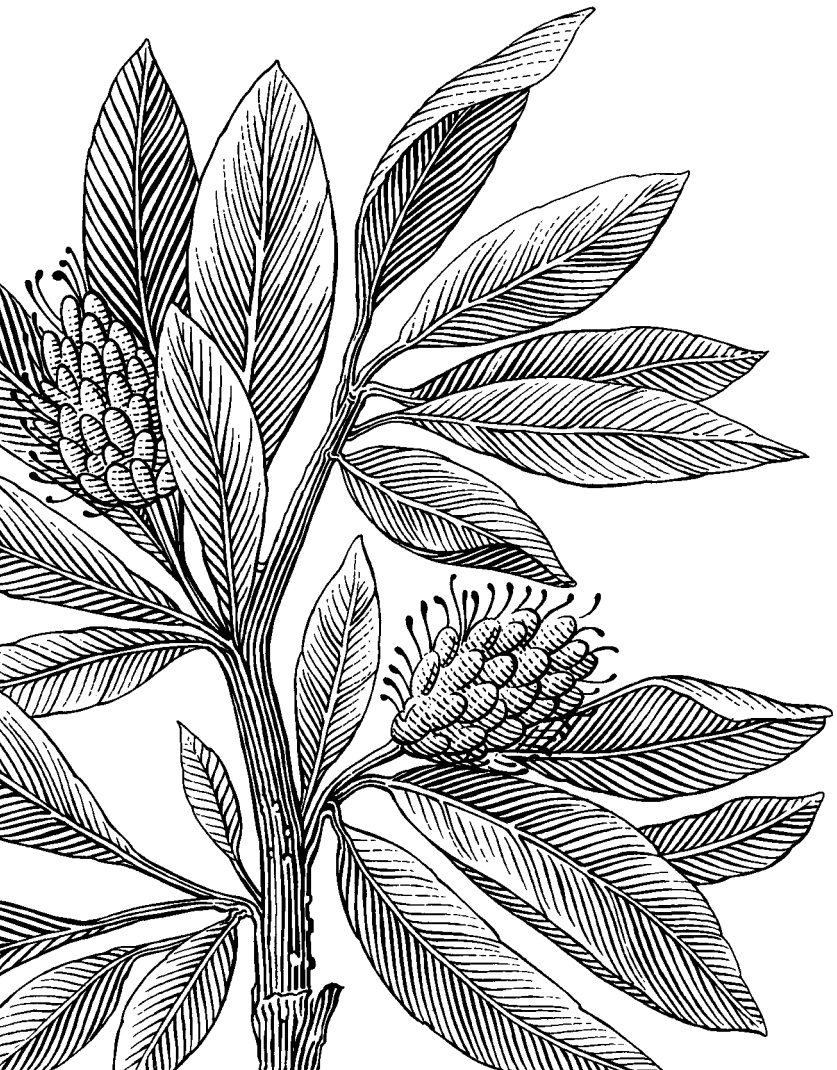
Linnæus University
Sweden

Assignment report

Information security policy document



Author:
Hussam AlKHAFAJI - ha223cz
Paolo Molinaro - pm222py
Rutger Nieuwenhuis - rn222np
Term: HT20
Course code: 1DV700

Linnæus University
Sweden

Contents

1 Introduction

This document is committed to institute an information security policy for Loco News based on ISO/IEC 27002 and GDPR. At the time of writing Loco News has no prior information security policy or high security standards on the sections that are specified in this document.

1.1 Security Goals

Loco News undertakes the implementation and controls the exercise of information security within the organization, to protect the confidentiality, integrity and availability of all assets. Information security responsibilities are fully defined and assigned. Conflicting tasks and areas of responsibility are separated to reduce the chances of misuse, unauthorized or unintended modification of the organization's assets.

This document has the goal to improve company knowledge on "best practices" and keep up-to-date on the subject of information security, and also:

- To improve the company knowledge on "best practices" and keep it up-to-date on the subject of information security.
- To ensure that the understanding of information security issues in the company is up-to-date and complete.
- To promptly receive information (alerts, warnings, patches to be applied) regarding vulnerabilities, possible attacks and countermeasures to be applied.

The overall goals for information security at Loco News are the following:

- To guarantee personnel and collaborators adequate knowledge and an adequate degree of awareness of the problems connected with the information security, in order to allow said subjects to acquire sufficient awareness of their responsibility.
- Ensure compliance with current laws, regulations and guidelines.
- Ensure that all external suppliers are aware of Loco News' information security problems and respect the security policy adopted.
- Comply with requirements for confidentiality, integrity and availability for Loco News' employees and other users.
- Establish controls for protecting Loco News' information and information systems against theft, abuse and other form of harm and loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- Ensure that Loco News is capable of continuing their services even if major security incidents occur.
- Ensure the protection of personal data (privacy) complying to GDPR.
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by Loco News.
- Comply with methods from international standards for information security ISO/IEC 27002.

- Ensure that external service providers comply with Loco News' information security needs and requirements.
- Ensure flexibility and an acceptable level of security for accessing information systems from off-site.

1.2 Security Strategy

In order to secure operations at Loco News even after serious incidents, Loco News shall ensure the availability of continuity plans, backup procedures, defence against damaging code and malicious activities, system and information access control, incident management and reporting.

The term information security is related to the following basic concepts:

- **Confidentiality**: Guarantees that certain information is preserved from improper access and is used exclusively by authorized parties.
- **Integrity**: Guarantees that all information is really that originally entered in the computer system and has been legitimately modified by authorized subjects.
- **Availability**: Guarantees availability of information in relation to the need for continuity of service provision and compliance with the rules that require it to be secure storage.
- **Authenticity**: Guarantees that the information received corresponds to that generated by the subject or entity that transmitted it.

Some of the most critical aspects supporting Loco News' activities are availability and reliability for network, infrastructure and services. Loco News practices openness and principles of public disclosure, but will in certain situations prioritize confidentiality over availability and integrity.

Every user of Loco News' information systems shall comply with this information security policy. Violation of this policy and of relevant security requirements will therefore constitute a breach of trust between the user and Loco News, and may have consequences for employment or contractual relationships.

1.3 Scope & Applicability

This information security policy:

- Applies to all employees, user and staff.
- Covers all information handled, stored, processed or shared by Loco News irrespective of whether that information originates with or is owned by Loco News.
- Applies to all computer and non-computer based information systems owned by Loco News or used for Loco News business or connected to Loco News managed networks.

2 Information security policies

This section provides management directions for information security in accordance with the business requirements of Loco News and relevant laws such as the GDRP in Europe.

2.1 Management direction for information security

This document represents the information security policy for Loco News, it is defined and approved by Loco News management and it is to be communicated to all employees and relevant external parties.

2.1.1 Information security

Information security is Preservation of confidentiality, integrity and availability of information, In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved [1]. The goal of all objectives from this document is to preserve the aforementioned qualities of all Loco News assets.

Information security roles: The responsibility of enforcing this document falls on the management starting from the CTO of Loco News. All other technical responsibilities needed to fulfill this document requirements and policies is the responsibility of the Info-Sec team hired by Loco News either by outsourcing or by full employment. The roles needed includes and not limited to: cyber-security expert, information privacy expert, cryptologist and risk management expert.

2.1.2 Business strategy policies

- Loco News business strategy revolves around the sensitivity of information before publication. Therefore, all employees are required to sign an NDA regarding all information deemed as critical for the business continuation of Loco News.

2.1.3 regulations, legislation and contracts

- Loco News and all its members must comply with all regulations and legislation concerning privacy, processing and storing of personal data and local laws. This includes but not limited to the GDRP and any other law Loco News is under.

- Loco News must specify policies regulating its contracts and outsourcing of work. These policies must protect loco news's resources and critical information.

2.1.4 policies to address the current threat and environment

- Loco News is always threatened by information theft and leakage and must there for specify policies for access control, cryptography, information classification and any other control that will remedy the current or future threats.

2.2 Review of the policies for information security

- Each policy in this document should be reviewed by Loco News periodically and in any other case that calls for the review of this document.

- Each policy must have an owner assigned to be responsible by management, the owner is required to review the policy in the hopes of improving it by applying updates according to the business, legal and environmental requirements of Loco News in which are mentioned above.

3 Organization of information security

3.1 Internal organization

- Loco News is to assign a security manager to take overall responsibility for the development and implementation of information security. The security manager is required to keep all the information security policies mentioned in Information security policies section up to date.
- The security manager may delegate others to fulfill certain security tasks either by direct employment or outsourcing but is still responsible for them and must see them finished.
- The security manager may appoint an owner for each asset (such as sensitive data) who then becomes responsible for its day-to-day protection. The ultimate responsibility always lays on the security manager.
- The security manager has the highest authorization in the company and must be well-screened to assume this role.
- The security manager must be given the opportunity to stay up-to-date with new technologies.

3.1.1 Segregation of duties

- Loco News may find difficulties to segregate duties due to its small size, it is nevertheless required to apply segregation as far as possible by employing certain controls such as monitoring of every operation and auditing as well as constant management supervision.

3.1.2 Contact with authorities

- Loco News must designate a manager who is always in contact with law enforcement and relevant agencies such as data protection agencies. The manager is required to contact the authorities in case of a breach of data or any other incident that might threaten the business continuity of Loco News.
- Loco News must devise a plan of action as part of its security incident management or the business continuity and contingency planning process to ensure that all incidents are reported in a timely manner.

3.1.3 Contact with special groups

- Loco News security personnel must keep contact with groups related to privacy and information processing to keep up with the changing laws and trends.
- Loco News security personnel must keep contact with groups interested in security and vulnerabilities to receive early information on possible threats that might threaten the business continuity of Loco News.

3.1.4 Information security and project management

- Loco News must include its security personnel in the planning and execution of its projects such as upcoming news articles and important announcements as they may entail serious threats to Loco News if disclosed without considerations.
- Loco News must consult its security personnel before, during and after the completion of a project.
- A risk assessment must be completed by the security personnel before the commencement of a project.

3.2 Mobile devices and teleworking

3.2.1 Mobile phones policy

- All mobile devices of employees must be registered and kept on a separate network with limited access and isolation from business information.
- Employees are prohibited from using their mobile phones as a medium to conduct work or to process Loco News's information. All business must be conducted from authorized machines (laptops, desktops) Failure to adhere may cause the employee to endure investigations.
- Every employee must install anti-malware software on their mobile phone and must use cryptography methods and other controls to ensure the safety of their own personal data.
- Employees are prohibited from connecting their mobile phones directly to any machine on-site or any machine off-site that is used to process business information.
- Loco News must arrange for additional training for employees to raise awareness of the dangers of using personal mobile phones to conduct Loco News's work.

3.2.2 Teleworking

- Loco News employees are allowed to work from off-site when they're away on a mission or when they're home.
- Employees are only allowed to telework using authorized laptop machines.
- Employees using the machines to telework must not change anything in the machine's environment without consulting the security personnel headed by the security manager.
- Employees bare the burden to find a secure place to conduct business where information cannot be extracted from them with or without their consent. Failure to do so puts employees in danger of legal actions.

- Employees are never allowed to connect directly to the internal network when working from afar as mentioned on the program security document, approved by management, that specifies the program supporting Loco News's business.
- Employees must configure their home networks according to the recommendations of the security personnel headed by the security manager.
- Loco News reserves rights to all the intellectual property and assets processed by the employees off-site whether this information is produced using a machine issued by Loco News or a personal authorized machine.
- Employees requesting to work off-site must consent to Loco News access to their privately owned machines in case they will be using it to conduct business.
- Employees requesting to work off-site must be given a clear definition of the work they are permitted to conduct as well as the the acceptable hours to conduct the work and the classification of information they might be processing.
- Loco News must conduct training focused around teleworking for all its employees. special training is required for back-ups, physical security, software security and business continuity.

4 Human resource security

4.1 Prior to employment

4.1.1 Screening

- Loco News must conduct screening to all its prospect employees according to the laws and ethics imposed by international and local governments.
- Loco News must at least confirm the applicant by an independent identity verification.
- The prospect employee must posses confirmation of claimed academic and professional qualifications.
- Loco News must run credit score checks and criminal record checks for prospect employees.
- If a prospect is considered for a security related role, extra steps should be taken to confirm that they posses the necessary competence to fulfill the role.
- If the prospect is considered for a security related role, They must go through intensive screening to ensure they can be trusted, especially if the role they might assume is critical to the business.

4.1.2 Terms and conditions of employment

- The contractual obligations must clearly state the information security obligations of every employee or contractor.
- All employees or contractors hired by Loco News who will be accessing confidential data must sign a non-disclosure agreement prior to being given access to information.
- The contract must clearly state the employees or contractor legal responsibilities and rights such as copyright laws and data protection.
- The contract must state actions to be taken if an employee or contractor breaks any of the obligations stated in the contract. These actions include but are not limited to: legal actions, expulsion from work.

4.2 During employment

4.2.1 Management responsibilities

- Loco News management must ensure that employees and contractors are sufficiently explained the information security aspects of their roles and obligations before being given confidential information or/and systems.
- Loco News management must provide employees and contractors with guides that state the information security expectations of their roles.
- Loco News management must ensure that employees and contractors are conform with terms and conditions of employment as well as Loco News information security policy document.

4.2.2 Information security training

- Loco News must provide information security training for its employees as well as for third-party contractors when relevant.
- The information security training must cover Loco News information security policy document as well as any other controls or countermeasures employed by Loco News.
- The training should focus on concerns facing critical assets of Loco News, which are mainly sensitive information and its processing.
- The training must cover basic information security principles such as password and malware protection as well as incident reporting.

4.2.3 Disciplinary actions

- A defined disciplinary process is communicated in the contract to employees and contractors.
- The disciplinary process ensure fair treatment of employees and takes into account all the factors of the incident.
- The disciplinary process is used by Loco News as a deterrent to ensure the following of its security policies and to ensure the confidentiality of its assets.

4.3 Termination of employment

4.3.1 Responsibilities

- Loco News management should clearly communicate the ongoing responsibilities and obligations of past employees and contractors. These obligations include but are not limited to: non-disclosure agreements.

5 Asset management

5.1 Responsibility

These policies aim to identify organizational assets and information assets and to define appropriate protections for them.

5.1.1 Inventory of assets

Assets associated with information should be inventoried to facilitate protection and classification.

- Management of Loco News must identify assets and measure their importance. These assets are usually timely sensitive information in the case of Loco News.

5.1.2 Ownership

All assets belonging to Loco News must be owned to facilitate handling, classification and protection.

- Loco News management must develop a procedure to give ownership of inventoried assets to relevant qualified employees such as security personnel, reporters, editors or managers. The owner can also be an entity inside Loco News.

- Asset owners must ensure that the assets are properly classified and inventoried and must ensure proper destruction when the asset time-frame is over.

5.1.3 Acceptable use of assets/Information

Loco News must clearly specify rules for acceptable use of their assets.

- Management should make aware any employee or third-party contractor of the information security policies if they will be interacting with Loco News assets.

5.1.4 Return of assets

All Loco News assets must be returned after use.

- Loco News management must specify how employees and contractors will return assets after use. In case the assets were bought, management must ensure they are safe to give away.

- In case employees have critical knowledge about an ongoing operation related to Loco News, management should ensure the knowledge is documented.

5.2 Classification

Loco News deals in information. To ensure information is receiving adequate protection, it must be classified very well into several categorize of variable importance.

5.2.1 Classification of information

Information inside Loco News should be classified using known conventions to render it easy to protect the most important assets.

- Assets and information should be classified by their owners as specified previously in this document.
- The classifications should follow a known convention that Loco News management imposes, The owners of assets must be accountable for the classification of their assets.

5.2.2 Labelling

Loco News assets must be labeled by its owners according to the classification scheme devised by Loco News.

- Owners of assets should apply clear labels to their classified information.
- The labelling of assets follows the same convention imposed by Loco News and specified in the previous section.

5.2.3 Handling of assets

Loco News assets must be handled according to the classification scheme devised by Loco News.

- Loco News must ensure safe handling of assets by developing clear procedures conforming with conventions imposed by Loco News.
- The procedure must detail all possibilities of assets such as temporary copies of assets or assets off-site of Loco News location.

5.3 Media handling

Loco News business revolves around information, Media handling ensures that this information is safe and is used according to known defined procedures.

5.3.1 Removable media

Removable media should be discouraged inside Loco News as they represent an attack surface where a rogue employee might transfer data, However, if there are no other options for transfer, removable media must be regulated to ensure safety of assets.

- Loco News must define procedures that are conform with their classification scheme to handle removable media.
- Loco News must only use removable media if there are no other available secure options.

- Transfer from and to removable media must be recorded by the security personnel.
- Assets inside removable media must be rendered unusable if no longer needed.
- Loco News security personnel, specifically the cryptologist, must define a cryptographic procedure to ensure the integrity and confidentiality of Loco News assets inside removable media.

5.3.2 Disposal of media

Since Loco News is in possession and will be in possession of highly sensitive data, any media on-site or off-site must be disposed of securely according to defined procedures.

- Any physical media is to be disposed of using conventional means such as shredding and ignition.
- Any electronic media is disposed of by handing it to the security team who will perform multiple secure wipes and removals to ensure secure disposal.

5.3.3 Physical media transfer

Loco News assets must be protected while in transfer as confidentiality is the most important quality for business continuity for Loco News as a news company.

- Physical media is to be transferred through either trusted employees or through trusted bodies such as the governmental post offices.
- Management should publish a list of trusted transfer mediums that are not related to Loco News directly.
- Security personnel must keep logs of transferred media. This includes time, destination, source and method of protection.

6 Access control

Restricting access to information and information processing services, using the two principles of ”need-to-know” and ”need-to-use”, is considered a fundamental objective of Loco News. All Loco News staff and interested third parties must be informed about the existence of a specific policy for the management and control of logical access to resources and bound, depending on their responsibilities or skills, to comply with the requirements. The instrumentation and instructions for access control must be kept constantly adequate to the business and access security needs, also in relation to organizational and technological developments.

6.1 Logical Access Control

Loco News provides and implements the process of ”Logical Access Management” for the assignment or revocation of access rights for all types of users and for all systems and services it provides to users, and it consists of the following:

- Access to information and functions of application systems must be limited to actual needs (need-to-know and need-to use).
- Removal or adaptation of access rights: the access rights of all personnel and users of external parties to information and information processing facilities must be removed upon termination of the employment relationship, contract or agreement, or adapted to any changes.
- Upon leaving the company, the access identifiers of personnel no longer in service and consultants no longer operational will be deactivated. Access must be revoked and the authorizations must be deleted correctly before getting subsequently assigned to different people.
- Management of privileged access rights: the assignment and use of utilities and administrative privileges must be restricted and controlled.
- In case it is necessary to access specific data/systems ”in an emergency”, personnel not yet qualified must request temporary qualification.
- Control of access to the source code of the programs: access to the source code of the programs must be limited to the actual operational needs and allowed only to authorized users.
- In case of the definition of new access credentials or modification of existing, a notification is sent to the interested party; it accesses the company information system in which it consults the credentials assigned and records its acceptance.

6.2 Passwords, Credentials and Authentication Tools

- The use and management of credentials must guarantee to avoid improper use of passwords and authentication credentials.
- Passwords generation rules apply to all personnel and third parties who use them to access company assets.

- The use of passwords and user credentials in general must be controlled with a formal management process.
- Password management systems must be interactive and must ensure quality passwords.
- Authentication systems must enforce compliance with the password policy.
- Credentials are personal and non-transferable, they must be assigned based on the need-to-use data or to company systems and must be managed at the same time as qualifications, based on the principle of “minimum privilege”.
- The passwords must be ”strong”, meaning constructed so as not to be easily guessed and carefully guarded, as well as being changed periodically.
- Authentication systems must ensure that the use of credentials complies with security policies.

6.3 Secure log-on procedures

Access to systems and applications must be controlled by secure log-on procedures. The use of utilities that may be able to bypass application and system controls must be limited and strictly controlled. The rules for accessing the corporate network via connections from the offices and remote locations must be followed.

Access to operating systems and applications must be controlled by log-on procedures:

- All Users must have an identification for personal use only, and a suitable identification technique must be used to ensure the claimed identity of a user.
- Identification codes, once used, cannot be reassigned to different people, even after some time.
- Systems must be in place to ensure an adequate quality of the passwords.
- Access to information and functionality of application systems by users and support staff must be limited on the basis of necessity.
- Systems critical to business and information security must have dedicated computing environments and systems.

The credentials are personal and non-transferable. Each user is responsible for the correct management of his own password, recognition devices, information for accessing systems and data. The credentials and identification devices must be properly stored and never be left unattended.

7 Cryptography

Cryptographic controls are needed to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. This includes information on employees' computers and information in the local database. A cryptography expert must be consulted to approve and renew the policy on the use of cryptographic controls. The consultation of a cryptography expert is necessary to maximize the benefits and minimize the risks and to avoid incorrect use. This includes the following rules and practices:

- Cryptographic algorithms, key lengths and usage practices must be selected according to best practice.
- Appropriate key management must be followed to secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying keys.
- Appropriate key management must be followed to secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying keys.
- All cryptographic keys must be protected against modification and loss; the authenticity of public keys should also be considered.
- In addition, secret and private keys must be protected against unauthorized use as well as disclosure.
- Equipment used to generate, store and archive keys has to be physically protected.
- All assets generated from Loco News need to have digital watermark and digital signature.
- Asymmetric encryption will be used for authentication purposes, for large amount of data (to ensure better performance and speed), and for data-at-rest (local backup).

8 Physical and environmental security

Loco News needs suitable physical access control measures and access rules for employees:

- Security perimeters must be defined and used to protect areas containing critical information and information processing structures;
- It must be assured that only authorized personnel can have access within the company perimeter.
- The premises containing IT equipment critical to the business, subject to specific regulations, or IT archives containing sensitive data, must be further controlled; unauthorized personnel cannot access it.
- Physical security must be designed and applied to offices, premises and plants.
- Procedures must be designed and implemented to work in safe areas.
- Access points through which unauthorized personnel could access the premises, must be controlled and, if possible, isolated from the information processing facilities to prevent unauthorized access.

The following is the floor plan of Loco News that can be used for reference while addressing the ”Physical Access Management” explained in the next subsection:

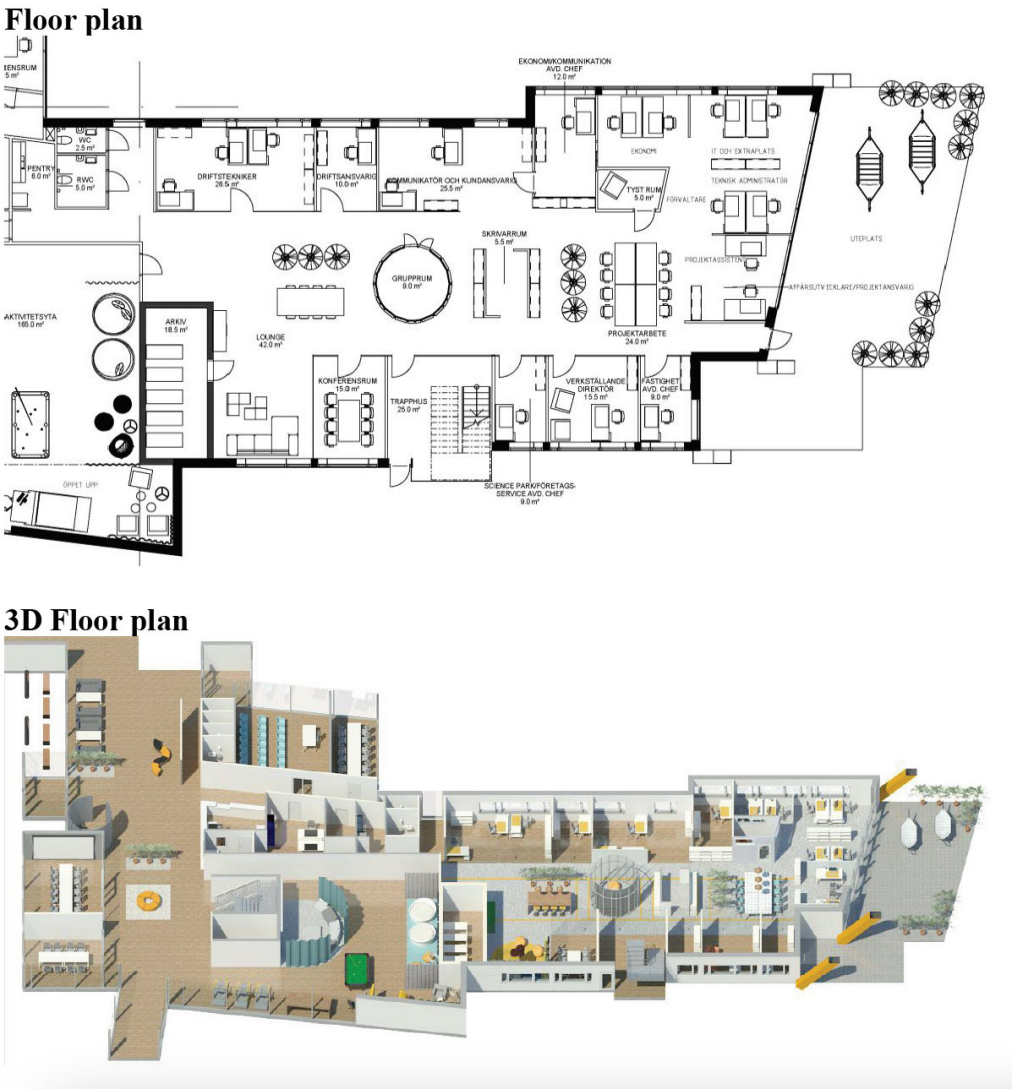


Figure 1. Loco News Floor Plan

8.1 Physical Access Management

A ”Physical Access Management” policy, and related responsible, should be instituted with the purpose of defining the system of authorizations and operating methods for managing access and staying in the Loco News offices during and outside normal service hours. It regulates access of employees, staff of external Companies / Bodies as part of the execution of a contract stipulated with Loco News, occasional visitors-guests, regular guests. Its scope includes:

- Access to all places and equipment relating to security.
- Methods of granting and revoking access authorizations.
- Methods for registering access.
- Required controls.

The process identifies, defines the roles, responsibilities, and modalities of:

- Access points of the Loco News offices and the protected premises located inside the offices.
- Access records.
- Surveillance, anti-intrusion and fire control systems.
- Request and assign access authorizations.
- The use of necessary access devices (badges, readers, turnstiles, etc.).
- Management of physical access of people entering and exiting the premises and protected premises.
- Management of the reception of people who do not belong to the company.

9 Operations security

As an organization with data assets, Loco News possesses information processing facilities, such as the local database. These facilities need to be protected in accordance with ISO/IEC 27002.

9.1 Management

To ensure the security of information processing facilities, Loco News needs to appoint a skilled person or a group of skilled persons as the responsible entity. The responsibilities of this entity will include:

- The documentation of operating procedures and making this document accessible by customers, as well as periodically reviewing and changing this document when necessary.
- The regulation of changes to organization, business, information handling facilities and systems altering information security, as well as maintaining an audit log of important customizations.
- The supervision of resource handling to guarantee the appropriate performance of systems, as well as monitoring systems and implementing controls to detect problems in time.
- The supervision of the separation of operational environments, advancements and verifications. This limits unauthorized access and disturbance to production.
- The addressing of potential technical vulnerabilities within a reasonable time frame to prevent further exploitation of the vulnerability. The entity should forward the technical vulnerability securely to those who can resolve it, for example the company technicians.

9.2 Malware

The information processing facilities need to be kept free from malware to ensure confidentiality, integrity and availability of the information contained in these facilities. Therefore, malware protection software should be installed on the devices of Loco News, as well as on the server. The current installation of anti-malware needs to be reviewed for effectiveness and update policy. If it is deemed not sufficient, other anti-malware software should be acquired. Furthermore, users need to be made aware of digital hygiene to further limit the chances of malware infection.

9.3 Back-ups

To avoid loss of data, the server needs to be regularly backed-up into the cloud as described by the Loco News system design document. Back-ups should happen on at least a daily interval.

9.4 Logging

To document incidents and produce evidence of potential incidents, user actions, exceptions, faults and accesses need to be logged. This includes actions taken by

administrators and privileged users. Logs need to be reviewed periodically to spot suspicious action.

Since logs may contain sensitive information, and must be protected from tempering, logs should be kept safe. They should be stored as copies outside of system administration.

It is of importance that all devices within the Loco News system have their clocks synchronised to the same time origin. This prevents timing issues in programs and logs. The changing of system time should only be available to administrators.

9.5 Control of operational software

To protect the confidentiality, integrity and availability of information systems, installation of software should abide to certain regulations. This is in order to protect against potentially damaging software being installed on Loco News systems. These regulations can include:

- Only installing software from approved sources.
- Only installing software that has been reviewed and approved by administrators.
- Only installing certain kinds of software.

The employees need to be made aware of these regulations.

9.6 Information system audits

Audits of the information systems need to be carefully planned, in order to not disturb production. For example, the local server cannot be offline during working hours, as this would disrupt employees.

10 Communications security

Communication networks must be adequately and constantly manned and monitored against intrusion, interception and attack attempts, in order to protect information in systems and applications.
The security mechanisms, service levels and management requirements of network must be identified and included in the service level agreements relating to the network, regardless of whether such services are provided internally or outsourced.
Networks must segregate groups of services, users and information systems to depending on the level of risk incumbent on the related assets. The development and production environments must be separated, defining suitable sub-networks isolated from each other or with controlled interconnection.

Loco News is equipped with an internal network, for temporary cache, and a could-based solution. A suitable level of security must be guaranteed for it; therefore, connections with the internal network from off-site users are forbidden in violation of company rules.
Employees must connect to the internal and external network only in compliance with the rules:

- Transmission of confidential information must take place within the network with authorized direct transfer protocols.
- Internet access within the workplace is restricted and monitored.
- Connections to networks via wireless connection can be made only by work devices with access control authentication.
- Internet navigation for guests, visitors and others is restricted and monitored.
- Connections from off-site employed is granted via extranet and proper authentication.

11 Systems acquisition, development and maintenance

11.1 Monitoring, Tracking and Testing

To guarantee the detection of anomalous events, accidents and vulnerabilities of information systems in order to ensure the security and availability of services and related information:

- The information systems, meaning the server room, the network and backup, must be periodically checked in order to assess the correct functioning of the security systems, hardware and software, implemented, as well as the presence of any vulnerabilities not found or known in the past.
- In the face of the results of all monitoring, tracing and verification activities, periodic analysis activities must be carried out, aimed at identifying critical areas and appropriate corrective and improvement actions.
- Periodic audits of the information security management system must be planned.
- Periodic reports must be requested to the cloud service provider.

11.2 Life cycle of system and services

To ensure that security aspects are included in all phases of design, development, operation, maintenance, assistance and decommissioning of IT systems and services, in the design and development phase, safety aspects must be appropriately considered.
In particular, the following issues must be addressed:

- Inclusion of the security requirements, also to protect any personal data processed, in the functional specifications of the services and systems.
- Adoption of best practices for software development and maintenance, like: schedule a regular maintenance, always make it a priority to review urgent fixes, test updates, and replicate in production.
- Periodic controlled management of documentation.
- Preparation of development and test environments with the use of formal acceptance procedures in the passage between environments.

In the operation phase, safety aspects must be appropriately considered. In particular, the following issues must be addressed:

- Capacity management of the technological infrastructure.
- Security of systems and data (configuration management, hardening, installation of anti-malware systems, encryption).
- Periodical check of backup and restore procedures.

- Periodical procedures for controlled decommissioning of systems (for example secure erasing of drives).
- Network security: segregation of networks, monitoring of gateways (firewalls).

Security aspects must be appropriately considered in the management of services. In particular, the following issues must be addressed:

- Monitoring of systems and services.
- Utilities management.
- Performance monitoring.

12 Supplier relationships

Company assets accessible by suppliers must be protected to maintain confidentiality, integrity and availability according to ISO/IEC 27002. At present, there is no agreement between Loco News and their suppliers.

12.1 Loco News supplier relationships

Loco News contains of one small office. As such, the needed supplies are very limited, and are constraint to basic office supplies. In addition to that, Loco News is planning to outsource work. A general agreement needs to be drafted for these supplier relationships.

12.2 Supplier relationship agreement

To supply any goods or services to Loco News, the supplier must agree to the following terms:

- Before, during and after accessing company assets, the supplier (and any goods or services they supply) will be subjected to extensive background checks to ensure the safety of company assets.
- For accessing any company assets, the supplier needs explicit permission. Initial accessible company assets will be discussed in the contract between the the supplier and the company. Additional assets that the company might want to access later on need explicit permission, which can be requested to the person responsible for supplier relationships (See next subsection).
- The supplier agrees not to intentionally cause harm to company assets, and to take measures to prevent unintentional harm to company assets.
- The supplier agrees that any actions they take on company assets are subjected to supervision.
- Any changes to this agreement by either party will have to be discussed between the company and the supplier before they take effect.

12.3 Enforcing and handling the supplier relationship agreement

To handle the supplier relationship agreement, one person or a group of people with appropriate skill are to be appointed responsible for supplier relationships. They should be given sufficient resources to handle their responsibility. This entity's responsibility includes:

- Enforcing the agreement and implementing controls (for example, supervising access to company assets).
- Handling supplier requests to new company assets.
- Discussing changes to the supplier agreement, requested by either the company, the supplier or another party.

- Customizing and extending the agreement for new supplier relationships, if necessary.

Furthermore, this entity should assess the necessity of the continuity of each supplier. If the continuity of the supplier is of importance, back-up suppliers should be prepared and managed in case the current supplier becomes unavailable, keeping in mind that the agreement for these supplier might be different than from the current one.

13 Information security incident management

It is of high importance that information security incidents are managed properly to avoid (further) damage to company assets, and to ensure the company can continue operating as much as possible. This should be done in accordance to ISO/IEC 27002.

13.1 Objectives in case of an information security incident

Information security incidents vary in severity. To assess which actions should be taken in case of an incident, it is important to set out certain objectives.

- **Confidentiality**
  In case of an information security incident, it is important to asses what data might have been compromised. In case this data breaks confidentiality agreements, appropriate actions should be taken. This can include actions to prevent the breach of further confidential data (such as taking servers offline), and to notify parties who might be affected by this breach of confidentiality.

- **Integrity**
  It is important to assess the integrity of data that might have been compromised, to prevent issues that false data might cause. This can be done by for example comparing previous hash values or back-ups of the data.

- **Availability**
  It should be assessed how the information security incidents affects the availability of assets, and consequently, the business continuity of the company. It is important that the company can resume business as much as possible in the case of an incident, for example by restoring back-ups.

13.2 Responsibility

To avoid disorder and to ensure a coordinated and organized response to an information security incident, a person or a group of people with appropriate skill should be appointed responsible for information security incidents. It is important that this entity knows objectives in case of an information security incident, as listed above. In case the incident exceeds organizational boundaries, this entity should work together the appropriate organizations for a collaborative response.

This entity also needs to be available (by employees and by outsiders), to contact in order to report information security incidents or weaknesses. This will result in faster responses, which will limit the potential damage caused by the incident or weakness.

It is possible to outsource the responsibility to an information security incident response team (ISIRT) to function as the required entity. The point of contact can be a company employee, that will forward the incidents to the ISIRT.

13.3 In case of an information security incident

In case of an information security incident, the responsible entity should:

- Assess the damages and classify the incident according to a scale. If an ISIRT is hired, this assessment should be done by the point of contact and then forwarded to the ISIRT for the following steps. Assessments should be recorded for future reference.
- Ensure that normal security level is resumed to prevent further damage.
- Recover and take action according to the objectives listed above.
- Conduct post-incident research to identify the source and work with evidence, in order to learn from incidents and take potential disciplinary/legal action. This should be done by certified personnel and tools, as this will strengthen the value of the evidence. When working with evidence, it is important to:
  - **Identify**
    Search for and recognize evidence
  - **Collect**
    Gather physical evidence
  - **Acquire**
    Create a copy of the evidence
  - **Preserve**
    Maintain the integrity of the evidence.

  It is advised to involve authorities when working with evidence, to prevent the hinder of legal action by improper handling or destruction of evidence. Be aware that evidence might exceed organizational or jurisdictional boundaries.

13.4 Security awareness training

All employees should go through mandatory security awareness training, in order to avoid accidental damage to company assets by employees. This training should include the following topics:

- General digital hygiene
- How to identify an information security incident. Examples of past incidents can be used.
- How to act in an information security incident:
  - Immediately notify the point of contact.
  - Carefully follow the instructions given by the point of contact. Do not attempt action on your own, as this might cause accidental damage to company assets.
- How to identify an information security weakness. Examples of past weaknesses can be used.

- How to act when an information security weakness is discovered:
  - Do not exploit the weakness or research the weakness further, as this might cause accidental damage to company assets.
  - Notify the point of contact about the weakness immediately.

14 Information security aspects of business continuity management

Adverse situations might intervene with Loco News business. It is important to have a business continuity and disaster recovery plan for adverse situations. Information security should also be taken into account in accordance with ISO/IEC 27002.

14.1 Information security in business continuity plan

Inside the Loco News business continuity and disaster recovery plan, an explicit section discussing information security should be included. What information security requirements should be included here, varies per adverse situation and severity of the disaster and should be discusses by the creator of the plan and the information security management entity of the organization. Generally, the information security requirements specified in this policy can be adhered to in adverse situations.

14.2 Handling information security requirements in adverse situations

In case of an adverse situation, the organization should ensure the required level of information security continuity. The information security entity of Loco News should ensure that information remains protected during business continuity processes. If any security controls fail during these processes, other controls should be implemented to remain at the acceptable level of security.

14.3 Ensuring information security continuity

To ensure information security continuity, continuity controls should be regularly tested for functionality and effectiveness, as well as general knowledge in adverse situations. These tests should be included with the organization's business continuity and disaster recovery tests, separated from general information security tests.

If security requirements change, continuity controls need to be reviewed. This ensures correct controls in adverse situations.

14.4 Redundant systems

An important control to assist information security in adverse situations is the presence of redundant systems. In adverse situations, the availability of the organization's local server cannot be guaranteed. It is therefore important the there are redundant server components available, so that in case of a destruction of the server in adverse situations, there can be a quick conversion to the redundant components, followed by the restoration of a cloud back-up to ensure availability of the Loco News server during adverse situations. It is important that this conversion is tested, to ensure no further complications in adverse situations.

15 Compliance

As an organization, Loco News has information security obligations that need to be abided to, in accordance with law, ISO/IEC 27002 and other entities that provide regulations.

15.1 Identification of obligations

It is important that all information security requirements are identified and documented. These requirements may include:

- Swedish law
- General Data Protection Regulation (GDPR)
- Obligations stated by contracts between organizations
- Obligations stated by companies disclosing data to Loco News for article purposes
- Obligations derived from intellectual property rights and proprietary software

15.2 Protection of records

As an organization with data assets, records need to be protected according to the GDPR. These regulations may vary per data set. Data sets should be classified using a classification scheme. Regulations may include:

- Reasons for data storage [2]
- Encryption of data [3]
- User requests to edit or delete personal data [4].

The type of system used for storage should also be considered. The system should allow for accessibility of data in a reasonable time frame, deletion of data and hardware degradation.

15.3 Abiding by regulations

It is of great importance to abide by the required regulations to prevent legal actions or deterioration of company relationships. Several steps should therefore be taken to ensure compliance:

- A skilled, overseeing entity needs to be appointed responsible for compliance with obligations. This entity can seek advice from experts in specific topics, such as:
  - Privacy laws
  - Cryptographic laws
  - Data protection laws

- The requirements needs to be regularly reviewed and kept up-to-date by the responsible entity.
- Employees need to be made aware of their responsibilities regarding compliance to obligations. This can include things such as:
  - Privacy of interviewed subjects
  - Intellectual property rights and usage of proprietary software
  - Leakage of protected information

15.4 Information security reviews

To ensure the compliance to obligations, periodic reviews are required. Guidelines for these reviews include:

- Any review should be done by competent and authorized entities or under supervision of such entities.
- Regular reviewing of compliance of information processing procedures by the skilled, responsible entity. Automated tools can assist with the reviewing process. In case of non-compliance, the responsible entity needs to:
  - Identify the fault
  - Evaluate the fault
  - Correct the fault
  - Review again to make sure there is compliance after the correction.

  Results of reviews should be recorded and forwarded to independent reviewers (see next point).
- Besides regular reviews by responsible entities, information security controls should also be regularly reviewed by skilled, independent entities to avoid potential mistakes by the responsible entity.
- Information systems need regular review by technical specialists.

References

[1] Information security. [Online]. Available: https://en.wikipedia.org/wiki/Information_security#Definition

[2] General data protection regulation (gdpr) recital 39. European Parliament and Council of the European Union. [Online]. Available: https://gdpr-info.eu/recitals/no-39/

[3] General data protection regulation (gdpr) article 32. European Parliament and Council of the European Union. [Online]. Available: https://gdpr-info.eu/art-32-gdpr/

[4] General data protection regulation (gdpr) recital 65. European Parliament and Council of the European Union. [Online]. Available: https://gdpr-info.eu/recitals/no-65/