Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 3 Part 2

- Ryustem Shaban (rs223fx)
- Ibrahim Groshar (ig222je)
- Faruk Yildirim (fy222av)
- Henry Shafer (hs223nr)

Information Security Policy

1. Purpose

Main purpose of this policy document is to provide protection for Loco News' information and services by ensuring confidentiality, integrity and availability with enforcement of compliances with Information Systems regulations such as ISO 27002 and the GDPR.

All individuals that are working with Loco News under agreed work contract or any other excessive third-party workers that are in cooperation with Loco News under formal agreement should be informed about the policy and should be practicing it appropriately.

The main objectives of this policy document are as follows:

- To ensure confidentiality, integrity, and availability of all information of the company information systems
- To ensure usage and implementation of appropriate measures to detect and respond to threats quickly without disturbing the work process.
- To ensure organizational assets are secured against cyber attacks
- To ensure that organization have appropriate and accurate policy structure against incidences which can disturb workflow and immediate recovery are being taken after the incident.
- To ensure data protection regulation compliances and information system standards to avoid organizational litigations.
- To ensure that organizational systems will be functional in and after cases of disruption.

Information / Information systems refers to:

- The company's servers (Web, Mail, Database, File, DHCP, DNS, Test)
- The company's intranet
- The company's software and hardware components
- The data belonging to the company
- The data belonging to employees and employers

Sensitive data / Information refers to:

- Personal data which can be used to identify a individuals' real-world identity and details about that specific individuals (name, ID, health, etc.)
- Data pertaining to the company's organizational structure
- Company Intellectual Property

Security incidents are any events that affect the confidentiality, integrity, or availability of any information system by violating this policy, such as:

- Noncompliance with data protection regulations and steps stated in the policy
- Software / Hardware malfunctions
- Unauthorized access

2. The Policy

Policies below should be practiced within all applicable areas of Loco News to ensure proper and effective delivery of services.

1. Information security policies

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Policy:

1.1. Employees in management positions at Loco news have laid out information security responsibilities and are responsible for their part and making sure their underlings take care of their responsibilities.

1.2. If any law changes occur that can affect information security, a meeting must be called within 72hrs with employees in management positions, in order to make any necessary changes to operations.

1.3. Information security policy is to be review with any changes to the business strategy.

1.4. All employees are responsible for information security meaning the protection of any sensitive data.

1.5. In a case where an employee of management position is unable to complete their information security responsibilities, the responsibilities will be handed down to the next subordinate.

1.6. All specified policies in this document are to be followed without exception by every employee.

1.7. Review of the layer out policies are to be review at least quarterly.

2. Organization of information security

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

Policy:

2.1. The CTO is in charge of information security, but every employee will play a roll.

2.2. Assets should be assigned to employees.

2.3. Individuals who use any company asset is in charge of that asset and will take responsibility for it if it is stolen or damaged.

2.4. Every employee should be given an authorization level according to the information necessary for them to do their job, these levels need to then be documented.

2.5. The CTO and other employees who works largely with information security should keep up to date on new potential security threats.

2.6. Employees are responsible for overseeing and checking reliable information sources.

2.7. Employees must have their responsibilities laid out and organized to prevent misuse of any assets.

2.8. Proper authorities should be easily reachable in case of any dispute or wrong doing at the work place.

2.9. Contact with a special interest group should be maintained in order to stay ahead of attackers and make sure the security systems are up to date.

2.10. All projects should keep information security in consideration, before, during, and after creation.

2.11. All mobile devices need to have the following; be registered, be password protected, software installation restrictions, restricted access to information services (access controls, cryptographic techniques, malware protection, remote disabling, erasure or lockout, backups, usage of web services and web apps)

3. Human resource security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Policy:

3.1. Job candidates must provide availability of satisfactory character references, e.g. one business and one personal.

3.2. Job candidates must provide a verified resume.

3.3. Job candidates must provide ID.

3.4. Before employment, background check must be conducted to see about previous criminal records or job losses.

3.5. Job candidates must be trusted, qualified, and competent.

3.6. The contractual agreements with employees and contractors should state their and the organization’s responsibilities for information security.

3.7. All contractual agreements include the signing of an NDA.

3.8. The contractual agreements should also layout, legal responsibilities, information and asset management responsibilities, the handling of information from other parties.

3.9. All employees are too be briefed on their information security responsibilities and provided with guidelines for how to carry out these responsibilities.

3.10. Employees are to have access to an anonymous channel to report information security violations.

3.11. Employees must keep informed on current information security threats.

3.12. There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

3.13. The steps to dealing with employment termination need to be defined.

4. Asset management

Objective: To identify organizational assets and define appropriate protection responsibilities

Policy:

4.1. Assets associated with information and information processing facilities should be identified and inventory of these assets should be drawn up and maintained.

4.2. Assets should have owners who are assigned when the asset is acquired, and they should be aware of their responsibilities pertaining to this asset.

4.3. Every asset needs to be, classified, protected, inventoried, periodically assessed, and properly handled when disposed of or deleted.

4.4. Assets are to have defined acceptable uses.

4.5. Upon employment termination assets are to be returned to Loco.

4.6. Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

4.7. Classification and label assignment should be defined and followed for all information.

4.8. Procedures for handling assets needs to be defined.

4.9. Access restrictions, maintenance, protection, and storage should all be considered for each asset.

4.10. When media is removed it should be made unrecoverable and a record should be kept of its use and removal.

4.11. Sensitive data on removable medias should be encrypted.

4.12. Sensitive data needs to have at least one back-up.

4.13. Media should be disposed of securely when no longer required.

4.14. Media should have defined procedures for deletion.

4.15. Media containing information should be protected against unauthorized access, misuse or corruption during transportation.

5. Access control

Objective: Access limit to information and information processing facilities in Loco News, ensuring authorized user access and preventing unauthorized access to systems and services. Making users accountable for safeguarding their authentication, information and preventing unauthorized access to systems and applications.

Policy:

5.1. Limitation of access to data or services, management of access rights in a networked environment, access control roles, e.g., access requests, access authorization, access administration, requirements for access request, periodic review of access rights, removal of access rights and roles with privileged access. Two principles are directing the access control policy:

Need-to-know: only grant access to the information you need to perform your tasks.

Need-to-use: only grant access to the information processing facilities you need to perform given task.

5.2. Users can only be provided access to the network services that they are authorized to use. Access control roles should be segregated, e.g. user authorization, access limitation and requests. Security requirements of applications and requirements for authorization, review and removal of access rights and roles with privileged access. Access to information and application system functions should be restricted in accordance with the two principles directing the access control policy.

5.3. Authorizing user access and preventing unauthorized access to systems and services. For that work, a formal user access provisioning process should be implemented to assign and deny access rights for all user types to all services and systems.

5.4. Processes managing user IDs: Users held responsible for their actions, disabling and removing users who have left the organization, maintaining a record of access rights granted to a user ID. Reviewing of access rights should be done by asset owners at regular intervals.

5.5. Users should be required to follow the organizations practices in the use of secret authentication information. Keep information from the company in the company, avoiding divulging it to any other party. The objective is to make users accountable for safeguarding their authentication information.

All users should be familiar with the following policies:

- Avoiding keeping secret information on a record (e.g. on a software, paper etc.);
- Changing the authentication information whenever there is a possible compromise;
- Passwords used for secret authentication information should have a sufficient minimum length and is easy to remember, not vulnerable to dictionary attacks, not formed on anything, something that can easily be guessed;
- To not share user's authentication information;
- Not use the same authentication information for non-business and business purposes.

6. Cryptography

Objective: To ensure the proper use of cryptography to protect the confidentiality, authenticity, and integrity of information.

Policy

6.1. Cryptographic keys should be developed and implemented by the following way. It consists of managing cryptographic keys, including generating, retrieving, distributing, destroying, storing and archiving keys. The cryptographic keys should be protected against modification. In addition, secret keys need to be protected against unauthorized use. Equipment used to store and generate the keys should be physically protected.

7. System acquisition, development and maintenance

Objective: To prevent unauthorized access to systems and applications and to control the access of information. Ensuring the information security is designed and implemented withing the development lifecycle of information systems and to ensure the protection of data used for testing.

Policy:

7.8. Information services passing through the public networks should be protected from unauthorized modification and disclosure. Secure development and environment are required to build up a secure service, software, and system. That is done to ensure that information security is designed and implemented within the development lifecycle of the information systems.

7.9. The test data should be protected, controlled, and selected carefully. The use of any personally identifiable information or any confidential information for testing purposes is forbidden, all sensitive data should be protected by removal or modification. When testing, there also should be separate authorization each time information is used to a test environment. All information used in a test environment should immediately be deleted after testing is complete.

8. Physical security

Objective: To ensure implementation of appropriate access control to protect Loco News' physical and technical assets and prevent unauthorized physical access, damage to equipment and inference to the Loco News' information and facilities processing.

Policy

8.1. Perimeters that contain information processing facilities' strength should be dependent from the risk assessments and facilities should be secured from break-ins and entrances should be extra secured. For emergency exists within the facility physical access control methods should be considered. Facilities processing information should be separated physically and for all facilities intruder detection system should be implemented

8.2. Entry controls for secure areas should be considered to ensure that access is made only by authorized individuals. Entry controls should be aiming to record entry and departures of each visitor and not leaving visitors unattended. Records should be kept with audit trail. Additionally, all employees should be carrying visible identification. Access rights for these individuals should be kept up to date.

8.3. Key facilities restricted from public access and to be prevented from being visible and audible from outside. Physical protection against malicious attacks, natural disasters or accidents should be designed and applied for all areas. Secure areas should be known by individuals by need-to-know basis and recording equipment within these areas should be restricted and locked.

8.4. Equipment within the facility should be cited, secured and for this equipment correct functionality should be ensured. These containing sensitive information should be safeguarded with additional attention. Malfunctions, power failures and other disruptions caused by failures which are limiting proper workflow should be avoided by checking power and telecommunications cables for proper functionality and segregating these cables.

8.5. All equipment's proper functionality should be ensured by maintaining the equipment by following the supplier's recommendations and processing the maintenance only by
authorized personnel. If maintenance scheduled to be done outside the facility special rules regarding protection of the sensitive information on the equipment should be on point.

8.6. Special rules should apply if off-site maintenance should be done between the external organization and Loco News. If sensitive information within the equipment was not appropriate to be cleared and identities managing the maintenance should be documented.
Off-site work protection should also be ensured by not leaving the equipment unattended and keeping record of information traffic and identities of the individuals.

8.7. Sensitive data should be securely deleted from assets, and encryption with complex keys should be applied to prevent it from being recovered or destroyed.

Media with sensitive or secret content should be deleted immediately from reproductive technologies such as printers, scanner, and digital cameras.

9. Operations security

Objective: To ensure that information, information processing facilities, software and hardware are protected against malware and in case of malicious actions all necessary information for proper functionality of the organization is copied accurately together with the records of all events.

Policy

9.1. Operating procedures should be accessible for all employees within Loco News and should be clearly covering everything about installation of systems and configuration processes. Handling, error handling and backup process instructions should be clearly stated. Additionally third-party and external support contacts in case of technical difficulties which cannot be handled by the employees

9.2. All changes that are being made within the company should be controlled and restricted only to authorized personnel appropriately. These changes should be documented and appropriately tested before proposing changes. Test environments should not have access to any development tools used in the workspace if not required. Users should use different accounts, and any confidential info should be kept away from the test environments when not required. Additional risk and hazard analysis should be considered following the security requirements and all employees should be informed regarding changes where appropriate.
In case of system failure, the system should have ability to be returned to an earlier state.

9.3. Resource usage should be monitored, and efficient working of all systems should be ensured. Assets with higher monetary cost should be safeguarded with additional protection. Capacity management should be considered. Optimization of system logic and restricting hungry services should also be considered for better system performance. Proper capacity management control should look like the following:

- Deleting unused(dark) data
- Application logic optimization
- High-consumption services should be avoided if not critical

9.4. To control the risk of information breaches, in process of development and testing segregation should be considered with clearly stated terms and conditions regarding software transfer from work to test environment. All testing tools should be restricted from the operational system.

9.5. Should be ensured that information and information processing facilities are protected against malware by implementing controls to restrict usage of unauthorized software. Additionally, terms that are clearly stating how to obtain information from external networks securely should be on point. Regular checks of critical for the organization software should be made and in case of breach data continuity plan should be available.

9.6. Controls such as black and whitelisting should be considered for detection and\or prevention usage of unauthorized software. For all software malware detection tools from authorized service providers should be considered to ensure proper security levels within the working environment. All anti-malware tool should be regularly checked and kept up to date. Additional control measures should be considered for information collection from the network. In case of vulnerability identification, the organization should define responsibilities and perform a hazard analysis. If patch is available from a legitimate source risk analysis should be made, otherwise patches should be remade, or other temporary controls should be applied. Systems at high risk should be prioritized and addressed first.

9.7. Copies of all critical data that was backed up should be checked and kept up to date in regular basis and kept away from site. Additionally audit logs should be used and all clocks should be synchronized to provide accurate time for all recordings.

10. Communications security

Objective: Information exchange controls within network should be designed to ensure confidentiality, integrity, and availability of the stored information.

Policy

10.1. Control measures should be on point to ensure prevention of unauthorized network, access to the network, wireless network and connected system applications. Should be additionally practiced monitoring the network to secure it from flaws.

10.2. All connection to the network that are being made by the system should be restricted and only connection to authorized networks should be allowed for the individuals within the facility.

10.3. Responsibilities for networks and computer operations should be separated.

10.4. Features for security should be considered, these features should be as following:

- Encryption
- Authentication
- Connection controls
- Restriction of access to the network services or applications

10.5. For large networks segregation should be considered with dividing it into separate network domains. Chosen domains should be filtered and based regarding their trust levels. Access between these networks should be done using gateways.

10.6. Terms and controls regarding protection of transferred and information should be implemented by the organizations. These terms should be covering the compromise of the organizational sensitive information and attachments. Additionally, terms regarding proper usage of email should be implemented as well by the organization. Cryptographic encryptions should be used to protect all organizational sensitive information. Transfer of confidential information over insecure network should be restricted. With agreements should be ensured that transfers are traceable and non-repudiational.

10.7. Confidentiality of the electronic messages should be ensured and their transfer to the correct address should be verify. Additionally, should be considered implementation of watermarks or signatures to ensure integrity. Organization should have terms for the information when the agreement period is over and additionally in case of agreement breaches.

11. System acquisition, development, and maintenance

Objective: To prevent unauthorized access to systems and applications and to control the access of information. Ensuring the information security is designed and implemented withing the development lifecycle of information systems. And to ensure the protection of data used for testing.

Policy

11.1. Information services passing through the public networks should be protected from unauthorized modification and disclosure. Secure development and environment are required to build up a secure service, software, and system. That is done to ensure that information security is designed and implemented within the development lifecycle of the information systems.

11.2. The test data should be protected, controlled, and selected carefully. The use of any personally identifiable information or any confidential information for testing purposes is forbidden, all sensitive data should be protected by removal or modification. When testing, there also should be separate authorization each time information is used to a test environment. All information used in a test environment should immediately be deleted after testing is complete.

12. Information security incident management

Objective: To ensure the effective way to the management of information security incidents, as well as communication on security events and weaknesses.

Policies

Following policies should be applied within the Loco News facility to ensure the incident management is applied effectively.

12.1. The management is responsible for appointing the roles and responsibilities that are well defined and established for incident management. The procedures of incident response, planning, preparation, incident monitoring, detecting, analyzing, reporting, recording incident management activities, evidence handling, and the response for incident management should be established.

12.2. The responsible personnel should handle the information security issues within the organization also maintain contact with the external groups and authorities that handle the issues related to information security and a contact point for security incidents should be implemented.

12.3. The reporting should include all necessary actions and all details should be noted directly include referencing the employees who commit security breaches and suitable feedback should be ensured.

12.4. All employees are responsible for reporting the information security events and weaknesses to point of contact as soon as possible, the report situations to be considered as; ineffective security control, any breach in CIA(confidentially etc.) expectations, human errors, physical breaches, violation of access, uncontrolled system change and malfunctions of software and hardware.

12.5. The point of contact is responsible for the assessment of each information security event and classification and prioritization of incidents should be done by point of contact.

12.6. Response for the information security events should be done with documented procedures. The response should be done by the nominated point of contact and other parties that are relevant to organization.

12.7. The response should include quick evidence gathering, information security forensics analysis, in required case escalation, effective communication with external and internal relevant people, and recording the incident.

12.8. The evidence gathering process should be developed and the collection of evidence should provide processes of identification, collection acquisition, and preservation of evidence.

13. Information security aspects of business continuity management

Objective:

The continuity of the information security and the organization’s business continuity management systems should be embedded, and availability of information processing facilities should be ensured.

Policy:

13.1. The continuity of the information security should be determined with continuity of the organization's business, the information security requirements are required to be classified in disaster recovery planning.

13.2. The continuity of information security should be established, documented, and implemented by the organization.

13.3. The adequate management structure should be established to an effective response to the disaster.

13.4. The responsible personnel should be nominated for the incident management.

13.5. The disaster management for the disaster which includes plans, response, and recovery procedures should be developed and approved with detailed management.

13.6 The organization should review, test, and validate the embedded information security continuity plan, in case of update and change organization should make required changes.

13.7. The implementation of information processing facilities should be redundancy sufficient to match availability requirements and business requirements for the availability of information systems should be identified, in case of availability cannot be guaranteed; current systems should be considered.

14. Compliance

Objective: To avoid breaches of information security from legal, statutory, regulatory, or contractual obligations and ensure that information security is implemented with the organizational policies and procedures.

Policy:

14.1. All relevant legislative statutory, regulatory, contractual requirements, specific controls, and individual responsibilities should be defined, documented, and kept to up to date and this process should be applied to each information system in the organization.

14.2. Managers are responsible for the identification and implementation of all legislations to their organizations to meet the requirements for their type of business if the organization leads the business in another country, managers are responsible for considering compliance in all relevant countries.

14.3.The organization should make sure that appropriate procedures are implemented to meet contractual legislative, regulatory, and contractual requirements related to intellectual property rights.

14.4.The policy that covers compliance intellectual property rights should be published and awareness of policy should be maintained.

14.5 The process of acquiring software should be through known channels and the organization should maintain the appropriate asset registers and identify all the assets, proof, and evidence for ownership of license, master disks, manuals etc.

14.6 Acquired software should be applied and used without violating copyrights or other legal, statutory, regulatory, or contractual obligations.

14.7 The organizational records should be classified, categorized, and stored safely. During storing process, type, condition, and required protection of records should be considered to prevent any possible record loss.

14.8 The privacy and protection of personally identifiable information should be developed, the development of privacy should be developed with the responsible institution or person such as the privacy officer. The policy should meet the legal requirements of privacy and protection of personally identifiable information.

14.9 The restriction of all cryptographic controls such as import or export hardware or software for performing cryptographic functions, usage of encryption, or mandatory or discretionary methods of access by the countries' authorities for the encrypted information should be considered.

14.10. The management is responsible to ensure the independent review of information security and the results of the review should be recorded and reported in case of weakness or fail the management should take corrective actions.

14.11. Managers should review the compliance of information processing procedures if non-compliance is found as a result; the manager should identify the causes, evaluate the need for the actions, implement the corrective actions and review the actions.

14.12. Technical compliance review of the information system should be regularly done, and the review should be with the assistance of automated tools which can generate technical reports. The reviews should be done by an experienced system engineer.