Policies and guidelines

Contents

* Budget setting
* Disaster recovery
* Updating security procedures
* Scheduling security audits

Code of conduct

* Email usage policy
* Internet usage policy
* Software acquisition and installation policy
* User area usage policy
* Account management policy

How employment contracts can affect security

* Hiring policies
* Separations of duties
* Disciplinary procedures
* Training and communicating with staff as to their responsibilities

Budget setting

Having a well managed budget setting means that an organisation is able to regulate, and monitor well how finances within a company are spent. It is essential to check yearly of an organisations budget setting and management of finances in order to ensure that organisational systems security is looked after well at an acceptable level. If an organisation such as Technology Today were to have a good budget setting, this could mean that they are able to keep a good budget for things like software licensing, audit costs or even costs based on staff training. It is best that the organisation keep a good and balanced budget in order not to go over budget.

Disaster recovery

When human or natural disasters occur, a disaster policy is to be followed in order for users to know what actions are to take place when these disasters happen. Whether the disaster is a fire, system or equipment failure or a computer virus the policy would have to be followed. If any of these disasters were to occur, this would mean that for example if there were to be a fire, important files and documents saved onto a computer could be backed up and would be able to use.

Updating security procedures

Regular updates and reviews of security procedures should be carried out on a recurring basis. It is essential for the required security to carry out these procedures in order to have updated information, for example if a security threat were to occur, and a security procedure is needed and is out of date, the information that was attained previously, is only useful at that specific time, whereas updating and reviewing security produces will provide new and useful knowledge that is able to deal with threats and to maintain a secure system.

Scheduling security audits

Security audits are done in a way to test how a company’s information security is doing. They can be carried out without informing employees within the organisation to ensure the company’s effectiveness of their systems. Scheduling security audits in an organisation ensures that a high level of security is made in order to protect information and data. When dealing with networked systems, scheduling an audit means that an analysis would be done in order to detect issues that may occur, such as threats. As security audits are made up of a series of tests, these tests make sure that information within a company is secure and up to standards.

Codes of conduct

Email usage policy

When sending an email, the policy oversees what types of subjects aren’t allowed whilst sending emails. If a user were to want to send attachments as part of their email, the email usage policy states the limit of attachments that can be sent and which file formats of an attachment the user can send. When it comes to issues of sending emails, sending information to external parties deliberately is stated as unacceptable behaviour as well as frequent issues, for example harassment, stalking, and spamming.

Internet usage policy

Network management tend to monitor network traffic, and so for example, by having the network monitored, if in a school or a workplace and an employee or student were to use the internet inappropriately, this determines exactly which websites cannot be used in the future, and which content cannot be downloaded. Also having the network monitored means that it could prevent workers from using websites with viruses and other treats trying to access the network.

Software acquisition and installation policy

The main reason to having software acquisition and installation policy is to prevent personal and unlicensed software from being installed onto their systems due to the fact that it is unlicensed and so duplicates cannot be made. Having this policy means that it prevents threats that could affect their system as well as traffic and compatibility issues. Software acquisition means being able to manage software being installed, for example, an organisation maintaining and managing software acquisition means that if the organisation has different departments, and one department wishes to install a software that is already on the system, it is unnecessary as it is already on the system, but is being used in another department. The organisation wouldn’t want to have duplicate of the software as it also means that money if spent a second time on that software. So it is best to follow the policy to keep out threats and not to have duplicates of software, as well as saving money.

User area usage policy

When it comes to copyright not being infringed in for example a college, as their system will contain a big amount of storage space for both users and staff, it is ensured that staff and students are told exactly what cannot be downloaded and stored onto the system to prevent copyright infringement if a user or staff were to download a file which has been asked not to be downloaded. Although, for example in an IT department of the college, the IT staff (and students) would require larger amounts of storage space for software (such as Adobe, Microsoft Office etc.) that both staff and students would use in lessons. This means that storage in the college could vary according to which department, or user most needs it.

Account management policy

Having an account on a computer system of an organisation or college consists of a user having a user ID and password. The account management policy comes with two sets of rules stating that:

* The user is to be responsible of maintaining a high level of service when using the network within the organisation/college
* The user is to not share and give out their password to anyone and to ensure that their passwords are current

How employment contracts can affect security

Hiring policies

Hiring policies occur when a company decided to hire a new employee. For example, when hiring a new employee, they would have to make thorough background checks, checking if the person has not got a criminal record, where they have previously worked and their references. The reason to this is to make sure about their decision of hiring the person; they would have to require such information as to where they have previously worked to make sure that they are hiring someone that is legit and hasn’t got a dangerous background that could affect the company’s reputation.

Separations of duties

Organisations tend to use teams in order to split responsibilities out t each member of staff in the team, making sure that every team member has duty to tend to, whereas if only one member of staff were to be dealing with responsibilities such as on system security, not everything needed will be done at once and the person may not fully understand what to do and not have full knowledge of the system, like a full team would have. Having a team deal with systems security ensures that the process is quick and fast, and that no other duties are left out.

Disciplinary procedures

Within an organisation, handling matters such as infringement has to be done in an exceptional procedure. For example, and employer cannot blame or accuse an employee for something they might not have done as it could lead to serious legal action. The procedure that would have to follow is to:

* suspend the employee, still paying them
* having a paid team to investigate the situation in a fair and understandable manner
* involve the police if it turns out to be a criminal situation

Training and communication with staff as to their responsibilities

After an employer has hired new employees, it is permitted that they receive the training that they need in order to be correctly sure of their responsibilities within the organisation, and when it comes to communication within the organisation, by having it practised, this ensures that new employees can maintain good communication with other staff when needed, for example if there were to be a problem with the security of the system and they require some help, they are able to call upon another staff asking them for help.