Linnéuniversitetet
Kalmar Växjö

Assignment 4

Security Policy
ISO - 27002

Authors:
Adam RASHDAN *ar223hf@student.lnu.se*
Kalid DIRIYE *kd222gb@student.lnu.se*
Rashed QAZIZADA *rq222ah@student.lnu.se*

Area: Computer Science
Supervisor: Ola Flygt
Course code: 1DV700
Semester: Autumn 2020

Contents

1 Information Security Policies

The management of data security objectives, by the organization should be documented. The objectives and policies should be approved by concerned officials and it must contain both high- and low-level policies. Later they must be approved by the organization.

1.1 Reviewing the Information Security policy

There is a dire need to review and revise the policies on regular basis. For this purpose, regular sittings should be arranged to review the policies, as in to make any changes. Once there is anything which is approved/suggested the higher officials need to approve this update.

2 Organization of information security

2.1 Roles and Responsibilities in IS Policy

The responsible persons are required to be appointed/defined. The persons will be responsible for information security risk, all the assets in the organization and also the processes involved with the organization.

2.2 Segregation of duties

There is a good possibility that a person may misuse its powers and company's assets. To avoid such incidents, it is required to divide and distribute such important tasks/assets among multiple persons. There is also some log which records all such activities. One example could be the person who signs and delivers all the checks for the organization. He can be drawn away for any reason.

2.3 Contact with authorities

It is also required to appoint or make persons responsible for contacting outer world people organizations. Like in an organization, people should know who is responsible for to contact with law enforcement agencies in case of any emergency, who is responsible for supervisory issue etc. This helps in reducing the impact of any unforeseen circumstances.

2.4 Contact with special interest groups

It is important to have latest security trends are practiced in the organization. For this purpose, special interest groups should be kept in good terms with the organization. For sometimes, the groups should be asked to have the advice for the organization.

2.5 Importance of IS in Project Management

The security of information should be well documented and also it should be placed in all the projects under the organization. The information security policy should also be made available to all the employees. Moreover, if there are any handbooks available for employees (under project management), then a chapter Information security should be included.

2.6 Mobile device policy

Mobile devices are a risky for the security of the organization. There should be a clear policy about if a person can use his own mobile device within the organization. There could also be case where mobile usage is dangerous for the information security in any part of the organization, hence the use of mobile phones should be prohibited in those areas of the organization.

2.7 Teleworking / working from home policy

Work from home policy should be made for the organization. There should be a clear policy that under what conditions an employee can be allowed to work from home. In the case, it should be made clear that which software is going to be used to access the premises, what network he an use for this purpose, and also what parts of the organization he can access.

3 Human resource security

3.1 Pre-employment screening

To hire new employees, there should be a well-documented policy for the initial screening procedures. For future employees, the organization should respect the confidentiality of their data and check whether the future employee is of any harm to the organization i.e. trust etc.

3.2 Terms of employment and information security

The contract of new employee (as well as all the employees) should contain the information security policy. Every worker who works for the firm should sign the contract containing information security policy. It important for everyone (specially the new ones) to know about the information information security policy.

3.3 Responsibility of Management

The major role for implementing the information security policy is Management. They should be an example for all the employees and contractors by showing and practicing the information security policy in a true sense.

3.4 Security awareness training

All the workers should be made to attend training sessions. These sessions will teach the importance of information security. The training for different area of workers, would be different. As all employees don't deal/handle same nature of the information. If a worker is promoted to some new position, then he must be trained for the specific post regarding the information security policies.

3.5 Disciplinary process

If any employee practices the violation of the information security policy, a strict disciplinary action must be taken against. This is necessary to be taken care of, as it will aware

the employees about the importance of information security policy and also it will also reduce the chances of same thing happening in future.

3.6 End or change of employment responsibilities

When a workers' job ends in an organization it is not obvious that their information security duties end as well. A specific policy or non-disclosure agreement must be signed by the employee and the contractor, to ensure that they will comply to information security policies even after leaving the organization, may be for a year or two.

4 Asset management

4.1 Inventory of assets

Data operating resources should be known to the firm. These resources must be listed in a directory and this directory should be well maintained. It is important to know that what assets organization currently own, how to use those assets and where those assets are at the moment. Knowledge is essentials of these resources/assets as it may help in knowing what harm they can produce. Such information about assets, might also help in the insurance and legal issues.

4.2 Ownership of assets assigned

To better take care of an asset. It is important that it must be assigned to an employee or a group of employees. This means, every asset in an organization must have any owner. This means that the owner will be responsible for the specific asset. This also helps in tracking the assets throughout its life cycle. But still the asset's health and condition should be daily monitored by the responsible person. Still the responsibility of the asset remains with the owner. Before assigning an asset to the employee, it must be approved by the relevant person in the management of the organization.

4.3 Using Assets in Acceptable Manner

All resources should be accessed meeting certain requirements. It is required that the user/owner of a certain asset must be aware of the information security policy.

4.4 Return of assets

There could be cases where an employee is not in need to a specific asset due to moving to a different department or the contract of an employee is expired. In such cases, all the resources/assets must be returned to the management. It is important to make a very clear policy for such cases, and this should be known to all the employees. And in case, if there is any knowledge with the employee which is not documented, it should be documented and returned to the officials.

4.5 Classification of assets

There are different types of resources in the information some are confidential, and some are not that important in terms of confidentiality. There should be a clear policy, which make assets non-confidential to severely confidential. The accountability of the confidential resources/assets depends completely on the handler of the resource.

4.6 Labelling of information

The information within an organization can be from categories, so it is important to label the information properly. In this way, we can easily classify the information in different groups. It is also important to keep track of the labels and information as it also adds a good amount of risk on information security. By this way, if the data is misused, at least some authorized personnel know where it belongs to.

4.7 Handling of assets

There should be a policy in place which deals with the handling of assets. To use resources the workers, need better understanding of the labeling and the way they are arranged into groups, their modifications, so there are least chances of the data to be misused. It is also important for the employees to know about the type of classification used by other organizations/departments, as it may differ.

4.8 Removable media management

Management should set up a procedure how remove-able media such as USB sticks, hard drives, and CD's are handled. Every aspect of these remove-able devices should be monitored carefully as in where these devices are used, how are they used, level of security these devices offer. There should also be some restrictions on what type of files can be stored on them and also in which areas of the organization it is allowed to use such media.

4.9 Disposal of media

The disposal of data is of immense importance in today's age. If any data/information is not required anymore, it should be carefully disposed of. And if the confidential data needs to be disposed-of, then the organization itself must take care of the disposal. If certain precautions are not followed, it may harm the company's strength.

4.10 Physical transport of media

There are instances that the media, can be stolen or the information is compromised, during physical transportation of the media. To make sure, and minimize the risk of information theft, it is important to have proper guidelines regarding the transportation of the media, like which couriers is to be used, how the data is encrypted, how the media is going to be transported etc. It can also be documented, where it is mentioned, what data is sent, how it is sent, and also how it is made secured, to avoid any sort of corruption or disorganization.

5 Access Control

5.1 Business Requirements of Access Control

For a business to run successfully, it is required to apply access control policy. The goal of the policy is to limit access to the information and processing facilities. You need to create an access control policy to define how access is managed and permissions. The rules for each asset are as follows: Access Rights Often, the property owner's employees who set access requirements, restrictions, and privileges on the asset, and the rights required to

access the facility to perform the task are defined. It also reduces the risk of disruption of critical business processes. Network access management is important. This is because the organization's complete network is not running and cannot be protected within the organization.

5.2 User access and information management

It is important to use a secure user access management. The use of secure access will make sure that no unauthorized access to systems and services is obtained. The other important feature is to have a user registration and unsubscribe system is required to provide user access and track usage. As an employee, you can set limited access as needed. ID sharing is not recommended as it will prevent you from tracking the correct users. User access permission is required. The system has a specific role based on the activities performed by specific types of employees and special permissions allow the same basic access when it needs to be managed as carefully as all administrators. have perks. This must be done officially, but the consequences of abuse are serious and need to be managed with care. Password, etc. Some protocols also force users not to share confidential references and require users to change their passwords. You need to use it first and run some secret credentials. Employees in your organization are not consistent, so you should check your access rights regularly. basis. Multipurpose access rights are sensitive and should be checked more frequently. If any of the employees have completed their tenure, the recipient's access rights must be removed. If the former employee has access to the service, the password should be changed immediately. Unauthorized access by former employees / partners can be quick and effective, so policy. No matter how perfect the policy, administrators need to make sure that all employees actually follow it.

5.3 System and application access control in privileged security program

the unauthorized access is critical in any system. To prevent unauthorized access to systems and applications, a mechanism is needed to control system access and application. If any policy that restricts access to any information or system or uses a secure login process should be implemented in practice, the password management system should be secure and follow the organization's confidential references policy. The password itself must be stored securely and transmitted by the password management system. It is important to strictly control access Use of privileged utility programs Ability to override access and system control can affect performance. Source code is the most valuable piece of code a system has. The source code of internal applications should not mean that unauthorized personnel have access and that authorized personnel should be regularly managed and reviewed.

6 Cryptography

6.1 cryptographic controls

Therefore, you need guidance on using cryptographic controls that specify when cryptographic control is needed and what type is appropriate for the situation. Encryption key management is another important thing to keep secure. This includes key generation, storage, retrieval, distribution, revocation and destruction, and there must be a policy to

manage keys throughout their life cycle, which may include the required length, algorithms used, and storage.

7 Physical and environmental security

7.1 Security perimeter management

Another important security perimeter is physical security as handover to the workplace may be attempted. Therefore, several measures must be taken, including entrance doors, closed offices, and reception areas with staff to control access. Access must be granted, and documented Visitors must not be allowed, if so, they must be identified. To protect offices, rooms and facilities, it should not be accessible to the public. The processing of the information takes place internally, and the better way is location. Organizations must be able to protect themselves from external and environmental threats. This includes adding multiple physical barriers to strong and safe buildings against natural disasters and unnatural threats such as mobs or breaks-ins. Safe areas may exist due to their classified or dangerous properties. In order for people to work in a safe area, the rule must be established. In order to protect the contents of the safe area, organizations should consider banning video and audio recording devices. The organization's shipping and loading area is an area that is not-it is an organization HR job, so the area must be secured to prevent unauthorized access such as Zones can be in remote parts of the building and exit entries must be properly separated and properly inspected.

7.2 Supporting utilities

Devices must be consistently localized and protected according to their classification. By controlling all types of access, equipment can be protected from damage, tampering, and unauthorized access. All support facilities must anticipate risks to avoid negative consequences. They should be regularly tested and able to perform automatic failure detection and can also provide backup for the facilities. In addition to communication, cables should be protected from damage, interference and interception. For this purpose, the cable should be placed under the floor or in / Behind an invisible wall or shielded with electromagnetism. Equipment should be well maintained to avoid damage or tampering. The recommended maintenance interval and the requirements of the insurance company should be observed. All errors should be recorded. Maintenance work can only be performed when authorized by personnel.

7.3 Physical Movement of Assets and their security

Sometimes assets can be moved off site, with many risks, beyond the control of the organization, they are easier to handle, unauthorized access or damage. Why and how long the asset will be off site. The building should be secured, protected. To mitigate this risk, the organization may exclude any off-site activities by regular personnel. Certain media that require proper process control can be reused, media may contain classified content that cannot be retrieved by overwriting, otherwise media should not be reused and physically destroyed during use and therefore should be protected adequate. Log sessions should be terminated automatically after a short period of inactivity and personnel should manually log out after the session. To ensure there is no information. , it is possible to gain unauthorized access to information on the desk or in the system, the desk should not contain

any physical information resources or media, and a computer should be logged off in the employee's absence.

8 Operations security

Operating systems must be officially documented and made available as official documentation for machine users. From the simple process of using a computer to use sophisticated tools, everything in the manual must be addressed. Great business process. For auditing purposes, it should be kept by the councilor. Managing the skills actually involves quite a large portions of the organization, so it is required to know the size of the organization, like how big it is. Hardware and hardware products can be developed (to make changes) either to improve working software / hardware or to create something completely new. Software and hardware should be checked before operating.

8.1 Malware Attacks and Prevention

Organizations must have the controls to detect, prevent, and repair malware attacks, and it is important that all employees are aware of the risks of malware, work safely, and educate them how to block malware.

8.2 Backup information policies

Backup policies are a well-known information security measure. Appropriate steps must be taken to back up information, software, and system images. Backups are so important that they need to be properly encrypted. You also need to check the backup. Integrity and whether they actually work.

8.3 Logging important data

Event logs are important for monitoring what's happening in your organization. Most electronic devices can log all user activities that capture security failures and incidents. To identify an issue, the logs can be checked, which may be in the audits. Logs are required to protect your information from interference and destruction. A good way to maintain log integrity is to automatically backup your logs to locations that have extreme control and access requirements. Similar accounts can access logs and other crates. It is important to restrict access to your logs by another level of logging system that privileged users can't access. The synchronized clock should be used on all systems. In this way you can carry out the activity. Many systems have been tracked correctly. The administrator should write down how to select the reference times and how to perform the synchronization.

8.4 Software and System installation and usage

The software installations are very critical for the security of the systems. There should be a proper control on the software installation. There must be a written about the installation of the software and also for who is responsible for the updating and uninstalls (if required). Otherwise it may have adverse effects.

Since it is almost impossible to operate a system without technical vulnerabilities, there must be adequate procedures and measures of action to detect them. A good way to

prevent this is to limit the user's access so that users cannot install the software themselves and have IT personnel install it after approval.

Audits can require in-depth access to a wealth of information, which will not disrupt the day-to-day operations of employees.

9 Communications security

You need to manage all networks in your organization. You should have an accurate overview of all networks and methods of protection to protect the information on your system. You can separate the network, not the entire network, system validation, and local access to the system. Service contracts must be entered into for all networks, irrespective of where the service is being provided (internally or externally). These agreements must clearly mention about the security mechanisms implemented, the level of services and all the requirements which are already set by the top management.

Information is shared inside and outside the organization. To reduce the risk of information leakage, there should be laws on the sharing of information in all forms, including digital documents, physical documents, and videos. As information transfer agreements are confidential, it is important for organizations to identify, legalize, and update these needs.

10 Acquisition, development and maintenance of System

Information systems have different requirements for security which are associated with them. The requirements may be based on legal issue or linked compliance of standards or regulations. All such requirements need to be properly documented and the management should ensure that the it is implemented in new information systems. Virtual Private Network (VPN) software was used. The relevant information must be protected from unauthorized access, redirection, copying or alteration. Signature of both sides.

10.1 System security policy

Information security begins with a secure system. Secure software and system development rules need to be documented by the organization and implemented during the development of new software and systems. If the system is installed for organizational development, system changes need to be formally documented. You should avoid automatic updates to critical systems that can cause your organization's systems to fail. After making changes to your system, you need to check performance and security. Making this a company policy ensures that processes run consistently and prevent unnecessary work interruptions and risks.

For all outsourced development, a complete consensus must be set, and requirements clarified prior to collaboration. Organizations need to be able to audit the development process and test deliverable before acceptance. During development, new / security updated systems should be thoroughly tested. Testing is best done by using realistic test inputs to the system and critically evaluating the output. Acceptance testing of new / updated systems requires well-documented and rigorously applied procedures. The test itself should be run independently of development and organizational security requirements.

Testing should be done in real-world situations using real test data. To mirror real world applications, insensitive operational data must be used for testing and it should be certified before use. Tests should be well documented and recorded for auditing and all operational test data will be removed after testing is complete.

11 Supplier relationships

11.1 Information security policy for supplier relationships

Since suppliers have access to certain assets, organizations need to establish a policy outlining the requirements to mitigate risk and documentation of delivery history. It is important that the policy is placed well before the start of supplier relationships. Both parties must agree upon such policies which may include, non-disclosure agreements, the process of supplying the products and any related documentation.

11.2 Addressing security within supplier agreements

There are chances that a supplier may be exposed to organization's information directly, or indirectly. So, the suppliers must agree and comply with established information security requirements. There are issues with the time of supply and when a specific supplier is done with the supplies in future, it is important to document it properly.

11.3 Information and communication technology supply chain

Any contact which is made with a supplier must specify the information security requirements which need to be fulfilled. This also applies to any contract for ICT services and supply chains. The example items should from supplier items should follow proper requirements, and a minimum level of security should be maintained.

11.4 Monitoring and review of supplier services

There are various issues which the suppliers which may arise over the time. The mistakes can be made accidently or on purpose. There could be instances when the right product is not delivered. It is important to keep track of the supplier and review its level of trust after some time. In this way the organization will keep track of the supplier, if there is some issue arises.

11.5 Managing changes to supplier services

The supplier services are as important as the system changes. So, it is required to make sure that the information security policies are up to date. If there is any change in the policy, it should be managed properly. As the outdated information security policies can create big new risks.

12 Information security incident management

12.1 Responsibilities and procedures

Management establishes responsibilities and procedures to ensure a fast, effective and organized response to address security vulnerabilities and incidents. It is simply an

event where some form of loss has occurred around confidentiality, integrity or availability.

13 Reporting information security events

Information security incidents and events can be reported through appropriate management channels as soon as possible. Employees and related stakeholders (e.g. suppliers) must be aware of their security incident reporting obligations and cover them as part of the general. Awareness and training play a vital role to identify the issues and their level of severity.

13.1 Reporting information security weaknesses

The weakness information security system is not of critical level, but it can prove to be lethal. As in the case of a weakness in the system, it is possible the incident can be avoided. It is essential for employees to be aware of the fact that when a security weakness is discovered, they must not try to prove it, as testing it can be understood.

13.2 Assessment and decision on information security events

Organizations must have a well-documented policy to investigate/assess the information security breach. If there is any such incident, then the responsible person should investigate the incident. Once a security event has been reported and recorded (for later future use), it will need to be evaluated to determine the best course of action to take.

13.3 Response to information security incidents

The individual assigned to handle security events will be responsible for restoring the normal security level by following all the procedures which are well documented. The whole process needs to recorded for future records.

13.4 Learning from information security incidents

Once the incident is resolved, it should be put into review and learning state. The responsible person should discuss the issues faced during the resolution of the incident. This will help in resolving future incidents and also to identify if there is some systematic issue.

13.5 Collection of evidence

To identify an incident, the procedure to identify, acquire and preserve all the related information is required. The information can be used as an evidence so special care should be taken in such cases. If the organization suspects or knows that a security case could lead to legal or disciplinary action, the Evidence collection must be carried out carefully, ensure good custody, and avoid threats to be caught by officials.

14 Business Continuity Management

14.1 Planning information security continuity

It is important to keep working in an environment when some crisis it an organization. In case of information security crisis, the best practice is to try to apply the basic and standard information security protocols.

14.2 Implementing information security continuity

Once the requirements have been identified, which is discussed in previous section, it is required to layout basic plan to resume the services. The plan should be set in a way that an acceptable information security must be in placed or resumed with.

14.3 Verify, review and evaluate information security continuity

Information security continuity controls which are applicable in a crisis are developed over time and should be updated if the size of organization increases. So, the protocols, which were applicable a couple of years ago, may not be acceptable now. It is required that the information security protocols to be updated every now and then.

15 Compliance

15.1 Identification of applicable legislation and contractual requirements

The contractual requirements may be received from many different sources and should be dealt with accordingly. It is important that an organization should know which requirements it should need to comply to. As the requirements are added or may get updated, it is also required that the requirements compliance overview is up to date.

15.2 Intellectual property rights

Intellectual property (IP) is the most important thing in an organization. This may lead to gain in value, and also may lead to a loss in organizational assets. So, it is required that the intellectual property documents are well maintained, and IP applications are filed at high priority, when required. The other issue, could cause a great loss to the organization is the use of someone else's IP. So that use must be properly documented as it can lead to a lawsuit.

15.3 Protection of records

All the records, either they are related to audit or the accounts must be properly managed. They should be secured as well as there could be loss of data and also may have some unauthorized access. Such information may be required at any time the organization itself or by audit firms, or by the legislation personals.

15.4 Privacy and protection of personally identifiable information

The personal data is the most important in an organization to maintain its authenticity and integrity. To make sure that the organizations do not use the personal data for other

purposes there are different laws applied in different countries and regions. So, an organization must follow the limitations which are imposed by the concerned authorities.

15.5 Regulation of cryptographic controls

The use of cryptographic technology is also depending on the laws and regulations. Organizations understand applicable technologies and implement controls and programmer awareness to ensure compliance with requirements.

15.6 Independent review of information security

It is important for an organization that they maintain a transparency in case of information security. So, it is required that the information security policies are kept up to date. The other thing which needs to be taken care of is the audit of the security policies. The organization must have an audit of their information security policies by an independent firm. This audit should happen on regular basis, or when there is a major change in the organization.

15.7 Technical compliance review

The data system should be updated regularly to comply with security policies and standard. Automatic tools are often used to check systems and networks to be technically compliant and that must be identified and used appropriately. The tools may often run some test to check any vulnerability in the system. The test may also be harmful for the system, so they may be run/executed with great care.