Students to answer a range of questions on the practical tasks they have viewed.	Lit Social So8 C3 Sp2 Sp5

34	**Summary of learning aim D and whole unit**	**Mock Assessment**	• **Lead-in:** Recap what has been covered in the course of the unit. • **Knowledge quiz:** Learners complete a self-marked informal quiz on learning aim D topics. • **Tutor presentation:** Summarise the key points of the unit, justifying the need for IT security and evaluating the effectiveness of the security measures that have been covered.	CD.D3 Demonstrate individual responsibility and effective self-management in the planning and protection of an IT system.	Students to answer a range of questions on the practical tasks they have viewed.	Lit Social So8 C3 Sp2 Sp5
35	**Mock assessment**	**Mock Assessment**	• **Tutor presentation:** Introduce the mock assessment. • **Individual activity:** Learners work on the mock assessment.	CD.D3 Demonstrate individual responsibility and effective self-management in the planning and protection of an IT system.	Learners complete the mock assessment as homework.	Lit Social So8 C3 Sp2 Sp5
36	**Summary of learning aim D and preparation for assessment**	**Assessment work**	• **Tutor-led discussion:** Give general group feedback on the mock assessment for learning aim D. • **Revision session:** Recap learning aim D topics, particularly covering any topics that learners struggled with on the mock assessment.	CD.D3 Demonstrate individual responsibility and effective self-management in the planning and		Lit Social

			• **Tutor presentation:** Introduce the assignment. • **Independent learning activity:** Complete work plan/schedule for the assignment, setting out when they plan to complete each part of the assignment. • **Plenary:** Q&A session on assessment.	protection of an IT system.		So8 C3 Sp2 Sp5
37	**Assessment 2** (learning aims C and D)	**Assessment work**	• **Assignment:** Learners work independently on the assignment for learning aim C and D. Learners to complete this outside class time.	CD.D3 Demonstrate individual responsibility and effective self-management in the planning and protection of an IT system.		Lit Social So8 C3 Sp2 Sp5