BTEC DIT

Component 3 Effective Digital practices

Learning Aim B: Policy

Knowledge and Assessment Organiser

Student name: .....

Who is responsible for data security?

Contents

Key terms

Exam question command words

Command verbs	Definition
Describe	To give an account of something, such as steps in a process or characteristics of something. The response should be developed as they are often linked, but do not need to include a justification or reason.
Discuss	Identify the issue/situation/problem/argument that is being assessed in the question. Explore all aspects of an issue/situation/problem/argument etc. by reasoning or argument.
Draw	Produce an annotated process either in the form of an information flow or data flow diagram
Evaluate	Review information then bring it together to form a conclusion, drawing on evidence, including strengths, weaknesses, alternative actions, relevant data or information. Come to a supported judgement of a subject's qualities and relation to its context.
Explain	An explanation that requires a justification/exemplification of a point. The answer must contain some element of reasoning/justification.
Give/State/Name	Require recall of one or more pieces of information.
Identify	Usually requires some key information to be selected from a given stimulus/resource.
Annotate the diagram to explain how ...	Label the diagram and provide an explanation for each identification.
Assess	Give careful consideration to all the factors or events that apply and identify which are the most important or relevant. Make a judgement on the importance of something, and come to a conclusion where needed.

Big Question: Who is responsible for data security?

- Small Question: What is a security policy?
- Small Question: What are the different IT policies used by organisations?
- Small Question: Who is responsible for security policy?
- Small Question: What is a password policy and device hardening?
- Small Question: What is the purpose of an acceptable software policy?
- Small Question: What is a disaster recovery policy?
- Small Question: Who is responsible for a disaster recovery policy?
- Small Question: What to do after an attack?

Essential knowledge

Security policies

Security policies describe how an organisation will secure its information systems. They set out the procedures that staff need to follow so as to keep systems secure and to minimise impact if there is a security breach. A designated individual will be responsible for each policy.

Types of policy

There will be policies to cover every aspect of an organisation's use of technologies. They may also be enforced by digital policies on network systems.

Area of technology	What the policy might include
Internet usage	What the internet can be and can't be used for while at work. Visiting inappropriate websites. Rules on downloading from the internet.
Email	Appropriate and inappropriate uses of email Procedures for dealing with attachments and precautions to be taken.
External devices	Rules on whether devices such as USB memory sticks and hard drives are permitted.
Passwords	Types of passwords that can be used (for example, complexity required, including length, combination of characters) and how often they must be changed. Guidelines on keeping passwords secure (for example, not writing them down or sharing accounts with other users)
Software	Software to be used for various tasks. Rules on downloading/installing software.
Personal devices	Rules about use of workers' own devices, such as smartphones, for accessing the organisation's systems.
Disposal of equipment	Rules about deletion of data from devices before disposal. Disposal of electronic equipment (WEEE regulations), reducing environmental impact of disposal.
Back up	How data is backed up, how often and by what method.
Device hardening	Rules and parameters for device hardening.

Defining responsibilities

To implement and maintain cybersecurity policies, companies will assign specific roles to IT staff or management. This allows for accountability and ensures staff are constantly aware of the actions they need to take.

- **Roles / responsibilities** – A member of the IT staff or management will be responsible for deciding what policies must be put in place. It's important that specific employees are assigned responsibilities for implementing these cybersecurity policies, usually members of the IT staff.
- **How to report concerns** – There should be clearly defined the person that staff should contact if they have a concern over a possible incident or poor practice. This is commonly the individual(s) responsible for implementing and maintaining the policy.
- **Reporting to staff/employees** – Security policies are only secure if staff are aware of the policy and its procedures. There should be someone responsible for making staff aware and training them on following the cybersecurity policies put in place.

Password policy and device hardening

Modern technologies can enable us to directly protect ourselves from cybersecurity threats. Security parameters can work in conjunction with these technologies to create a system which has better overall security.

Your cybersecurity policies will define security parameters that must be implemented and maintained to protect the business from harm caused by an incident. These parameters might include the following:

Password Policies

The password policy defines a set of instructions informing employees on rules they must follow when setting and protecting their password. This helps prevents attackers from gaining unauthorised access through cracking passwords or stealing data. A password policy will consider:

- **The don'ts of password creation** – A password must not be guessable, it must therefore NOT contain personal information such as common words, memorable phrases, or dictionary words. Also, you should not use the same password on multiple systems.
- **The dos of password creation** – A good password will be at least 8 characters, and will contain a variety of upper-case letters, lower case letters, numbers and special characters.
- **Protection of passwords** – Password must be stored in a secure database. They must be changed regularly, or immediately if generated automatically. It is important that passwords are never shared, or written down somewhere.

Device hardening

We've learnt in previous lessons that device hardening is the implementation of technologies to protect a system's data from harm.

Our cybersecurity policies will usually define the parameters for device hardening. This means what technologies should be implemented and how they should be configured and maintained.

For example, this might include:

- Anti-virus must be installed on all IT systems. Virus definitions must be updated every evening at 10 pm and a full scan of all storage devices performed at 11 pm.
- A hardware firewall must be installed between the company LAN and internet. The firewall must be configured to block all ports except ports 53, 443 & 80.

- Full-backups of company data must be performed every Sunday at 1 am. Incremental backups of changes will be made every day at 11 pm. Backups must be stored on the remote backup server.

This is just a few parameters we can set to harden our devices. If implemented and enforced then it will go a long way to protecting our systems from all kinds of cybersecurity threats.

Acceptable software policy

An acceptable software policy is used to control and restrict software installation on a system. The use of an acceptable software policy helps IT staff to prevent employees from accidentally downloading unauthorised material, which may contain malware or may conflict with current / older software and hardware. It is important to consider:

- **It's limitations during installation** – Tediously, employees may find they are unable to install any software without the permission of IT staff. To install a new piece of software, employees must request software they need installed to IT staff who will consider their request, and ensure the software is fit to run on the system.
- **Enforcement and punishment** – IT staff can enforce the policy by configuring an employee's access rights to block installation. Employees can be punished for breaching the acceptable software policy, this may include a warning, suspension, or restriction from using the IT systems, depending on the situation.

Disaster Recovery plan

A disaster recovery policy ensures an organisation's readiness to respond to a disaster. By keeping a detailed, well-documented plan, normal business service can be resumed as soon as possible.

Disaster recovery is effective in the event of all kinds of incidents that may harm business data, including data loss (theft, accidental deletion, internal threats or human error), environmental threats (natural disasters, fires, floods), hardware failure and malware attack.

Below is an example of the different considerations that need to be taken in to account in a disaster recovery plan. Each consideration is essential in ensuring that the organisation is correctly prepared:

- **Who is responsible for what** – the policy will define the responsibility for different staff in preparing for and responding to a disaster. This ensures people have accountability if something isn't completed correctly and reduces confusion in who should be doing what.
- **Dos and don'ts for staff** – the policy will define the procedures that staff members should follow and what they should not do, in the event of a disaster. This might be to tell staff that they should report an incident immediately to the incident response lead.
- **Defining the backup process** – the policy will define what data will be backed up, how often it will be backed up, when it will be backed up and where it will be backed up to. These will depend on the

business. For some, weekly backups on a Sunday evening is fine. But others that will be nowhere near often enough.

- **Timeline for data recovery** – the policy will define the priority systems that need to be restored asap and show the timeline for how long it can take to recover each system showing the order in which we should target recovery after a disaster.
- **Location for alternative provision** – the policy will likely define where additional hardware, software & personnel are available to continue business operations while the main site is recovered. Many businesses will pay for a "hot site" where they can instantly switch business operation over to after a disaster.

Actions to take after an attack

Employees must be aware of the actions they should take following an attack so that the organisation can resume its functionality as soon as possible and minimise potential damage.

A business will normally take the following steps: investigate, respond, manage, recover and analyse.

Action	Description
Investigate	• Investigate the attributes of an attack to determine a response. Identify when and why the attack happened, the type of attack that has occurred, and how the organisation's core services have been impacted. Establish the severity of the attack, which can be used to decide the level of response required.
Respond	• Inform the relevant stakeholders (e.g. customer, employees & suppliers) the attack has affected as well as relevant authorities (e.g. the police). It is especially important to inform customers, as a data breach will require action from their end (i.e. changing their password). It's also a legal requirement and if not done, could lead to massive fines.
Manage	• Isolate & contain the attack to prevent it from causing further damage. Target the problem, using appropriate measures to resume services where appropriate (e.g. using a firewall to block malicious traffic).
Recover	• Implement the disaster recovery policy in order to correct any damage caused by the incident (e.g. restore the most recent backup). This may involve establishing new plans to stop similar attacks in the future.

Action	Description
Analyse	• Work with employees to establish information about the attack to help prevent future threats. Analyse why, how, who and the lessons learned in order to assess what changes can be made. Update policies and procedures as a result of this analysis.

B3: Exam Questions

A local travel agency sells holidays through high street shops and online.

The travel agency has an Acceptable Use Policy.

Explain **two** purposes of this policy.

(4)

1 .....

.....

.....

.....

2 .....

.....

.....

.....

Question Number	Answer	Additional Guidance	Mark
	Any **two** explanations such as: • So staff know what items are covered (hardware, documents) (1) and how they should be treated. (1) • So staff are aware of how they should behave (1) and what they shouldn't do when dealing with other staff and customers. (1) • So all staff can sign to say they will agree to all conditions set in the policy (1) and are aware of any sanctions that may be put in place if the agreement is breached (1) • So the company will be able to monitor their staff (1) and if there are issues they can be reprimanded/dealt with. (1) Accept any other appropriate response	• Award one mark for a purpose and one mark for a linked explanation of that purpose • Purpose and justification may be reversed. • Each purpose can only be awarded a maximum of two marks	4

Articles for Wider Reading and Flipped Learning

Subscribe and watch the YouTube clip on Cyber security.

https://www.youtube.com/watch?v=jGBdmHvNXfs&list=PLmyUnKEeJk-6gijRiVKEfcvZhwcj6LWpo&index=5

(ADD QR CODE FOR ANY LINKS)

Policies - Know it all Ninja

Read through the topics on **security policies.** Remember to complete the on-line quiz to gain house points!

https://www.knowitallninja.com/modules/policy/