Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 4
Loco News INFOSEC Policy

Group Members: <Fabian Dacic>, <Yuyao Duan>, <Fredric Eriksson>, <Fang Fang>

Table of Contents

1. Introduction

This policy applies to all users (employees, subcontractors and suppliers) at “Loco News”. All users are required to comply with the terms of this policy as well all applicable laws and legislation.

1.1 Purpose

This policy provides management direction and support for information technology security in accordance with “Loco News” operational requirements. This policy is in-line with the ISO standard ISO/IEC 27002:2013, Information technology - Security techniques - Code of Practice for Information Security Controls.

This policy defines the framework by which information security will be managed and supported at Loco News. Information security is supported by procedures, processes, organization and software and hardware functions.

1.2 General principles

“Loco News” should comply with ISO 27002 to ensure that all IT-systems are secure, and users handle the information in a secure way.

CTO should ensure that information security is a part of “Loco News” current and future information systems and applications, including both software and hardware, over the entire lifecycle. CTO is also responsible to inform all users about this policy and secure that users act in accordance with this policy.

All users are responsible for compliance with this policy and for managing information in a secure manner:

- All users must comply with relevant legal and regulatory requirements.
- All users assist with the protection of “Loco News” data and information, to prevent unauthorized person's access.
- All users should adopt a risk-based approach to information security, to ensure that all information related risks are managed in a consistent and effective manner.
- All users should apply approved information security processes, solutions and services, where possible, to avoid creation of disparate IT security controls.

2. Organization of information security

In order for a policy regarding organization of information security being developed and implemented for the organization “Loco News”, this document complies and adheres to the standards by the ISO 27000 family of certifications. The objective is to ensure security of internal organization as well as security of mobile devices and teleworking.

2.1 Policy on internal organization

The main objectives of security of internal organization include initiating and controlling the implementation and operation of information security within the organization.

2.1.1 Information security roles and duties

1) The responsibilities for all the individual assets for carrying out information security processes of “Loco News” should be identified.
2) All the major information assets should be accounted for and assigned to the owner.
3) In order to achieve security of information assets, all personnel should be assigned corresponding authorization levels and comply with the principle of minimizing authorization.
4) “Loco News” should assign and nominate personnel to coordinate and oversight with suppliers of information security.

2.1.2 Separation of duties

1) Conflict duties and responsibilities of “Loco News” should be identified and minimized.
2) No single person of “Loco News” or stakeholders of “Loco News” is allowed to access, modify or use assets without authorization or detection.
3) No single person of top management of “Loco News” is allowed to have full authorization without personnel supervision of corresponding level.

2.1.3 Contact with authorities and special interest groups

1) All inner staff and stakeholders of “Loco News” should report to the CTO in a timely manner when information security incidents are identified.
2) CTO has authority to decide internal processing or contact relevant authorities depending on the situation, at the same time reporting to the top management and CEO.
3) CTO is responsible for oversighting and making information security incident management processes to response attacks and maintain business continuity.
4) CTO is responsible for assigning and monitoring personnel to maintain contacts including but not limited to fire departments, telecommunication providers, electricity suppliers, and water suppliers etc.
5) CTO is responsible for supervision and management of maintaining contact with special interest groups with respect to knowledge sharing and continuing education of information security.

2.2 Policy on mobile devices and teleworking

The main objective of this policy is to secure using mobile devices and teleworking.

2.2.1 Using mobile devices

1) All mobile devices in "Loco News" office environments should be strictly supervision and be classified as private devices and business use of devices which have separated internet access.
2) All mobile devices in "Loco News" office environment are required to be registered and supervised.
3) All required software needs to be preinstalled and all personnel do not have permission to install extra software on the mobile devices.
4) All mobile devices of "Loco News" should have physical protections that include but not limit to positioning, biometrics, remote lock etc.
5) All mobile devices of "Loco New" must be preinstalled enterprise VPN to access web apps and services.
6) All mobile devices of "Loco News" must be installed with enterprise anti-malware software.

2.2.2 Using teleworking

1) CTO is responsible for making detailed regulations under what circumstances using teleworking.
2) All employees' private devices do not have access to web apps and databases of "Loco News" and do not have access to store information and data.
3) All teleworking infrastructure and devices must be installed with malware protection and firewall.
4) All voice and video call should be conducted with enterprise-level encrypted communication software.
5) All business mobile devices should be able to detect local network environments and to confirm if the network configuration fulfils the requirements.

3. Human resource security

In order for a policy regarding human resource security being developed and implemented for the organization "Loco News", this document complies and adheres to the standards by the ISO 27000 family of certifications. The objective of this policy is to support "Loco News" identifying suitable employees and contractors simultaneously clarifying their responsibilities, aiming to build up a safe and stable human resource system.

3.1 Policy on prior to employment

The main objective of this policy is to support "Loco News" to identify appropriate human resources.

1) All applicants' curriculum vitae should be verified which includes but not limit to academic qualifications, professional qualifications, independent identity, credit review, and criminal records etc.
2) "Loco News" should assess applicants' personality prior to employment.
3) The applicants for specific information security role should be tested and proved with necessary competence to perform the security role.
4) All employees and contractors of "Loco News" should sign confidentiality before gaining access to information facilities.
5) "Loco News" should clarify the legal responsibilities and rights of applicants before the work starts.

3.2 Policy on during employment

The main objective of this policy is to ensure all personnel of "Loco News" fulfil the corresponded security responsibilities.

1) CTO is responsible for establishing archives of descriptions of roles and responsibilities of related information security roles.
2) CTO is responsible for establishing detailed regulations and incentive system to motivate personnel to achieve security awareness and execute security regulations.
3) Management team are responsible for initiating and maintaining periodic education which includes and but not limits to skill education, qualification education, security education etc.
4) An appropriate and complete disciplinary process should be established to cover both employees and contractors.
5) CTO and management team should establish a comprehensive procedure to identify a breach:
    a) Unintentional or intentional
    b) First offence or repeat offence
    c) Whether or not the violator properly trained
6) When deliberate breaches happen, the management team should immediately take actions.

3.3 Policy on termination and change of employment

The main objective of this policy is to protect the interests of "Loco News" when changing or termination of employment happens.

1) CTO and management are responsible for identifying focal information security responsibilities and duties that remain valid after termination or change of employment happens.
2) CTO and management should assess and define valid periods of related responsibilities and duties after termination or change of employment.
3) The above terms and regulations must be contained in the employment contract.

4. Asset management

In order for a policy regarding asset management being developed and implemented for the organization “Loco News”, this document complies and adheres to the standards by the ISO 27000 family of certifications. The objective of this policy is to support “Loco News” identifying organizational assets, information and establishing related protection responsibilities.

4.1 Policy on responsibility distribution

The main objective of this policy is to define appropriate protection duties of the related organizational assets of “Loco News”.

1) All the assets related to information and information processing facilities should be identified and the life cycle of each asset should be documented by the management of “Loco News”. Inventory of these assets should be maintained.
2) All the assets of “Loco News” should be assigned with ownership.
3) Owners of the assets are responsible for asset protection and management over the whole asset lifecycle.
4) All shared assets of “Loco News” should be properly protected and managed by corresponding procedures to ensure that the related responsibilities are accurately assigned.
5) When termination of employment happens, the relevant employees, contractors, or external party users should return all related organizational assets.
6) The management of “Loco News” should carefully check the returned assets and identify if potential damage exists. The previous asset owner is responsible for compensation.

4.2 Policy on information classification

The main objective of this policy is to ensure all information of “Loco News” receiving appropriate classification and protection.

1) CTO and management team of “Loco News” should establish comprehensive information classification scheme which can be used to identify the protection level of different information.
2) The classification scheme should include detailed measures and criteria which can be reviewed and assessed periodically.
3) The established classification scheme should be consistent across whole organization and personnel can have common understanding on it.
4) Information classification scheme should be supported with practical information labelling procedures to:
    a) Accurately reflect classification scheme
    b) Accurately reflect the format of the information
    c) How labels are attached

d) The procedures of assessment

5) CTO and management team of "Loco News" should establish practical procedures for:

a) Handling

b) Processing

c) Storing

d) Communicating

4.3 Policy on media handling

The main objective of this policy is to strengthen information protection by preventing unauthorized information operations.

1) CTO and management team of "Loco News" should establish comprehensive information handling procedures for:

a) Destruction of re-usable media

b) Recording of removable media when it is moved

c) Removable media should apply cryptographic techniques

d) Using removable media to transfer data should be monitored

2) CTO and management team of "Loco News" should establish detailed and practical procedures for secure disposal of media.

3) Physical media containing organizational information should be properly protected during transportation in order to against:

a) Unauthorized access

b) Misuse

c) Corruption

5. Access Control

In order for a policy regarding access control being developed and implemented for the organization "Loco News", this document complies and adheres to the standards by the ISO 27000 family of certifications. The objective of this policy is to support "Loco News" to establish access control security.

5.1 Policy on business requirement

The main objective of this policy is to ensure focal organization to limit access to information and information processing facilities.

1) Top management of "Loco News" is responsible for establishing access classification which is based on:
    a) User roles
    b) Access rights
    c) Facilities
2) The access control scheme should consider both logical design and physical design.
3) In reference and accordance to ISO 27002 subsection 9.1.1, the access control scheme should minimize user role's facility access and avoid roles with privilege access.
4) The access control scheme should minimize the user role's information access to perform job tasks.
5) Only authorized user can access the network services of "Loco News".
6) All personnel of "Loco News" need to be assigned roles to be able to access network services and information facilities.
7) All information facilities of "Loco News" must equip VPN to access network services.
8) The network services of "Loco News" should differ and provide separated internet access to private and business devices respectively.
9) The network system of "Loco News" should be able to monitor user's access to information systems and establish a comprehensive log.

5.2 Policy on user access management

The main objective of this policy is to ensure that only authorized user is able to access systems and services of "Loco News".

1) All users of "Loco News" should be assigned with unique user ID to achieve user behaviour accountability.
2) CTO and management team is responsible for access rights distribution, access distribution need to restrict privileged access rights.
3) All user IDs should be reviewed periodically in order to change, update, or revoke access rights.

5.3 Policy on user responsibilities

The main objective of this policy is to build up users' security awareness of their authentication information.

1) "Loco News" should arrange security education to build up employees' responsibilities of safeguarding personal secret authentication.
2) All users should avoid keeping a record of secret authentication information.
3) When authentication information is under risk of compromise, the user is responsible for changing authentication information.

5.4 Policy on system and application access control

The main objective of this policy is to prevent unauthorized access to information systems and relevant facilities.

1) CTO is responsible for establishing information access restrictions to control and limit:
    a) Data accessed by a particular user
    b) The rights of users reading, writing, deleting, and executing
    c) Access to sensitive applications and data
2) CTO and management team are responsible for designing and establishing a secure log-on procedure.
3) It is not allowed to provide help message during log-on procedures.
4) The system will not provide prompts until whole log-on process is completed.
5) The system will not certify logon information until input all demanded data.
6) The system should provide limited time for logon procedure.
7) All successful logon sessions should be terminated based on a predefined period of inactivity.
8) Password standards should meet following requirement in order to achieve logical security:
    a) A password is required to have minimum length of eight characters and enforce to have capital letter and special characters
    b) Passwords are not allowed to be based on dates (year, month, week etc.), names (family names, first names, company names), telephone numbers, car registration numbers, words contained in a dictionary or from foreign languages
    c) The temporary passwords are forced to be changed when user first time logon the system
    d) Password will not be displayed when user entering
    e) Password is forced to be changed every 60 days

6. Cryptography

In order for a policy regarding cryptography being developed and implemented for the organization "Loco News", the objective is to ensure usage of cryptography to protect the confidentiality, integrity, authenticity of the information within the organization.

6.1 Policy on cryptographic controls

The main security objectives of cryptographic controls are: confidentiality, integrity/authenticity, non-repudiation and authentication.

1) In compliance to general data protection regulation (GDPR), the storage containing sensitive data including assorted information which might be confidential of the organization named "Loco News" is to be encrypted for safeguarding.
2) An approved and risk-assessed based encryption algorithm is to be implemented with consideration that there is the possibility of devices being used outside the facility of the organization "Loco News". In other words, an encryption method for data in motion along with a secure channel regarding such operations have to be considered during the development and implementation of an encryption algorithm.
    a) Users have to be notified if encryption is being used over the network in which the user is in.
    b) Encryption is required and has to be designed for operations such as: transfer of sensitive data inclusive or assorted information, remote network traffic regardless of environment and privileged network access etc.
3) An approved and risk-assessed key management method is to be developed and implemented which is compatible with the aforementioned encryption algorithm and the organization "Loco News" with its goals. Along with the key management, key generation and the policy itself, the organization has to assign roles and responsibilities to certain employees regarding respective points aforementioned.
4) The base operations of the organization "Loco News" and considering the nature of the business which is a news station, a management plan and modification of data inclusive or assorted information of the organization are of utmost importance.
5) Along with the security measures for data inclusive or assorted information, ranging from user-password to biometric measures such as a fingerprint reader that will be developed and implemented throughout the organization "Loco News", other content inspection such as malware detection and monitoring need to be considered.

The implementation of this policy should be following all juridical perimeters, regulations and laws of the establishment in which the organization "Loco News" is to be found and that adopting the policy in case of changes might be necessary and have to be kept in consideration.

6.2 Policy on key management

In compliance to GDPR, encryption that will entail data inclusive or assorted information, key management is to be conducted within the organization “Loco News”.

1) The system which will be developed and implemented for the organization will include aspects such as: generation, issuing and obtaining the key certificates, distribution, storage, modifications, contingency plans and monitoring of the usage of keys within and without the perimeters of the establishment.

2) The key management system should be in tandem and accordance with the system that is to be implemented for the organization. Regarding the authenticity of the keys, certifications issued by a certification authority that provide a certain degree of trust should be consulted.

7. Physical and environmental security

In order for a policy regarding physical and environmental security being developed and implemented for the organization "Loco News", the objective of the policy is to establish preventative measures against unauthorized physical access, damage and interference to the organization's data and assorted information and the facilities surrounding such manners.

7.1 Policy on physical security parameter

In compliance to the physical security professional (PSP) certification establishing a physical security parameter based on a risk-assessment of the threats that the organization could face is mandatory. That could include countermeasures such as:

i) Barrier fencing
ii) Digital locks
iii) Protective barriers
iv) Adequate lightning
v) Security guards
vi) Surveillance cameras
vii) Sensors
viii) Fire retardants
ix) Assess control

7.2 Policy on physical entry controls

The organization "Loco News" is to secure its facilities with appropriate entry controls in which only authorized personnel are allowed to roam the premises and access.

1) The entities responsible are to log and record every entry and departure of visitors into the facilities of the organization.
2) Employees of the organization, visitors and affiliates are required to bear a form of identification that will allow them access to the premises throughout the facilities of the organization based on their access grants.
3) Access rights are to be reviewed and updated as the organization might see fit.

7.3 Policy on securing offices, rooms and facilities

The organization "Loco News" is to establish a secure perimeter and emphasize the instruction that public access is denied to the key facilities of the organization.

1) Information and processing facilities regarding the information should be shielded and not be readily accessible for the public.
2) Security measures should include however are not limited to: electromagnetic shielding, reinforced walls, and monitored premises at all times.

7.4 Policy on protecting against external and environmental threats

The organization “Loco News” is to enforce their facilities and establish a secure perimeter in case of environmental threats such as earthquakes, flood, fire and other external threats such as civil unrest. These are a few of the threats that are to be considered.

1) Regarding these threats, reinforced structure which includes bases of the buildings, every floor, room of the facilities and walls are to be reviewed in order for a plan of upgrading them to be developed and implemented.
2) Fire retardants, emergency escape routes and routines, first-aid kits and accessories are necessary for the organization to be compliant to the ISO standards and other safety certificates.

7.5 Policy on working in secure areas

The organization “Loco News” is to inform its employers, employees, affiliates, contractors, third parties about the existence, operations and activities within the sound areas.

1) Local procedures that are to be established by the organization throughout the development and implementation of the policy need to ensure training and protocols regarding safety in the facilities.
2) Vacant secure areas of the facilities of the organization are to be periodically reviewed and monitored by a security staff that the responsible team will assign them to various stations. Visitors of the facilities that the organization operates are to be accompanied throughout and informed of their access rights and restricted areas.

7.6 Policy on delivery and loading areas

The organization “Loco News” is to set up, monitor, maintain and review areas in which deliveries and loading will be conducted for the organization.

1) Man-trap design is necessary for these areas due to the fact that materials that can be fragile or confidential that will be either extracted or placed onto various forms of transportation.
2) Any material should be registered and logged in compliance with the assessment procedure aforementioned earlier.
3) All materials should be segregated from each other in separate rooms or facilities of the organization if possible to adhere to the ISO standards.

7.7 Policy on equipment

In compliance to the physical and environment professional certifications, the main goal of the policies regarding equipment is to prevent acts of dishonesty, theft, misconduct, compromise of the data inclusive or assets such as assorted information and all operations related to said elements of the organization “Loco News”.

7.7.1 Equipment siting and protection

The equipment used within the facilities of the organization "Loco News" has to be located and set up in a way that the implementation adheres the certifications and standards. The goal is to ensure that there is a low risk to none regarding equipment in case of hazards of any kind.

1) Equipment should not be placed in locations in which there might be an incitement of a hazard of any kind.
2) In case of equipment that requires special attention and usage, the equipment and the vacant area should be safeguarded.
3) Through risk assessment and controls, the level of risk should be lowered to a minimum considering the physical and environmental threats regarding the equipment.
4) Guidelines regarding basic human activities such as eating, drinking, and smoking in the proximity of information processing facilities of the organization "Loco News" need to be established and in accordance with the regulations and laws such as the Work Environment Act, of the geolocation of establishment, Sweden, due to the fact they have to be in tandem with the policy.
    a) For eating, all employees are required to have a rest and a designated area in which they are to eat. It is common courtesy for work environments to not allow foods, such as nuts, that may trigger allergies hence why it is important to conduct a survey and gather information regarding such matters.
    b) For drinking, all employees are required to not consume alcoholic beverages or any other beverage which may trigger allergies to others in the designated areas around the facilities of the organization
    c) For smoking, employees that smoke are required to be in a designated area for smoking with cans specifically made to intercept any hazard which may derive from tobacco substances therefore the organization and the bodies responsible can consider an outdoor cigarette receptacle.
5) Throughout the development and implementation of this policy, security certifications along with regulations have to also be met depending on the geolocation of the establishment.

7.7.2 Supporting utilities

The supporting utilities that can be found in the facilities of the organization "Loco News", have to be protective of the equipment regarding any disruptions or threats that the equipment might face.

1) According to the specifications and the requirements of the organization, the manufacturer of the uninterrupted power supply (UPS) that the organization utilizes needs conformity.
2) The supporting utilities that will be used throughout the facility, which can be against either physical or environmental threat need to be periodically reviewed, maintained, updated, alarmed in case of being disrupted and monitored. Emergency supporting utilities may include however not limited to:
    i. Fire retardant utilities

ii. First-aid kits

iii. Emergency valves

iv. Emergency switches

v. Emergency lightning

3) Equipment needs to be located near emergency exits and rooms.

7.7.3 Cabling security

All cables related to transportation of the data throughout the facilities of the organization "Loco News" and the critical systems of the organization are to be safeguarded and reinforced structurally for maximum safety.

7.7.4 Equipment maintenance

All equipment within and without the premises of the facilities of organization "Loco News" are to be maintained periodically.

1) In case of maintenance, it should be done no other than the appropriate personnel that the bodies responsible assign the duty to and the process should be affirmative and in accordance with the supplier.

2) Records regarding the state of the equipment have to be kept at all times and reviewed for errors.

3) Insurance policies should be in synthesis with this policy regarding maintenance requirements.

7.7.5 Removal assets

All assets which includes: equipment, data or assorted information within and without the facilities of the organization "Loco News" in case of removal, should be notified to the appropriate section and done so with authorization from the organization's personnel.

7.7.6 Security of equipment and assets off-premises

All equipment and assets should be risk-assessed in case of working outside the organization's premises.

1) Equipment and media should not be left unattended and in case of an intrusion, said elements are to engage in a safety-lock mechanism. That can be locking the device temporarily until personnel with authorization arrives.

2) For certain delicate equipment, manufacturers' instructions regarding the safety of their product should be followed.

3) When working on off-premises of the organization clear-desk policy should be in power immediately, other security measures such as secure cabinet files, safety mechanisms implemented to the organization's devices should be developed and implemented.

4) It is of essence to inform the employees of the risks that may follow. That includes eavesdropping, cyberattacks, possible breaches of the information privacy law physical and so forth. Along with informing, solution suggestions to said risks are advised:
    a) Encryption
    b) Network logging and segregation
    c) Authentication and authorization
    d) Firewalls
    e) Antimalware software
5) Logging is a must.

7.7.7 Secure disposal and reuse of equipment

All equipment in case of disposal or reuse are to be reviewed by the personnel responsible of the organization "Loco News" so that data inclusive or assorted information is backed up and not accessible to unauthorized individuals or even the public.

1) Equipment is to be encrypted with such methods that the equipment can withstand attacks such as brute force ones.
2) For that encryption keys have to be long and themselves kept confidential within and without the organization.

Therefore techniques, methods and algorithms are to be developed and implemented to the equipment aforementioned.

7.7.8 Unattended user equipment

All equipment that is under the property of the organization "Loco News" is to be safeguarded by safety mechanisms is left unattended and there is a possibility of intrusion.

1) Logging off whenever the session of work is over.
2) General logging of the devices to monitor loggings of the devices is necessary to detect any anomalies.
3) Safety mechanisms such as logging off the device until appropriate personnel authorizes with a form of identification such as a username and password should be in place.

7.7.9 Clear desk and clean screen

Any data or assorted information that is left unattended is to be handled in accordance with the clear desk and clean screen policy.

1) Sensitive or critical business information both on paper and digital media should be either encrypted or locked away for safety reasons.
2) Computers and other electronic devices that are vital for the organization's operations should be equipped with safety mechanisms such as logging off automatically when left unattended by the personnel of the organization.

3) Printers and their products which can be media containing sensitive information are to be handled in such a way that unauthorized individuals or the public may not have access to them.

    a) Printers of the organization should require authentication and be monitored for activities periodically.

    b) Printers of the organization should be equipped with safety mechanisms such as a pin lock to deter unauthorized access.

8. Operations security

The main objective of this sector is to provide security and corrections regarding the operations that will be carried out throughout the facilities of the organization “Loco News”.

8.1 Policy on documented operating procedures

When developing operating procedures, it is important that in compliance to standard operating procedures that the procedures regarding any section or task that will be conducted within and without the facilities of the organization.

1) Complex tasks are required to have manuals, standard operating procedure, and contingency plans in case of an emergency.
    a) Processing and documenting data and assorted information of the organization need to be both automated through a system and manual meaning done by authorized personnel of the organization.
    b) Installation, maintenance, upgrade, configuration of the organization’s systems and software require manuals for personnel of the organization.
    c) In case of failures, there should be a procedure which has restored the system’s functionality back to normal otherwise if that is unachievable, a procedure for backing up the system is to be conducted by personnel of the organization.

8.1.1 Change and capacity management

Controls require addressing, approval, reviewing, identification, recording, planning, testing, and verification from the authorized and appropriate personnel of the organization “Loco News”.

1) In case that the inquiries are indeed approved, the entities responsible are to ensure satisfactory control of all changes in all sectors of the organization. Inadequate changes may affect system effectiveness and safety.
2) Regarding capacity management, capacity requirements should be considered before developing and implementing the system to ensure optimal system performance.
    a) Different measures such as monitoring the health of the capacity storage so that issues are identified as soon as possible.
    b) Attention needs to be paid to any resources that might lead to times and high costs.
    c) Managers are required to be able to handle any inquiries regarding capacity without the need of other personnel to avoid intrusion.
3) A documented capacity management which also addresses the capacity of the human resources, offices and facilities of the organization should be considered mission critical.

8.1.2 Separation of development, testing and operational environments

The organization “Loco News” is to separate development, testing and operational environments to reduce risks of intrusion and misconduct within and without the facilities of the organization.

1) Rules and notifications whenever a project pass from development to testing and final product should be well established among the facility in order to minimize miscommunication between the sectors of the organization.
2) Equipment and environments should differ between operational and development projects.
3) Any major changes should be conducted in the testing phase of the projects. The development utilities should not be included in the operational project unless required and deemed necessary by the appropriate bodies responsible and managers of the project. In regards to that, different user profiles should be used in the development project compared to the operational one, and no sensitive data is to be copied into the testing project. Notifications regarding any changes, errors, and successes are necessary for information.

8.2 Policy on protection from malware

The organization "Loco News" is to ensure that data and assorted information along with any related facilities are protected against malware.

1) Establishing controls that disallow activities such as accessing untrusted websites or uncertified applications on operating systems, quarantining the malware and tracing its origin are certain of the many controls that will aid the organization in protecting its assets against malwares.
2) Defining formalities, procedures, and responsibilities regarding protection against malware to the organization and its affiliate members is of importance. After defining aforementioned elements, the bodies responsible for the organization are to conduct regular reviews of the assets of the organization that might be vulnerable to malware attacks.
    a) Periodically regular reviews may include however is not limited to vulnerability and risk-assessment of the asset of the organization regarding different malware attacks such as:
        i. Computer viruses
        ii. Trojan horses
        iii. Worms
        iv. Ransomware
        v. Adware
        vi. Scareware
    b) All files that are received via networks are to be scanned for malware including webpages, attachments and downloads.
3) In case of an intrusion which leads to the data and assorted information being open for compromise or is compromised, an isolated environment is to be prepared in advance throughout the development and implementation of the project of the organization.

8.3 Policy on backup

The organization “Loco News” is to establish mechanisms and procedures that will protect loss of data and assorted information of the organization.

1) Means of backup are to be implemented throughout the organization’s system that allow protection against loss of data and mitigate such cases.
    a) Said means are to be established in a remote location for maximum protection and the backups themselves should be accurate and identical to the original ones.
    b) Considering that the organization is keen on confidentiality, backups should also be encrypted for further added protection against threats.
2) The retention period should also be reviewed and be in accordance with the organization.
3) A policy regarding backups needs to be established in order to determine what data can be received from the equipment of the organization and an isolated environment in case of intrusion is of importance.

8.4 Policy on logging and monitoring

Events must be recorded in order to generate evidence for the organization “Loco News”. Events recorded must be compliant with the general data protection regulations.

1) Network access, system activities, utilities, privileges, attempts and records of transactions between applications are recorded within and without premises of the organization for the purpose of generating evidence.

8.5 Policy on control of the operational software

The organization “Loco News” is to emphasize a strict policy regarding all operational software about integrity.

1) Software usage and restrictions are to be of importance and emphasized among the organization.
    a) Old software is not to be used and should be archived instead for purposes that they may serve as evidence or a testing environment for new features regarding software.

8.6 Policy on technical vulnerability management

The organization “Loco News” is to ensure that technical vulnerabilities are managed properly by a group that is assigned to such tasks by the entities responsible regarding management.

1) In case of changes to the system, Loco News is to do so outside business hours and with proper management, affiliate members and other entities monitoring the situation within a proper environment.

9. Communications security

In order for the organization “Loco News” is to establish a communication security state that has a security parameter set around networks in facilities that either process or handle the information due to the sensitivity of the process.

1) Special controls and monitoring along with authentication.
    a) Network access points, traffic types and limits are to be monitored and changed if they are deemed so by the responsible entities that the organization and its affiliate members may assign. These are solely done for the purpose of safety and this particular guideline is compliant with regulations issued by the Swedish authorities.
2) Security of network services needs to be implemented in accordance to what the network service providers can offer and the employer’s requirements.
    a) The security package that is followed by the providers need to also be compliant with the system of the organization.
3) Groups of information services, users and information systems should be segregated based on networks so that conflicts and intrusion can be avoided as much as possible.
    a) Employees of the organization are to connect on a network which is set up specifically for their work environment and is secure regarding the operations carried out.
    b) Guests are to connect on a network which is set up and asks for authentication by either sending an email or text message to the entity to confirm their usage of the network, and accept the guidelines that the organization might have regarding it.
4) During information transfer within and without the organization, there should be security during the transfer itself. That includes handling different policies, procedures, agreements, confidentiality or non-disclosure agreements in addition to electronic messaging being appropriately protected and monitored by the organization in case of an intrusion.
5) Third parties inclusive or affiliates of third parties interacting with the organization “Loco News” may have different policies, regulations and certifications which can be incompatible with the ones of the organization. That has to be kept in consideration.
    a) If a case of such nature occurs, negotiations are to be established with the opposing party in order for a solution regarding such documents to be found and applied.

10. System acquisition, development and maintenance

System Owners, System Administrators, Project Managers and staff appointed as responsible for purchase are responsible for ensuring that all information systems and services are security reviewed in-line with this policy. This applies to current systems when they are subject to upgrade or change as well as when new systems before they are acquired. Users should only use information systems that are approved by CTO.

10.1 Policy on system acquisition

1) Information security requirements analysis and specification should be included in the requirements for new information systems and enhancements of existing information systems.
2) Requirements should be identified and documented. Requirements should be in-line with business goals, decided business cases and security policy.
3) During the process of identifying requirements following security requirements should be considered:
    a) Cryptographic controls of network communication and hardware storage
    b) Authentication
    c) Authorization process
    d) User's duties and responsibilities
    e) Monitoring and logging of transaction
    f) Interfaces to other systems for exchange of data
    g) For applications with services on public network all security requirements above should be included
4) Acquire of new software, hardware and information services should include:
    a) Formal testing and assessment of identified business goals and security requirements should be carried out and documented
    b) For applications with services on public network a detailed risk assessment of security requirements should be done
    c) Security requirements should be addressed with suppliers and included contracts

10.2 Policy on development and maintenance

1) Information security should be designed and implemented within the systems (soft- and hardware) development life cycle.
2) Testing and development of new systems should be done on servers that are separated from the production environment. This also applies to changes, upgrades and installation of service packages/patches of present systems.

3) For new and existing systems following project method should be applied and documented both for in-house and outsourced projects.
    a) Project objectives, extend and risks
    b) Project plan with budget, timetable, milestones, project organisation, activities and tasks
    c) Mandatory activities and tasks are:
        i. Weekly project meeting and monthly steering committee meeting
        ii. Quality review in conjunction with milestones
        iii. Specification of functionality for new system or changes for existing system and functionality for security should be included
        iv. Development of test and acceptance cases which also includes testing of all security functions
        v. Execution and formal approval of acceptances, test and security cases should be done by executor and project manager. Acceptance cases should also be approved by the system owner
        vi. Implementation and risk assessment plan
        vii. Formal handover to responsible system owner after project is implemented and project closed

11. Supplier relationships

In order for ensuring protection of the “Loco News” resources and information assets, any access provided to supplier or subcontractor of information systems services must be correctly risk-managed and covered by a formal agreement. The formal agreement should at least contain following.

1) Requirement of compliance with “Loco News” project method for development and support of information systems
2) Requirement for Non-disclosure (NDA) agreements with each individual at supplier that has access to information classified as confidential information by “Loco News”.
3) Agreed service level (SLA)
4) Terms of how to solve conflicts and terminate agreement

All employees at “Loco News” who is responsible for purchase of supplier or subcontractor of services of information systems should:

1) Secure that security requirements and procedures are followed by the supplier or subcontractor.
2) In an appropriate way monitor and measure the delivered service:
    a) For service like internet connection monitoring and measure can be done on monthly basis and at total review is done at least every second year.
    b) For development and testing of applications and hardware a weekly or at least a monthly follow up is done of the deliveries and cost according to “Loco News” project plan. Formal reviews should be carried out according to project plan.

12. Information security incident management

In order for establishing an effective security incident management system, all employees, suppliers and subcontractors are responsible for compliance with “Loco News” information and security incident policy.

The CTO of “Loco News” is responsible for:

1) Education and information of all employees, suppliers and subcontractors on how they should handle information and incident security
2) Reporting and classification of security incidents and weaknesses
3) Chain of command and action to be taken for security incidents
    a) Who to contact and when and how an incident should be escalated to the next level of the organisation.
    b) Action and documentation according to classification.
4) At least monthly review of all incidents and decisions on how future incidents should be avoided. This can also be done for the individual incident when it is at hand.

The MD at “Loco News” is responsible that the agenda at each top management meeting contains reporting of security incidents.

13. Business continuity management

In order for establishing a plan to diminish the negative impacts to the company and personnel from accidents or unforeseen events is advised.

13.1 Policy on personnel

1) Adequate personnel responsible in case of disruptive events.
2) Inform personnel on how to proceed on unforeseen events.
3) Documented plans and responses should be developed and approved.

13.2 Policy on software

1) Exercising and testing the functionality of security procedures and tools in order to maintain a safe working environment.
2) Exercising the knowledge and routine in order to ensure that the performance is consistent with the information security objectives.

14. Compliance with laws and regulations

The organization “Loco News” should comply with the following regulations otherwise the corporation might be subject to legal action by an agent.

14.1 Policy on intellectual property rights should be followed

Intellectual property rights include software, copyright, trademarks. In order to not violate them the following procedures are advised:

1) All staff of “Loco News” must prove ownership of individual software licenses. If software is issued by the company then the company must prove ownership instead.
2) Acquiring software only through known and reputable sources, to ensure copyright is not violated.
3) Providing a policy for disposing of or transferring software to each other.
4) Copyright law should always be considered by personnel before publishing articles.
5) All forms of intellectual property rights policies must be made aware to personnel.
6) A Manager must be in place to regulate that all compliances regarding intellectual property laws are followed by personnel.

14.2 Policy on records should be protected

The server room should be protected from destruction, unauthorized access and possible falsification of information located inside. It is advised to do the following:

1) Guidelines should be issued on the retention, storage, handling and disposal of records and information.
2) Retention schedules are used in order to identify records and the period of time it should be retained.
3) An inventory of sources of key information should be maintained.

14.3 Policy on privacy of personal data must be protected

“Loco News” privacy and protection of personal information must be developed, because many of the journalists' lives might come to harm if their information is leaked. A privacy officer is advised, the officer should provide guidance to personnel and service providers on responsibilities and specific procedures.

14.4 Policy on compliance with security policies and standards

Managers should identify cases of non-compliance in the workplace and are expected to act against such cases. Automatic measurement and reporting tools are advised, such measures allow the managers to effectively achieve this goal.

14.5 Policy on technical compliance

"Loco News" systems should be reviewed regularly for compliance with information security policies and standards. Technical compliance objective is to examine the operational systems and ensure that hardware and software controls have been implemented in order to detect vulnerabilities, to be able to test for technical compliance one the following procedures is advised:

1) A technical specialist might generate results with the assistance of automatic tools.
2) A system engineer can manually generate the results.