Unit 7, P4

Thomas Robinson

SOLIHULL COLLEGE

Disaster Recovery Policy

A Disaster Recovery policy covers what events are taken when a disaster occurs. This can be human-error—such as accidental file deletion—or an uncontrollable event—such as hardware failure.

Often it will contain how data is stored and replicated, and what actions must be taken to restore data. If the company has one, it may also set out instructions on how to switch to an alternative site or instruct employees to work from home.

Updating of Security Procedures

Security Procedures should be kept up to date on a regular basis to ensure they cover new potential threats that may have emerged against the organisation. This can cover both physical threats, and virtual threats and may include tasks such as updating antivirus software and intrusion detection systems.

Scheduling of Security Audits

Regular audits ensure that the security procedures and policies are being adhered to. This could consist of checking that CCTV cameras or antivirus software is operational.

Codes of Conduct

Codes of conduct are sets of rules that govern the use of devices, service and equipment that belong to an organisation. For example: a company email policy may restrict the usage of the corporate email to only official purposes with no personal use; or an internet usage policy may stipulate that social media access is prohibited during work hours.

There can be additional policies and procedures relating to the setup and configuration of hardware and software that govern software licensing and hardware acquisition.

Surveillance Policies

Surveillance policies outline how employees may be monitored. This can include anything from computer logging to CCTV. These policies must outline exactly what surveillance is being carried out, by whom and why.

Risk Management

Risk management involves identifying potential issues that could develop and outlining how they will be dealt with. The importance of allocating time to each risk can be ranked by judging the likelihood of it happening.

Budget Setting

Budgets for all policies—especially security—should be clearly outlined. There should also be contingency available in the event of an unforeseen disaster or issue.

Unit 7, Assignment 2 – Task Two (P5)

Thomas Robinson

SOLIHULL COLLEGE

Hiring Policies

Includes background checks which check legitimacy of qualifications, credit score, social media as well as gathering information from references to assess a worker's competency. Also includes criminal record checks. Would improve Oadby College's IT security since new employees would be vetted for past wrongdoings and competency for the role.

Separation of Duties

Ensuring that one employee does not have the burden of too much responsibility so the company or department can still function with their absence. Can help security by restricting what information people have access to read or modify.

Training

Informs the employee on how to perform their duties and access common company services. Could also cover specific tasks such as fire safety or first aid. Will ensure Oadby staff are performing as best they can and are able to do their jobs effectively.

Unit 7, Assignment 2 – P6 Legislation

Thomas Robinson

SOLIHULL COLLEGE

Legislation (P4)

Computer Misuse Act (1990)

This act prevents unauthorised access to computer systems (hacking) as well as unauthorised access with intent to commit further offences. It additionally covers unauthorised modification of computer material and making, supplying, or obtaining anything which can be used in computer misuse offences.

Copyright Design & Patents Act (1988)

The C, D & P Act protects intellectual property, such as brand names, stories and designs.

There are different protections that can apply to works: copyright, patents, licensing, and trademarks.

Copyright

Copyright defines rights the creator has over their own work. It also applies to digital work, such as music, videos, code, etc. Does not need to be applied for – it is automatically assumed when you create a piece of work. Copyright makes it illegal to copy work without permission; the owner can take legal action.

Patents

Patents give the inventor the right to decide if/how an invention can be used by others.

Trademarks

Trademarks cover brand names, logos and other "service marks."

Data Protection Act (2018)

- Governs handling of personal information
- Affects both data held in paper and digital forms
- Upheld by ICO
- Healthcare Records
- Criminal Justice
- Financial Institutions
- Biological

All businesses must register with ICO and state what information they hold and why.

The Data Protection Act governs the handling of personal information by organisations. It applies to both data held in physical and digital forms. It requires that all businesses register with the ICO (Information Commissioners Office) and state what information they hold and why.

There are eight principles of the data protection act – they are to make sure that data is:

- used fairly, lawfully, and transparently
- used for specific, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, when necessary, kept up to date
- kept for no longer than necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Unit 7, Assignment 2 – Task Four (M3)

Thomas Robinson

SOLIHULL COLLEGE

Ethics of CCTV

For:

- Capture evidence of crimes and wrongdoings
- This deters criminals
- Create sense of security

Against:

- Improperly configured cameras could capture personal information (for example, on computer screens in an office or documents on a desk)
- Expensive
- Cannot protect against all crimes (many will be undeterred)

Watching Live v Recorded

- Live monitoring can spot issues before they escalate but could be considered creepy or unnerving knowing someone is watching
- How is recorded video safeguarded? Under what conditions is it accessed?

What if party responsible for watching/recording abuses power?

- Leaks of data (company info/secrets, personal information)
- Leaks of happenings the company may not wish to have exposed (eg: Matt Hancock's snog)

Freedom of Information Act & The Electoral Roll

What is the Freedom of Information Act?

The FoI act only applies to public-sector organisations such as government agencies and local authorities, which reduces the scope for unethical behavior significantly. Exemptions to the act disallow fulfillment of requests that pose a significant burden or could harm staff or the requestee, and one is unlikely to get detailed information about a certain individual since these requests can also be refused.

Broad information pertaining to sensitive information can and has been requested, for example, the number of LGBTQ+ staff employed at a business or internal communications, messages, and policies. Additionally, what is considered in the "public interest" can vary from person-to-person and therefore which information is acceptable to make available can be uncertain.

- Only applies to public sector organisations

- Exceptions disallow tasks that pose a significant burden or could harm staff/the requestee
- Unlikely to get detailed information about a certain individual
- Could get broad data about groups of people that may object
- What is/isn't in "public interest"

What is the Electoral Roll?

The electoral roll is a large database of everyone in the UK that has registered to vote in local or national elections. It contains full names, addresses and other occupants of the household.

There is a public copy—called the "open register"—that is available to everyone for a fee or through certain websites. It is possible to opt-out of the public copy of the record.

A private copy is made available to organisations for the purpose of proving one's identity. It is held by institutions such as banks and credit agencies who often obtain a new copy every 28 days. It is also used for electoral purposes, such as sending out poll cards and political campaigns. It is not possible to opt-out of the full register.

- Name, address, other occupants at address
- Is opt-out if you do not wish to be included in the public copy (though you will still be in private copy available to businesses that require it)

Oadby College's Use of Data

Oadby College obtained a copy of the electoral roll using the Freedom of Information Act and used the addresses contained within it to send out prospectuses (marketing content).

Whether this was a violation of privacy depends on which copy of the electoral roll was received. If only the open register was used, you could argue that this data is meant to be public in the first place since anyone can purchase a copy. However, under the Freedom of Information Act, the requestee should first check that the information is not available from other sources. Oadby College should have purchased a copy of the data rather than procuring it in this manner. Additionally, the Freedom of Information act states that any received information should be fit for public publication and does not "unfairly" reveal any personal details. People in the open electoral roll had the option to opt-out and chose not to, so the release of their information could be considered fair and expected. However, under the Data Protection Act, the use of their personal data for marketing communications without express consent could be considered unlawful.

Unit 7, Assignment 2 – Task Five (D2)

Thomas Robinson

SOLIHULL COLLEGE

What measures are currently in place? How can they be improved?

Oadby College currently has a range of varyingly effective security measures already in place.

The college has network access control levels in place using user groups. These groups are “staff”, “student” and “administrator.”
This provides some segregation for permissions however I would suggest introducing further fine-grained groups. For example, staff should be split into job roles and assigned permissions appropriate for them; a caterer does not need the same level of access as a tutor.

Staff are currently required to change their passwords on a monthly basis, which was previously common practice. However, the National Cyber Security Centre has released further password guidance that suggests this is a poor policy, since it encourages the use of simpler passwords that are easier to remember and update. Additionally, if an attacker was to gain access using a compromised password, they would likely make use of their access immediately and therefore a monthly password change would no nothing to stop them.

IT Suites and offices require swipe card access. This is effective since the access to these areas can be restricted to certain individuals or groups and logs can be kept regarding who accessed which area and when. This system would be more effective if it was extended to all rooms, rather than just offices and IT rooms. This would allow the college a greater level of analysis about the paths their staff and students take around the building as well as logging who was in what location and when.

In addition to the swipe cards, IT suites and their surrounding corridors have CCTV coverage. This allows the college to monitor for any wrongdoing, particularly theft in the case of the IT suites. Again, this CCTV system would be more effective if it covered all corridors and common areas as well as outdoor spaces. This would ensure greater security.

When enrolling at the college, adults are required to sign and agree to an IT acceptable use document. There are no guidelines covering the use of email. This acceptable use document should be extended to govern the appropriate use of email and should be agreed to by all staff and students, not just the adult students.

Incoming emails are scanned for viruses; this could be extended to cover incoming and outgoing emails. Virus scanning should also be in place on end-devices. It was not specified which antivirus solution is used, how often it is updated and who is responsible for its routine operation.

It was additionally not stated on what schedule software and hardware is refreshed and kept up to date.

Further Recommendations

In addition to the measures already in place, the following could be implemented to further increase security.

The College could implement visitor passes and allow visitors and guests to sign in/out upon arrival and departure. In addition, these third parties could be required to have an escort to keep an eye on their activity when in the building.

Security guards could be employed to look out for suspicious behaviour and to monitor CCTV and network traffic and computer usage could also be monitored.

The IT team could draft a disaster recovery policy that outlines how the college would recover from data loss or another incident. This would also outline what measures are taken to ensure data integrity and data security as well as how the College is complying with data protection legislation.

Staff and students could both be trained to be aware of common risks and threats and how they can be overcome or avoided.