Linnéuniversitetet
Kalmar Växjö

Information Security Policy
Loco News

Group Members: <Viktor Petelin>, <Saki Dollfus Di Volckersberg>, <Sameed Alam Khan>, <Ekaterina Simakina>

1. Introduction

The company's information security policy (ISP) defines a system of views on the problem of ensuring information security. It is a systematic statement of high-level goals and objectives of protection, which must be guided in its activities, as well as the basic principles of building an information security management system (ISMS) of the organisation. Ensuring information security is a necessary condition for the successful implementation of the statutory activities of the company. Ensuring information security includes any activity aimed at protecting information resources and/or supporting infrastructure. The Policy covers all automated and telecommunication systems owned and used by the company, Loco News.

2. Purpose

The main aim of this Policy is to protect information resources from possible material, physical, moral or other damage to them, through accidental or intentional impact on information, processing and transmission processes. This policy is set to minimise risks of information security.

To achieve the main goal, it is necessary to ensure the effective solution of the following tasks:

- timely identification, assessment and forecasting of sources of information security threats;

- creation of a mechanism for rapid response to information security threats;

- prevention and/ or reduction of damage from the implementation of information security threats;

- protection against interference in the process of functioning of

by unauthorised persons;

- ensuring the continuity of critical business processes;

- achieving adequacy of measures to protect against information security threats;

- study of partners, clients, competitors and job candidates;

- preventing the infiltration of organised crime structures and individuals with unlawful intentions;

- identification, prevention and suppression of possible illegal and other negative activities of employees;

- improvement of business reputation and corporate culture.

3. Grounds for development

This policy has been developed on the basis of the standard ISO/IEC 27002 as well as interests and goals of the organisation.

4. Scope

This policy applies to all business processes of the Institution and is mandatory for use by all employees and management of the Institution.
The policy applies to the information systems of the company.
Persons who are engaged in the development of internal documents of Loco News, regulating information security issues, have to be guided by this Policy.

5. Information security policies

5.1 Management direction for information security.

Management should define a set of policies to clarify their direction of, and support for, information security. Information security policies should be reviewed at planned intervals, or in the event of changes in the organisation's environment, business environment, legislation, or technical area, to ensure their continuing suitability, adequacy and effectiveness. The assignment of general and specific responsibilities for managing information security to certain roles, processes for handling deviations and exceptions should also be carried out.
The policy should include access control, information classification, physical and environmental security, acceptable use of assets, mobile devices and teleworking, restrictions on software installations and use, protection from malware, cryptographic controls, management of technical vulnerabilities, privacy and protection of personally identifiable information , supplier relationships. Company policy should also provide a foundation for information security and should be part of an education, training and awareness program.

6. Organisation of information security

6.1 Internal organisation.

All information security responsibilities should be defined and assigned. In determining responsibilities, account should be taken of the ownership of information assets or groups of assets.
Role Based Access Control (RBAC). It is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with specific business functions - for example, executive level, engineering level 1, etc. - rather than based on the identity of individual users. The role-based security model builds on a complex structure of role assignments, role authorization, and role permissions, designed using role-based engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC structures.
One of the goals of role allocation is to reduce the potential for unauthorised or unintentional changes or misuse of any of the organisation's assets.
Adequate contacts should be maintained with the relevant authorities and contacts with interest groups or other specialised security forums and professional associations.
The governments of many countries are interested in ensuring and developing cybersecurity and personal data protection in particular. The European Cybercrime Convention acts at the world level to combat Internet fraud and provides national criminal law institutions with cooperative mechanisms to investigate and prosecute computer crimes. For example, The General Data Protection Regulation 2016/679 is “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April

2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data". There are also many standards and protocols that help to implement data protection in compliance with legislation such as ISO / IEC 27001 - this is an international standard for information security
management. Domestic legislation of countries is often based on international agreements that are used to regulate confidentiality.
It is necessary to choose the person who will establish this contact, determine the circumstances and the nature of the information that should be provided. Information security must be taken into account in project management regardless of the type of project.

6.2 Mobile devices and teleworking.

The organisation is responsible for developing policies for mobile devices and should provide for registration / de-registration of mobile devices, physical security requirements, technical security requirements including remote connections, software management, access control, and encryption at rest. /on my way.
The system must be designed with the context in which it will be used and where the data will go. The mobile application must be secure and the choice of a vulnerable programming language can harm the application. The system must be designed with the context in which it will be used and where the data will go. The mobile application must be secure and the choice of a vulnerable programming language can harm the application. The main conditions for this choice: 1. Maximum control from the programming language, strict types of languages so that the compiler or development environment catches data errors and compilation. 2. Compilation - checking the code before it is executed.
Data should not be code, so passer functions with full caller privileges should not be used when writing code. Program execution is memory safe until a certain list of bad things, called memory access errors, occurs: buffer overflow, dereferencing a null pointer, use after free, use of uninitialized memory, illegal release (of an already freed pointer or a pointer without errors).
The physical security of devices in public places and other unprotected places should also be considered. Employees should be aware of the need to constantly protect their device from unauthorised access.
The use of a VPN is recommended. Provider (ISP) has access to everything that a user does on the network. Note that internet traffic may include sensitive information such as a bank account information, credit card numbers or login credentials. Attackers use wide networks, so accessing the Internet without a username, password, and VPN poses a higher risk. To mitigate this risk, the company should use a VPN and set a password to use the Internet on its premises. The main purpose of using a VPN is to hide online activity, create enhanced privacy and internet security for a PC or any other device. VPN helps to protect a company, a user from hackers and surveillance on public networks. VPN is also useful for hiding IP address, browsing activity, and identity on any Wi-Fi network. It helps a user to browse the web safely and securely by encrypting the connection and hiding the location, username and password to log in. VPN, when combined with additional anti-tracking tools, can increase anonymity and help hide from intruders. Using a VPN for the network not only adds an extra layer of protection, but it also makes it harder to see what a user does, since hackers will not be able to find the IP address.

7. Human resource security

The roles and responsibilities for ensuring the security of information resources, described in accordance with the Organisation's Information Security Policy, must be communicated to the employee during employment and included in his or her job responsibilities. This should include both general responsibilities for implementing and maintaining the security policy and specific responsibilities for protecting resources.

7.1. Terms of employment.

All hired employees have to approve and sign their employment contracts, which establish their responsibility for information security (IS). The agreement has to include the consent of the employee to carry out control activities on the part of the company for verification of compliance with IS requirements, as well as the obligation to non-disclose confidential information. The contract must describe the measures which will be taken in case of non-compliance by an employee with information security requirements. Responsibilities for ensuring information security should be included in the job descriptions of each employee of the company. All hired employees must be familiarised with the list of information, limited access, with the established regime with it and with the measures of responsibility for violation of this regime. When providing employees access to the company's information system, they have to familiarise themself with signatures about the instructions for the users of the information system.

7.2. Responsibility of management.

The Management of the company Loco News should require all employees, contractors and users of third parties to take security measures in accordance with the policies and procedures established in this organisation. In accordance with the established procedure, without notifying users Authorised employees by the management of the company have the right to carry out inspections such as:

- Implementation of existing instructions on information security issues;

- Data located on data carriers;

- The procedure for the use of information resources by employees;

- Contents of official correspondence.

7.3. Information Security Training

All employees must undergo periodic training in the field of information security policies and procedures adopted by the company.

7.4. Termination or modification of the employment relationship.

In case of dismissal, all rights granted to the employee to access information system resources should be removed. When labour relations change, only those rights that are not necessary in a new employment relations are removed.

8. Asset management

In the company Loco News, all resources should be identified and evaluated in terms of their importance. A register (list) should be drawn up for all valuable resources.

Thanks to information about the resources of the organisation, information is protected, the degree of which is commensurate with the value and importance of the resources.

The following types of resources are available in the companies' information system:

- information resources containing confidential information and/or restricted access information, including information on the financial activities of the Institution;

- openly disseminated information necessary for the work of the organisation, regardless of the form and type of its presentation;

- information infrastructure, including information processing and analysis systems, technical and software means of its processing, transmission and display, including channels of information exchange and telecommunications, information protection systems and means, objects and premises in which such systems are located.

For each resource, an owner should be assigned who is responsible for the appropriate classification of information and resources related to information processing tools, as well as for the assignment and periodic verification of access rights and categories defined by access control policies.

Classification of information

All information resources to be protected should be classified according to the importance and degree of access.

The classification of information must be documented and approved by the management of the company.

Classification of information should be carried out by the owner of the resource storing or processing information to determine the category of the resource. Periodically, the classification should be reviewed to maintain its relevance to the resource category. Resources containing confidential or critical information should have a corresponding mark (stamp).

9. Access control

The main users of information in the company's information system are employees of structural divisions.

The level of authority of each user is determined individually. Each employee uses only the rights prescribed to him in relation to the information with which he or she needs to work in accordance with the duties of the post. The admission of users to work with information resources should be strictly regulated. Any changes in the composition and powers of users of subsystems should be made

in accordance with the established procedure, in accordance with the regulations for granting user access.

Each user allowed to work with a specific information asset (IA) of the organisation must be assigned a personal unique name (user account), under which he or she will register and work with IA. In case of production need, several unique names (accounts) can be mapped to some employees.

A temporary account can be created for a user for a limited period of time to perform tasks that require extended powers, or to configure, test the information system, to organise guest access (visitors, employees of third-party organisations, interns and other users with temporary access to the information system).

In general, it is forbidden to create and use a shared user account for a group of users. Where necessary, due to the nature of the automated business process or work organisation, the use of a shared account must be accompanied by a note in the computer time log that must uniquely identify the current account holder at any given time.

Simultaneous use of one common user account by different users is prohibited.

Registered accounts are divided into:

- User account. It is designed for authentication users of the company's information resource;

- System account. It is used for the needs of the operating system;

- Service account. It is designed for the functioning of individual processes or applications.

System accounts are generated by the operating system and should only be used in cases prescribed by the operating system documentation.

Service accounts are used only to run and operate services or applications. The use of system or service accounts to register users in the system is strictly prohibited.

Information Security Policy Organisation Procedures for registering and blocking user accounts should be applied in compliance with the following rules:

- the use of unique identifiers (ID) of users to unambiguously identify and compare the person with the actions committed by him;

- allow the use of group ID only if it is necessary to perform the task;

- the granting and blocking of rights must be authorised and documented;

- granting access rights to the information resource, only after coordination with the owner of this information resource;

- registration and blocking of accounts are allowed with the separate permission of the Management of the company;

- the level of authority granted shall be in accordance with the operational necessity and this Policy and shall not jeopardise the delimitation of operating modes;

- coordination of changes in access rights with the information system department;

- documentation of access rights assigned to the user;

- familiarisation of users under the signature with written documents in which their access rights are regulated;

- granting access from the moment of completion of the registration procedure;

- ensuring that a formal list of all users registered to work with the AI or service is created and maintained;

- immediate deletion or blocking of access rights of users who have changed their position, form of employment or resigned from the Institution;

- auditing ID and user accounts for unused ones, deleting them and locking them.

- ensuring that unnecessary user ID are not available to other users;

- enable users to be granted access according to their job titles based on business requirements by summarising a number of access rights into generic user access profiles.

9.1 Privilege management

An employee's access to the company's information resources has to be authorised by the head of the structural unit in which the employee is enrolled according to the staffing table and the owners of the corresponding information resources. Access is managed in accordance with established procedures. The granting of privileges and their use should be strictly limited and manageable. The distribution of privileges should be managed through the registration process of these privileges.

The following steps should be considered:

- The access privileges associated with each system product, such as the operating system, database management system, and each application, as well as the users to whom they should be granted, must be identified.

- Privileges should be granted to users on the basis of business necessity and only for the period of time necessary to achieve the intended objectives, for example, privileges that are minimally necessary to perform their functional duties, only when these privileges are necessary;

The organisation's information security policy to achieve its goals, such as the privileges minimum required to perform their functional duties, only when those privileges are necessary;

- there must be a process for authorising and reporting on all privileges granted, and privileges cannot be granted until the registration process is complete;

- unique privileges must be assigned to a different user ID than the one used in the normal user experience.

Control and periodic review of user access rights to the information resources of the company is carried out in the process of auditing information security in accordance with the information security audit rules and established procedures.

9.2. Password Management.

Passwords allow a company to verify the identity of the user to access the information system or service. Passwords provide identification and authentication based on information known only to the user.

The provision of passwords should be controlled through a formal procedure that meets the following requirements:

- all users should be acquainted with the requirement to keep personal and group passwords secret;

- it is necessary to configure the system in such a way that when a user first logs in with a temporary, assigned password to him or her then the system immediately requires changing it;

- temporary passwords should be assigned to a user only after the user is identified.

- it is necessary to avoid the transmission of passwords using third parties or unencrypted email;

- temporary passwords should not be guessable and repeated from user to user

- the user must acknowledge receipt of the password

- passwords should be stored electronically only in a secure form

- passwords assigned by the software manufacturer should be changed immediately after the installation is complete

Requirements for password length: user's password are changed at least once every 90 days. If necessary, the company can consider the possibility of using other technologies for identifying and authenticating users.

9.3. Access Control

To ensure effective access control, it is necessary to introduce a formal process for regularly checking the access rights of users, which meets the following requirements:

- user access rights should be checked at regular intervals (at least once every six months), as well as after making any changes to the information system;

- the access rights of users should be checked and reassigned when changing happened in their job duties in the company, as well as when moving from one job to another within the organisation;

- verification of the rights of users who have special privileges for access to the system should be carried out more often (at least once every 3 months);

- it is necessary to regularly check the adequacy of the assigned privileges, in order to avoid any of the users receiving excessive rights;

- changes to privileged accounts must be logged.

Control over the implementation of user access control procedures should include:

- control over the addition, deletion and modification of identifiers, authentication data and other identification objects;

- authenticate users before changing passwords.

- immediate blocking of access rights upon dismissal;

- blocking accounts that are inactive for more than 40 days;

- enabling accounts used by vendors for remote support only for the duration of the work;

- tracking of deleted accounts used by suppliers during work;

- prevent the reuse of the user ID and/or device for at least three years;

- familiarisation with the rules and procedures for authentication of all users who have access to restricted information;

- use authentication mechanisms when accessing any database containing restricted information, including access by applications, administrators and any other users;

- allow queries and direct database access only for database administrators.

- blocking the account for a period equal to 30 minutes or until the account is unlocked by the administrator;

- blocking of user accounts when the results of monitoring (viewing, analysis) of logs of registration of security events of user actions that are attributed by the operator to information security violation events are detected.

9.4. Remote Access.

All remote access connections to the networks of the company will be through the approved remote access methods with data encryption and multi-factor authentication.

Remote users may only connect to the organisation networks when officially approved by the applicant's supervisor or management.

The ability to remotely print or copy confidential information must be disabled.

Users granted remote access privileges must be given remote access instructions and responsibilities.

Remote access to information resources has to be logged.

Remote sessions must be terminated after a specified period of inactivity.

Secure connection to another private network is prohibited while connected to the (organisation network unless approved in advance by IT management.

Non-organization computer systems requiring network connection must comply with all applicable company IT standards and may not be connected without prior written approval from IT management.

9.4. Using Passwords

The user ID and password in the information system are the credentials on the basis of which an employee of the company is granted access rights, the actions performed by him or her in the system are recorded and the confidentiality regime of the information processed (created, transmitted and stored) by the employee is ensured.

It is not allowed for different users to use the same credentials.

The initial password value of the user account is set by the security administrator.

Personal passwords are set for the first time by employees of the information system department.

After the first login to the system and in the future, passwords are selected by users of the automated system themselves, taking into account the following requirements:

- password length must be at least 8 characters;

- password characters must include three of the four types of characters: uppercase letters, lowercase letters , digits; special characters (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);

- the password should not contain easily calculated combinations of characters, for example, first names, last names, phone numbers, dates; sequential characters on the keyboard ("12345678", "QWERTY", etc.); generally accepted abbreviations ("USER", "TEST", etc.); a casually used word, for example, the names or surnames of friends, colleagues, actors or fairy-tale characters, animal names; computer term, command, name of companies, web sites, hardware or software; any of the above in reverse spelling; any of the above with the addition of numbers at the beginning or end;

- when changing the password, the value of the new one should differ from the previous one in at least 4 positions;

- different information systems need to set their own, different passwords.

An employee is prohibited from:

- share a password with someone else,

- specify a password in e-mail messages,

- store passwords written on paper in an easily accessible place.

- use the same password as for other systems (for example, home Internet provider, free email, forums, etc.),

- use the same password to access different corporate information systems. The user should not log on automatically. Leaving the workplace, the user is obliged to lock the computer (using the combinns Win + "L" or Ctrl + Alt + Delete → "Lock computer").

The employee is obliged to:

- In case of suspicion that the password has become known to someone, change the password and report the fact of compromise to an authorised employee of the information system department,

- Immediately inform the IP officer if asked for a password,

- Change your password every 90 days,

- Change the password at the request of the Information Security Administrator. After 3 unsuccessful attempts to enter the password, the account is blocked for 30 minutes. If the account is systematically blocked by the employee (more than 3 times), the information security administrator is notified.

The company reserves the right to:

- periodically check the validity of user passwords which are used by employees to access the information system;

- take disciplinary action against staff members who violate the provisions of this policy.

9.5. User equipment

Users must provide the necessary protection for unattended equipment. All users should be aware of the information security requirements and the rules for the protection of unattended equipment, as well as their responsibilities to ensure this protection.

9.6. A Clean Desk Policy (CDP)

CDP is a corporate requirement that defines how employees should leave their workplace when they leave the office.

Employees of the company are required to:

- Keep passwords a secret.

- Close active sessions when they are finished.

- At the end of the session, log out of the system at universal computers, servers and office PCs.

It is forbidden to record passwords, for example, on paper, in a program file or in a handheld device.

Documents and media with confidential information should be removed to lockable places (safes, cabinets, etc.), especially when leaving the workplace.

Computers and terminals should be left in a completed logoff state when they are unattended. The user should not log on automatically.

Leaving the workplace, the user is obliged to lock the computer (using the combinations Win + "L" or Ctrl + Alt + Delete → "Lock computer").

Documents containing confidential information should be removed from printing devices immediately. At the end of the working day, employees tidy up their desks in order and put all office documents in a lockable cabinet or safe. For the disposal of confidential documents, paper shredders should be used. At the end of the working day and in case of a long absence from the workplace, it is necessary to lock all cabinets and safes.

9.7. Mobile computer equipment.

When using mobile devices (laptops, tablets and mobile phones), special precautions must be taken to prevent the compromise of information belonging to the company. It is necessary to adopt an official policy that takes into account the risk associated with the use of mobile computers and in particular with work in an unprotected environment.

10. Cryptography

All cryptographic information protection facilities (CIPF) have to be taken into account in the relevant journal of accounting of the CIPF.

The organisation has to manage keys for the effective application of cryptographic methods.

Compromise or loss of cryptographic keys may lead to a violation of the confidentiality, authenticity and / or integrity of information. All keys must be protected from alteration, loss and destruction. In addition, private and secret keys must be protected from unauthorised disclosure. The equipment used to generate, store and archive keys must be physically protected.

Cryptographic systems and techniques should be used to protect sensitive information when other controls do not provide adequate protection. For critical information, encryption should be used when it is stored in databases or transmitted over commercial or open networks, such as the Internet. Encryption of any other information in the information system of the Institution should be carried out only after obtaining written permission to do it.

10.1. Requirements for ensuring information security when using cryptographic protection systems.

Encryption is a cryptographic method that can be used to ensure the protection of sensitive, confidential or critical information. Cryptographic protection systems should be supplied by

developers with a full set of operational documentation, including a description of the key system, the rules for working with it and the justification of the necessary organisational and staff support.

The procedure for the application of the CIPF is determined by the management of the company and should include:

- implementation procedures, including procedures for embedding cryptographic protection systems in the information system;

- operating procedures;

- the procedure for restoring operability in emergency cases;

- how changes are made;

- decommissioning procedure;

- how key information is managed;

- how key information is handled, including actions when keys are changed and compromised.

To encrypt sensitive information, the minimum allowable key length is 128 bits.

When using encryption in an information system, the organisation should use only approved standard algorithms.

10.2 Electronic digital signatures (EDS).

EDS provides protection of authentication and integrity of electronic documents. EDS can be used for any form of document processed electronically. EDS should be implemented using a cryptographic method based on a uniquely related key pair, where one key is used to create a signature (secret/private key) and the other is used to verify the signature (public key).

It is necessary to ensure with special care the confidentiality of the private key, which should be kept secret, since anyone who has access to it can sign documents (payments, contracts), thereby falsifying the signature of the owner of the key. Public key integrity must be protected when using a public key certificate. The cryptographic keys used for digital signatures must be different from those used for encryption.

10.3 Key management.

Any compromise or loss of cryptographic keys may result in compromise of the confidentiality, authenticity, and/or integrity of the information.

A security system should be applied to ensure that the companies' information system uses cryptographic methods with respect to public keys, where each user has a key pair, a public key (which can be shown to anyone) and a private key (which must be kept secret).

Public key methods should be used for encryption and for generating digital signatures.

Keys must be protected from alteration and destruction, and secret and private keys must be protected from unauthorised disclosure.

Cryptographic techniques can also be used for this purpose. Physical security should be used to protect the equipment used to make, store and archive keys.

Users' private keys should be stored in the same way as passwords. Any suspicion of compromise of the private key should be reported immediately to the information system department.

It is necessary that the key usage security system is based on the harmonisation of methods, procedures and secure methods for:

- key generation when using various cryptographic systems and applications;

- generation and receipt of public key certificates;

- distribution of keys intended for users, including instructions on how to activate them upon receipt;

- key storage (this requires instructions to authorised users to gain access to the keys);

- key rollover or renewal, including key rollover procedures and deadlines;

- how to proceed with compromised keys;

- key revocation, including how keys are revoked or deactivated if the keys have been compromised or the user has left the organisation (in which case the keys must be archived).

- recovery of keys that have been lost or corrupted to declassify encrypted information;

- archiving and backing up keys;

- destruction of keys;

- key registration and auditing of key management activities.

To reduce the likelihood of compromise, the keys should be subject to the start and end dates of the action. Therefore, they can only be used for a limited period of time, depending on the circumstances of the use of cryptographic tools, control and the degree of risk of disclosure.

It is necessary to protect public keys from the threats of forgery of a digital signature and replacement of the user's public key with their own. This issue is solved by using a public key certificate. Certificates must be produced in a way that uniquely links information relating to the owner of the open/secret pair.

11. Physical and environmental security

To comply with the security guidelines, the company Loco News should take in consideration a better security control regarding the physical placement of their assets and how they are protected. This

includes where the assets are located, who has access to them, how they are protected and who oversees their protection.

For an easier reading, the assets have been divided into two categories: servers and computers.

11.1 Assets location

Servers

The Company's servers are in a basement space shared with a neighbouring company. Loco News should consider moving the location of the server room to an enclosed space that cannot be accessed from external parties.

The following points should be followed regarding the location of the servers:

- a defined space which is not used for any other purposes,
- the door(s) that give access to the room should be alarmed fire doors,
- the room should be sturdy with windows equipped with lock,
- the room itself should be lockable,
- the access to the room should be placed in an area viewable from multiple perspectives.

The servers should also be placed in an environment where they can receive adequate cooling.

Computers

The Company has both laptops and desktops. Particular attention is needed for the location of desktops inside the office. Computers should be placed in an environment where they cannot be accessed from third parties and are protected from eventual accidents (see 7.3). Security priority should be in any case given to the servers.

11.2 Individual access to the assets

Servers

Entry to the server room should be always regulated and controlled. Only authorised personnel who are directly in charge of server maintenance and control should be granted access to the room, to ensure that assets will not be compromised by untrusted individuals (employees of the Company or external party). Access key should be in the form of an electronic card that can easily record the time of access and the original owner of the key. These access records should be stored in a log which is immediately identifiable and accessible, so that it cannot be confused with other logs or documents.

Computers

Physical access to the computers should only be granted to employees inside the office space. For further regulations concerning access, see Access control.

11.3 Assets protection

More specific protection should be required to ensure the correct functioning of Loco News' assets.

The Company's environments are protected by an alarm system which follows local regulations. The alarm system should be periodically tested and checked by authorised individuals to ensure that it is up to date with the local regulations.

The Company should also install security cameras where the important assets are located.

When dealing with sensitive information, the Company should consider not allowing the use of personal devices inside the building and keep the employees from using the laptops outside the Company.

Servers

A dedicated policy should be created regarding the protection of the server room. In particular:

- no food or drinks should be allowed inside,
- no smoking inside the server room and ideally no smoking on the entire floor,
- temperature and humidity of the room should be checked periodically and should always be constant,
- the room should contain the servers, nothing else,
- power cables should be adequately protected, particular attention should be dedicated to checking eventual water infiltrations.

11.4 Assets protection control

To speed up and facilitate the guidelines shown in the previous points, a dedicated individual should be appointed to oversee the security system of the building.

This individual should be a trusted employee of the company (newly hired or already employed) with the necessary knowledge regarding physical security. The task of this employee should be to keep logs of access to the sensitive spaces of the Company, to keep logs of visitors, to keep logs of deliveries, to check the alarm system of the building, to check the security camera system.

12. Operation security

Control regarding correct operations of information is necessary for Loco News. This section of the policy will illustrate the actions that need to be taken to ensure security concerning this aspect.

Like it was illustrated in point 7.4, an individual should be appointed to be in charge of overseeing the operation security. In particular, this individual should be responsible for:

- keeping a log of all operations,
- controlling any changes regarding management,
- checking whether the environments are ideal for a certain operation.

Further information regarding each point will be illustrated in this section.

12.1.1 Operations log

A log of all the operations should be kept in digital form and with one or more backups.

This log should be accessible with the right credentials by any employee that would wish to do so, excluding confidential operations.

The operations inside the log should be correctly divided into categories, in order to easily access the information inside it.

The content of the log should include:

- the installation and configuration of systems,
- access to computers,
- backup times and dates,
- system errors and failures,
- log of external technical support operations,
- monitoring of procedures.

An accurate record of operations is vital to ensure a quick way to find the source of an error and solutions to contrast malfunctioning.

12.1.2 Control of changes in management

Changes in management include:

- changes to the organisation,
- business processes,
- information processing facilities and systems.

In particular, the individual in charge of operation security should be allowed to control and record any changes concerning the three points listed above. This includes:

- controlling and testing the impact of this changes to the security,
- approving the changes,
- communicating the changes to the involved personnel,
- planning a way to recover from these changes in case of unforeseen events,
- controlling the changes concerning capacity.

Further information can be given regarding the last point listed above.

The individual in charge of operation security should be allowed to control the changes and usage of capacity of resources. This includes the capacity of devices, which need constant control to ensure that enough space is available in case of emergency.

Capacity can be acquired by:

- deleting obsolete data,
- removing unnecessary applications or programs,
- optimising batch processes and schedules,
- optimising application logic or database queries,
- denying or restricting bandwidth for resource-hungry services if these are not business critical.

12.1.3 Secure environment

It is important for the operations to be successful to have the correct environment.

The individual assigned to operation security management should check the security of these environments.

To reduce the risk of unauthorised access from third parties and unwanted accidents, the environments should be divided according to their purpose in development, testing and operational environments.

The transfer of assets from one environment to another should be recorded in a log, unless previously authorised.

12.2 Protection unwanted activities

In an online environment like the one used by the company Loco News, it is important to keep in mind that menaces such as malwares could negatively affect the operations of the company.

Private information kept by the Company can become a target of hackers, it is then important to have a plan that allows prevention, detection, and recovery from these attacks.

Prevention and recovery in particular can be done via backups. It is recommended to Loco News to make a backup of the used information.

When making a backup it is important to consider the following points:

- a backup should be frequently updated,
- it should be stored far from where the original data is stored,
- multiple backup copies are recommended,
- every change to the backups should be recorded in a log,
- restoration of the backup data should be tested.

It is also necessary to have a dedicated policy regarding malware protection to follow when dealing with sensitive data. In particular:

- controls should be implemented to detect unauthorised applications,
- implement a way of detecting suspicious websites,
- reduce technical vulnerabilities that could be exploited by malwares,
- use antiviruses and updating them regularly,
- train the employees on the danger of malwares and the ways they operate,
- have a set of operations to do in case of loss of data caused by malwares.

12.3 Access logs

An additional log the Company should consider implementing is a log of all the accesses.

To make the log effective as much detailed information as possible should be included in the records.

This includes things such as:

- ID,
- date, time of access,
- level of authority,
- time spent on operation.

Due to the highly sensitive nature of these details, the log should be accessible only via authorisation. Any modification to the logs should be possible only by those previously authorised and these modifications should also be recorded.

13. Communications security

The company lacks measures that protect the network used to work. Regulations are necessary to illustrate the security process that defends the communications and ensures that the information is delivered to the right individual and is not compromised in the process.

The communication security process can be divided into sections, which will be explained below.

13.1 Network security

Loco News employees work mainly using the computers provided by the Company and exchange data via a network system. Clear regulations should be established regarding the management of the network. This includes who has access to the network, what can access the network and what is accessible from the network. Failure to identify these regulations can result in third parties violating the access and stealing sensitive information from the Company.

The network should also be divided in domains which require different authorisations to access.

This allows better control over the operations that make use of the same network.

13.2 Information transfer

When transferring information, it is vital to keep it uncompromised and to have it delivered to the right individual. The information can also be in physical form or travel via a network. A policy that regulates information transfer is necessary for Loco News.

The following actions should be considered:

- control how and when copy machines are used,
- control if data was modified or copied,
- use cryptography to protect the data,
- adequately train the employees regarding the importance of keeping information private,
- paying particular attention to who has access to a certain kind of information.

14. System acquisition, development and maintenance

14.1 Security requirements of information systems.

Information security related requirements should be incorporated into any requirements for new information systems or enhancements to existing information systems.

Information security needs should be determined using a variety of approaches, such as defining policy and regulatory compliance criteria, threat analysis, incident assessment, and the use of vulnerability thresholds. Security requirements should be documented and agreed upon so that they can be referenced when purchasing or developing a solution. It is not recommended to select or develop a solution and then evaluate the level of security capabilities. This often results in higher risks and costs, and can also cause problems in applicable legislation such as the GDPR, which encourages security philosophies and practises such as the Data Protection Impact on Privacy Assessment (DPIA).
When developing any new system or modifying existing systems, it is important to understand what the business requirements for security controls are by performing a risk assessment. This should be done before a solution is selected or developed. Security considerations should be taken into account at the earliest opportunity to ensure that the correct requirements are identified before a decision is made.
Special attention is required to who has access to the information stored in the application database, in other words, to the security of the information.
To ensure that established safety criteria are met, product acceptance criteria, such as functionality criteria, need to be defined. These criteria should be considered before purchasing a product. Additional functionality should be reviewed to ensure that there are no unacceptable risks.

14.2 Security in development and support processes.

Whenever possible, separating development, testing, and operations is important to separate the roles involved. The rules for moving software from a development state to a working state should be defined and documented.
The level of separation required to prevent operational problems between the production environment, test environment, and development environment must be considered to ensure that the production environment is adequately protected.
Information security considerations for application services transmitted over public networks should include the following:
a) the level of confidence each party requires in each other's claimed identity, e.g. through authentication. Usernames and passwords must be provided instead of user-generated ones to ensure account security. In the case of this company, it may be useful to consider IP access in addition to other methods, since employees can easily access information from outside using their laptops. Access must also be granted for a limited time and must expire after inactivity.
b) authorization processes associated with who may approve contents of, issue or sign key transactional documents;
c) ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;
d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;
e) the level of trust required in the integrity of key documents;
f) the protection requirements of any confidential information;
g) the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;
h) the degree of verification appropriate to verify payment information supplied by a customer;

i) selecting the most appropriate settlement form of payment to guard against fraud;
j) the level of protection required to maintain the confidentiality and integrity of order information;
k) avoidance of loss or duplication of transaction information;
l) liability associated with any fraudulent transactions;
m) insurance requirements.

Unverified or malicious code can cause serious operational problems. Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities can lead to unintended changes to software and information if they use the same computing environment. Separate development, test, and operational tools to reduce the risk of accidental modification or unauthorised access to operational software and business data.

14.3 Test data.

Test data must be carefully selected, protected and controlled. Test data should ideally be created in a generic form that is not related to actual system data. However, it is recognized that it is often necessary to use real-time data to conduct accurate testing. Where live data is used for testing, this should be; Maximum anonymous; Carefully selected and fixed for the testing period; Securely removed after testing is complete. The use of operational data must be pre-authorized, recorded and controlled. The auditor expects to see robust procedures for protecting data used in test environments, especially if it is all or part of live data.

15. Supplier Relationships

The purpose of supply relationship policy is to guarantee the assurance of Loco news resources that are available by suppliers and keep a concurred degree of data security and administration conveyance by supplier arrangements.

The association ought to recognize and command data security controls to explicitly address Supplier admittance to the association's data in the approach. These controls should address cycles and methodology to be executed by the association, just as those cycles and strategies that the association ought to require the provider to carry out, including:

- recognizing and recording the kinds of suppliers, for example, IT administrations, strategies utilities, financial administrations, IT framework parts, whom the association will permit to get to its data;

- a normalised interaction and lifecycle for overseeing supplier connections;

- characterising the sorts of data access that various kinds of suppliers will be permitted, and observing and controlling the access;

- least data security necessities for each kind of data and sort of admittance to fill in as the reason for individual supplier arrangements in light of the association's business needs and prerequisites and its danger profile;

- cycles and methodology for checking adherence to set up data security prerequisites for each kind of supplier and sort of access, including third-party and item approval;

- precision and entirety control to guarantee the uprightness of the data or data handling given by one or the other party;

- kinds of commitments relevant to suppliers to secure the association's data;

- taking care of occurrences and possibilities related to supplier access including liabilities of both the association and suppliers;

- versatility and, if vital, recuperation and possibility game plans to guarantee the accessibility of the data or data handling given by one or the other party;

- mindfulness preparing for the association's faculty engaged with acquisitions in regards to pertinent approaches, cycles, and methodology;

- conditions under which data security necessities and controls will be reported in an arrangement endorsed by both parties.

Suppliers will not have access to Loco's information unless the following conditions are met:

- Justifications have been supplied in the right format.

- It was authorised by management.

- The proper security controls have been carried out.

- A contract has been signed, specifying the terms and conditions, when applicable.

16. Information security aspects of business continuity management

The main objective of information security continuity is that it should be embedded in the organisation's business continuity management systems. The association ought to decide its necessities for data security and the continuity of data security management in adverse circumstances. An association ought to decide if the continuity of data security is caught inside the business continuity management process or inside the disaster recovery management process. Data security necessities ought to be resolved when making arrangements for business continuity and disaster recovery. The association ought to set up, report, execute and keep up with the process strategies, and controls to guarantee the necessary degree of continuity for data security during an unfriendly circumstance. An organisation should ensure that:

- A sufficient management structure is set up to get ready for, moderate, and react to a problematic occasion utilising a workforce with the essential power, insight, and skill.

- Recorded plans, reaction, and recovery systems are created and supported, enumerating how the association will deal with a troublesome occasion and will keep up with its data security to a foreordained level, in view of management-endorsed data security continuity targets.

- Incident reaction workforce with the essential obligation, authority, and capability to make due to an occurrence and keep up with data security is assigned.

- The information security continuity requires the organisation to establish data security controls inside business continuity or disaster recovery processes, methodology furthermore supporting frameworks and gadgets.

- It should implement and document the processes, strategies, and execution changes to keep up with existing data security controls during an unfriendly circumstance.

- The organisation should maintain controls for data security controls that can't be kept up with during an adverse circumstance.

- The organisation should include data security experts while building up, executing, and keeping up with business continuity or disaster recovery cycles and techniques.

The information security management must also be verified by the association through the following steps:

- Practising and testing the usefulness of data security continuity processes, methods also controls to guarantee that they are reliable with the data security continuity objectives.

- Surveying the legitimacy and adequacy of data security continuity estimates when data frameworks, data security processes, methodology, and controls or business continuity management/disaster recovery management processes and arrangements change.

- Practising and testing the information and routine to work data security continuity processes, systems, and controls to guarantee that their presentation is predictable with the data security continuity objectives.

17. Information security incident management

The aim of information security incident management is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. The executive's obligations and strategies ought to be set up to guarantee a speedy, powerful, and precise reaction to data security occurrences. The objectives for information security incident management ought to have concurred with management, and it ought to be guaranteed that those answerable for information security incident management comprehend the association's needs for taking care of information security incidents. The following procedures should be developed within the organisation:

- Methodology for incident reaction planning and arrangement and methodology for checking, recognizing, investigating, and announcing information security occasions furthermore incidents.

- Systems for logging incident management exercises and systems for treatment of legal proof.

- Systems for reaction including those for heightening, controlled recovery from an incident, what's more correspondence to inner and outer individuals or associations.

Information security occasions ought to be reported through fitting management channels as

rapidly as could really be expected. All representatives and project workers ought to be made mindful of their obligation to report information security occasions as fast as could really be expected. They ought to likewise know about the methodology for detailing information security occasions and the resource to which the occasions ought to be reported. The information security event must always be reported when:

1. access violations
2. human errors
3. uncontrolled system changes
4. malfunctions of software or hardware
5. non-compliance with policies or guidelines

Breakdowns or other system errors might be a mark of a security assault or real security break and ought to consequently forever be accounted for as an information security event. The response for information security incident must be following:

1. Guarantee that all elaborate reaction exercises are appropriately logged for later examination.
2. When the incident has been effectively managed, officially shut and record it.
3. The primary objective of incident reaction is to continue normal security level and afterward start the vital recovery.
4. Gather proof as quickly as possible after the event.
5. Communicating the presence of the information security incident or any significant details thereof to other inward and outer individuals or associations with a need-to-know.

18. Compliance

18.1 Compliance with legal and contractual requirements.

All relevant legal, regulatory, contractual requirements regarding ***intellectual property rights*** and the use of proprietary software products, ***protection of records***, destruction, tampering, unauthorised access and unauthorised release, ***privacy and protection of personally identifiable information***, conducting an information campaign with staff and stakeholders to ensure an ongoing understanding of the individual's responsibility to protect confidentiality, the identifiable ***cryptographic controls*** and their use, the implementation of a monitoring and awareness program to ensure that the requirements are met and the organisation's approach to meeting those requirements should be clearly defined, documented and maintained for each information system and organisation.

18.2 Information security reviews.

Information systems should be regularly reviewed for compliance with the organisation's information security policies and standards. Automated tools are commonly used to validate systems and networks against technical requirements and must be identified and implemented as needed. When tools such as these are used, they should be limited to as few authorised personnel as possible, and their use should be carefully monitored and coordinated to prevent compromising the availability and integrity of the system. The organisation’s information security arrangements should be independently reviewed (audited) and reported to management. Managers should also routinely review employees’

and systems' compliance with security policies, procedures etc. and initiate corrective actions where necessary.

References:

1. International Organisation for Standardisation (ISO) 2013, *Information technology — Security techniques — Code of practice for information security controls*, ISO/IEC 27002:2013(E), Switzerland.