Group E
Melat Getachew, Philomina Ejegi Ede, Gowthami Rapalli, Henok Rezene

Loco News Information Security Policy

Table of Contents

1. Objectives

The policy aims to describe the measures to be taken for maintaining confidentiality of information while ensuring information access for authorized persons and maintaining integrity of information. In this regard, the policy covers areas of human resource security, asset management, access control, cryptographic controls, physical and environmental security, operations security, communication security, system acquisition and development, security in supplier relationships, incident management and continuity of information security. The policy also focuses on effective communication of laid out policies to employees and other relevant parties and outlines the necessity of developing, reviewing, and evaluating the effectiveness of policy at regular intervals.

1.1. Organization of information security

A well-organized hierarchical structure in implementing information security protocols is necessary. In this regard, the responsibilities for individuals should be precisely defined and allocated, and the allocated responsibilities and authorization levels must be well documented. To reduce the risk of accidental or deliberate misuse of organizational assets, conflicting duties should be segregated. Specifically, duties related to initiation and authorization of an event must be well seperated.

1.2. Human resource security

Security issues related to human resource management constitute the prime focus of any organization. During the recruitment of employees, a transparant process for screening the applicants seeking employment is essential. The process must involve rigorous background verification checks of candidates seeking employment through character references at the professional and personal level, verification for accuracy of the information in person's curriculum vitae, confirmation of academic and professional qualifications, identity checks and verifying credit score and criminal records of individuals.It is important that the screening process should be well-informed to all the candidates through employment advertisements. Information received during the screening process should be handled based on appropriate legislation in place. The employment contract should contain a non disclosure agreement (NDA) related to information security that must be signed by employees before obtaining access to information. Information security awareness programmes should be organized to educate employees and contractors about their roles and responsibilities for the information security branch is essential. When an employee resigns or is terminated by the company, the ongoing information security requirements should be clearly communicated to employees as a part of the termination responsibilities and the employee should be asked to sign a new NDA associated with termination.

2. Asset Management and Access control

Organization assets should be identified, classified and well protected. The assets can be broadly classified as current assets, fixed assets, and intangible assets. Current assets are cash or cash equivalents such as deposit accounts, money orders, bank cheques, inventory,stocks that can be converted into cash within a year or so. Fixed assets are long-term assets such as property, buildings, plants, equipment, tools, furniture, hardware devices, machinery, and long-term investments. Intangible assets constitute software licenses, intellectual property, patents, copyright, franchises, and brand name. Awareness programs must be conducted for employees and external party users to train them in responsibilities associated with information security in asset management. Outdated or unused assets can be handled by having a digital database that includes information such as the root cause of datedness, personal responsible for management of the asset, and planned schedule to identify the reusability of these assets. In handling of removable media, information about allowed devices, data that can copied to allowed devices, locations from where data can be copied must be clearly specified to employees. Removable media must be encrypted, and file transfers must be audited. To mitigate risks associated with malware propagation, antivirus controls must be mandated. Alternatively, cloud-based file transfer services such as Dropbox or Google Drive can be considered for secure transfer services such as Dropbox or Google Drive can be considered for secure transfer of information after appropriate assessment of related risks.

Access control is the most critical component in information security of any organization. Access control can be categorized into physical access to office spaces, tools and equipment, and virtual access to data, information, and software. In the case of physical access, access cards or biometric control should be mandated. Separate mechanisms or temporary access cards must be inplace to manage visitor access to manage spaces. The first step in access control must be identifying people responsible for granting access controls. Second, a well-defined role-based access control model [1] must be developed that should take into consideration the segregation of responsibilities and the principle of least privilege[2]. The information access must be regulated through two-way authentication involving a password and a temporary secure access key. Third, the type of access, reason for access and duration of access must be properly documented. Finally, access control based on discretion of management should be avoided as much as possible.

3. Operations security

The company's operations security should be upgraded to meet the ISO 27002 standard. To reach this standard, seven categories and 14 controls needed to be implemented.

3.1 Operational procedures and responsibilities

This is the first category of the operation security. The purpose of this category is to ensure that information processing and related facilities are operated safely. This safety can be achieved by ensuring and running four controls.

3.1.1 Documented operating procedures

This is the first control, and its purpose is to ensure all operating procedures are documented and made available to all users who need them. Moreover, implementation guidance for the documented procedures associated with information processing, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling and safety should be prepared for the operational activities.

3.1.2 Change management

Any change to the organization, business processes, information processing facilities and systems that affect information security should be controlled. To achieve this the company should implement several implementation guidelines. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained. Significant changes should be recorded and identified. The company needs to emphasize on this control because Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Any changes to the environmental environment are often a security problem which affects the reliability of certain applications and should be made with caution.

3.1.3. Capacity management

This third control should be implemented, as it helps the organization to manage its current and future resources to ensure its performance is as planned and required. For the organization to maintain and improve its information processing efficiency and performance capabilities it should ensure that its resources, especially those serving critical business operations, are sufficient and capable of handling extra requirements that might arise. One of the most important aspects of capacity management is the ability to scale. The organization should be able to predict what their performance requirements are going to be and act upon this analysis an organization should not be driven reactively and by resources once needed rather that it should plan ahead. This analysis needs to take several factors into consideration. Business units should be involved and consulted to understand what their future expectations and requirements are.

The procurement process and product availability should be calculated. The current performance levels should be constantly monitored analyzing trends of usage in practice and improving current capacity levels. Disk space could be saved by deleting obsolete data decommissioning unutilized systems optimizing bandwidth usage and relocating resources to serve more critical activities. A capacity management plan should be maintained and constantly reviewed and updated.

3.1.4. Separation of development, testing and operational environments

The organization should separate its development and testing environment from its operational environment to prevent fatal consequences. This control ensures this does not happen. There are two main risks that an organization would face if it does not separate its landscape. The first risk is related to authorization where personnel who have access to the development environment should not be doing changes or have privileges to the operational environment. The second risk is related to the successful deployment of new solutions, changes and practices. Before deploying directly to the operational environment, a solution has to be properly developed and tested in environments where errors and problems would not cause a direct damage to the organization and would allow an opportunity to fix them before deploying in the operational environment. The transfer of solutions from the development to the testing and eventually to the operational environment should be regulated, authorized, documented, and monitored. The solutions should be developed and tested taking into account all the information systems that are available and used in the operational environments.

3.2. Protection from malware

Protection from malware is the second category of Operation Security and its objective is to ensure that information and information processing facilities are protected against malware. It has only one control called Controls Against Malware. This is a big threat, and the organization must secure its operations by implementing a number of procedures.

3.2.1 Controls against malware

Detection, prevention, and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The organization should make its users aware of the risks of malware and how to avoid them. A formal policy should be established and published that addresses proper internet and technology usage in general and for business purposes in particular to ensure that employees know their responsibilities. Users should not be allowed to install and download software on their own.

3.3 Backup

Backup is the third category of the operations security with the main purpose of protecting information from being completely lost. It has only one control.

3.3.1 Information backup

Information backup, states that a backup and recovery process should be in place and constantly tested. Information and related systems are prone to accidental or deliberate damage and corruption. One of the best ways to guarantee that critical information would not be lost forever is to have another intact copy of it which provides redundancy as long as the backup is secure. To meet this, the organization should establish backup policy and procedures which takes the business requirements and the information classification scheme into consideration. It should define the backup plan, the frequency, the retention period, and the security measurements of the data. To support this policy, adequate technologies and equipment should be in place and constantly maintained. To properly operate this equipment, trained and skilled staff should be available to ensure a successful backup process. The restoration and recovery of data is as important as taking the backup. The organization should test the backup to minimize the risk. An important part of the information or system may be lost due to natural or human hazards. So, it is necessary to have a copy of the data in order not to lose critical information forever. The organization should have a backup policy and procedures to maintain information security.

3.4 Logging and monitoring

Logging and Monitoring is the fourth category of operations security and its objective is to record events and generate evidence. It has four controls which are listed below.

3.4.1 Event logging

The first control is called Event Logging. This controls event logs recording user activities, exceptions, faults, and information. Security events should be produced, kept, and regularly reviewed.

3.4.2. Protection of log information

The second control is called Protection of log information which protects logging facilities and log information against tampering and unauthorized access.

3.4.3 Administrator and operator logs

The third control is called administrator and operator logs. As administrators have additional access system administrators and system operator activities should be logged and the logs

protected and regularly reviewed. Clock synchronization is the fourth category which states that information systems should be synchronized to a single time source.

Control of operational software is the fifth category, and its objective is to control the integrity of operational systems by controlling what gets installed on them. It has one control called installation of software on operational systems. Installation, updating and changing of any software on the operational system should be authorized by management and performed only by authorized and skilled administrators.

The sixth category of the operation security is called technical vulnerability management and its objective is to avoid vulnerability being exploited by attackers. management of the two controls under this category are management of technical vulnerabilities and restriction of software installation.

3.4.4 Clock synchronization

Events and logs lose a great deal of their importance if they can not be pinned to specific times. So, this control states that this information system should be synchronized to a single time source. Synchronization and accuracy of the time of logs are dictated by business requirements for example to ensure that a backup has been taken on a specific time. They are also dictated by legal and regular requirements for example for investigation and auditing purposes. The organization's syncing and information's systems should be properly configured and documented. Using a network time protocol server which all information systems can sync with is a normal practice. This server then syncs with external NTP servers to maintain an accurate time. Clock synchronization is also important for tracking security logs and correlating between events which gives security operating center personnel a better idea of the timestamps of an attack and how long each stage of an attack took inside the organization.

3.5 Control of operational software

This category helps the organization to protect the integrity of the operational systems by controlling what gets installed on them. It has only one control, installation of software on operational systems.

3.5.1 installation of software on operational systems

Installation, updating and changing of any software on operational systems should be authorized by management and performed only by authorized and skilled administrators. The software to be allowed include software that is being developed which should not move to the operational environment before going through sufficient development and testing. A configuration management process should be in place to control how changes are planned, tested, and applied.

All changes should be documented, and rollback strategy should be developed so that unsuccessful changes can be discarded, and the initial state can be restored.

3.6 Technical vulnerability management

The objective of this category is to avoid vulnerabilities being exploited by attackers. So, the organization should be equipped with a proper technique to manage vulnerabilities. To do this, it should implement the following two controls:

3.6.1 Management of technical vulnerabilities

The organizations should try to identify its information systems vulnerabilities proactively and before they have been exploited and used to cause damage to the organization. These vulnerabilities should be assessed and then treated to eliminate their effects. A prerequisite to a good vulnerability management process is knowing what the organization's assets specifically are, how they are operated, and the security measures already in place to protect them. Additional to this a risk management should be in place which helps in prioritizing what vulnerabilities the organization should deal first. A timeline should be defined to deal with the criticality of the vulnerability.

3.6.2 Restriction on software installation

The organization should control what software its employees are allowed to install on their information systems. Allowing an employee to install any software that he wants on his systems might represent a real risk. The reason is that employees might not have the security skills to assess the software or to properly configure it. The organization should restrict employees from installing personal software that could be malicious or that affect their business productivity. Only authorized personnel should have the privilege rights to install software on a system.

3.7 Information systems audit consideration

This is the last category, and its goal is to help the organization to plan and perform audit activities in a manner that does not have an effect on operational environments. This category has only one control called information systems audit controls.

3.7.1 Information systems audit controls

Audit activities are important to verify information and systems integrity but performing them should not disrupt operations or affect its performance. Prior to performing any audit activities, the approval of the relevant management should be obtained having been provided with plan time and scope of the audit activities. Access to the information systems should be limited to

reviewing information and systems logs. If it is necessary, audit activities should be taken place outside the business hours to minimize its effect on the operational environment.

4. Communications security

The organization's daily communication should take place in a secure way. Therefore the organization should ensure a proper communication security is implemented. Communications security has two categories which in turn each category has a number of controls.

4.1 Network security management

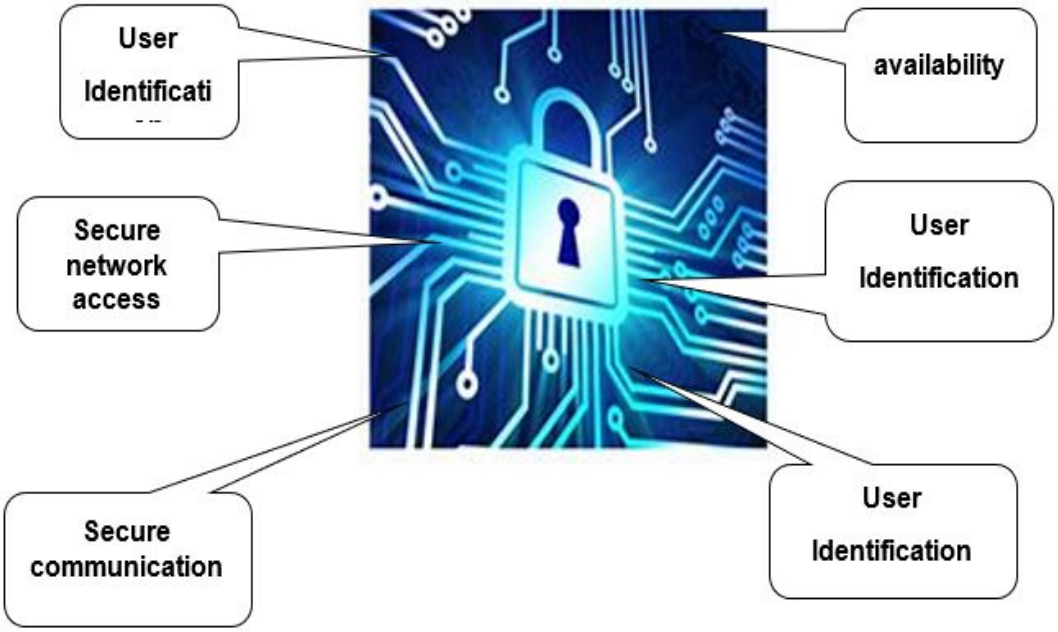
This Is she first category with the goal to ensure the security of information and networks. This category has three controls.

4.1.1. Network control

Network security occupies a major portion of a technical information domain. It involves protecting the perimeter of an organization's infrastructure as well as the internal network connecting the information systems. Rolls and responsibilities of network management should be defined within the organization and the assigned staff should be skilled in managing the network devices and services and connectivity from a security perspective. Controls should be established to protect the network parameter from external threats and ensure that any data accessed by the employee through the Internet or public network is secure.

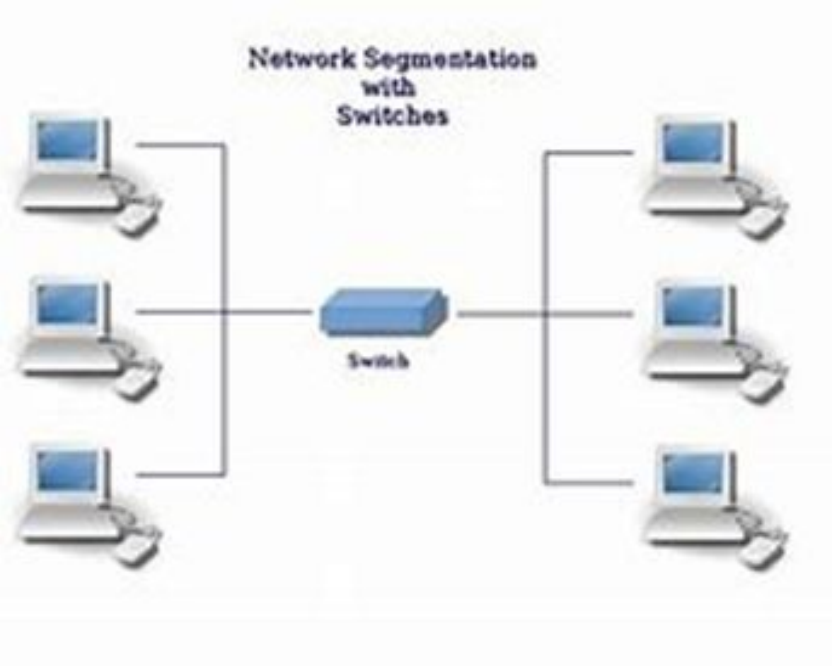
4.1.2 Security of network services

The goal of this control is to ensure that the requirements of network services are met and there are service agreements in place defining those requirements. Network services include covering the organization's needs of the network such as providing reliable wired and wireless networks, virtual private networks, and network connections and authentication and authorization services, safe data transfers and encryption and other security features that ensure the safety of the organization's information and systems. The organization should ensure service usage should be restricted to authorized personnel. Authorization levels should be implemented based on the business requirements of the roles.



4.1.3. Segregation in networks

To maintain separate authorization levels and access control, networks should be segregated creating separate groups of users, systems, and information services. Segregation at a network level is normally called segmentation which could be achieved by physically separating networks or logically by using virtual local area networks. The organization can achieve this by using network devices with such capabilities such as switches, rooters, and wireless network. Each domain in the network should have its own security and account policies and trust between domains can be established depending on the requirements.



4.2 Information transfer

The second category of the communication security class is called Information transfer. This category is concerned with the protection of data transferred inside an organization and any external entity. The organization must secure its transfer of information both outside and inside. It has four controls.

4.2.1. Information transfer policies and procedures

There are many risks affecting information when it is being transferred or in transit. Information can be captured in the middle for example by a man in the middle attack and can then be manipulated, stolen, copied, and even destroyed. The organization should take security measures which protects or mitigates such attacks by using strong encryption or virtual private networks. Users should not be allowed to automatically forward business emails to external accounts. Incoming emails should be checked for malicious attacks.

4.2.2. Agreements on information transfer

This control specifically deals with information transfer with external parties whether the information is transferred electronically or physically and the agreements to be established to ensure the security of the information. The organization should control the electronic transfer of information is traceable and non-repudiating meaning that the sender or receiver of data can not deny his actions. This can be achieved with logging outgoing and incoming communications and

being able to identify traffic being sent and received depending on the sensitivity of the information. For physical transfer, of data a proper courier should be selected that meets the organizational standards.

4.2.3. Electronic messaging

This is the third control and includes messages communicated through emails, social media, or any other electronic data exchange. The goal of this control is to safeguard those messages from unauthorized access. It is recommended to use security appliances or software to protect incoming and outgoing messages. Sensitive messages leaving the organization should be authorized and when possible have external layers of protection such as encryption. Incoming messages should be checked for malware or malicious links. The real sender of a message and its content should be verified to avoid spear phishing attacks that try to compromise the organization’s systems.

4.2.4 Confidentiality or non-disclosure agreements

To protect its information from unauthorized disclosure by employees and external and external parties, an organization should define and enforce legally binding agreements to be signed by those employees and parties. Agreements should be specific in scope stating what information is to be protected and the agreement's expected duration which could be indefinite if the information is confidential and has not been declassified yet. Information protections should rely on the information classification shame. The agreements should include terms that define what actions will be taken by the organization of the employees or external parties that have made violations and disclosed information without authorization. These terms should be of legal nature and would allow the organization to prosecute violators in compliance with the applicable laws and regulations.

5. System acquisition, development, and Maintenance

Organization should ensure its development and maintenance is at a higher standard to secure its information processing capability. This class has three categories with several controls.

5.1 Security requirement of information systems

The objective of this category is that information security applied to the entire lifecycle of any information system in the organization. The organization should make sure that information security is not limited to only some part of the information system. not This category has three controls.

5.1.1 Information security requirements, analysis, and specification

The company should implement this control which has the purpose to ensure that any new system or upgrades to existing systems should conform to the information security requirements of the organization which is often overlooked for the sake of performance and better capabilities. Identifying the required level of security requirements has several dependencies. It is influenced by the sensitivity of the information that the system will handle the level of threat that the organization faces and the compliance requirements to standards, policies, and frameworks. Once the security requirements are identified they should be integrated into the early stages of new information system projects implementing security controls in the planning and design stages provides a solid base to build on and saves lots of efforts later on when trying to manage security issues. The new information system project should consider user authentication requirements, access control requirements, data control requirements as well as logging and monitoring requirements.

5.1.2 Security application services on public networks

Organizations provide services and transfer information on the internet or public networks all the time to conduct their business and apply as well to transmitting sensitive information. This control ensures that this information is secured and protected from unauthorized disclosure or modification. The organization should verify the identity of the other party that they are providing or receiving information from by using authentication mechanisms such as digital certificates. Sensitive information should be authorized before it is sent over public networks depending on its criticality. Data loss prevention should be utilized to avoid unauthorized intentional or accidental transmittal of sensitive data.

5.1.3. Protecting application services transactions

Organizations provided applications should be secured and service transactions should be protected from unauthorized access. The risk affecting an applications transaction include Mis

rooted transaction unauthorized interception and alteration, unauthorized disclosure, duplicated transactions and unverified recipients or transmitters. The organization should deploy measures to prevent those risks from impacting its business. Digital certificates and signatures should be used to verify the involved parties in a transaction. User authentication information should be kept safe and it is preferable to utilize to form authentication to increase the level of protection. All user data should be kept private complying with the relevant laws and agreements. The communications of transactions should be encrypted to ensure confidentiality and integrity of the data. Backing of the transaction data should be considered depending on the organizations policies and business requirements.

5.2 Security in development and support processes

This is the second category, and its objective is to ensure that information security is considered and implemented in all phases of an information systems lifecycle. This category has nine controls.

5.2.1 Secure development policy

This control ensures developers develop secure software and consider security as a major requirement equal to performance and availability. A policy should be developed and implemented setting the rules for all developments in an organization. The policy should include measures to secure the development environment which are secured from unauthorized access. Security should be applied on the software design phase and checks should be performed at regular points within the project's milestones. Assessments should be performed to discover any vulnerabilities and fix them when reusing code from other developers. It should be checked if it complies with the security requirements of the organization.

5.2.2. System change control procedures

Changes could happen for many reasons. But to make sure that it is successful and improves the information systems and processes it must be controlled through formal change procedures. This second control ensures this. Change could provide functionalities but could introduce new risks as well and could compromise existing security controls. Change should not be random and should not be performed without prior risk and impact assessment. Failing to properly test and understand all the dependencies of a change could have catastrophic effects. A rollback plan should be developed in case the change was unsuccessful and did not serve its purpose. All changes should be authorized, approved, and documented for future reference including related documents such as authorization forms, change schedules and version control.

5.2.3. Technical review of applications after operating platforms changes

The purpose of this control is to ensure that system and platform changes do not have an impact on the business applications depending on them. Operating systems, databases and other platforms are usually updated or upgraded providing additional features and capabilities and performance enhancement and better security controls. Tests and reviews should be performed to ensure that the integrity of the applications is not affected before system changes are scheduled. Application teams should be informed beforehand and should have enough time to perform all the necessary tests.

5.2.4. Restrictions on changes to software packages

This control deals directly with modifications that an organization might consider performing on a software package provided by a vendor. Vendors supply their software in packages and in many cases altering the functionality of the software or modifying its aspects are not recommended and might even be prohibited by the vendor. Performing modifications to the software should be checked with the vendor and will require their acceptance. There is a serious risk that a modification might cause issues with software compromising its integrity and built-in controls. The best solution if a modification is required is to check directly with the vendor if they can do the change themselves or to keep the original software and apply change to a specific copy or version of it.

5.2.5 Secure system engineering principles

This control applies to in-house and outsourced information system engineering activities and ensures that the information security needs are met. Security principles should be established and followed in information system engineering projects throughout the applications technology and data. There should be a balance between security measures and accessibility requirements while ensuring that known vulnerabilities are analyzed and controlled. Security principles include providing guidance on authentication techniques, data validation, debugging codes and security input and output interfaces of an application. These controls should be constantly reviewed and a security policy documenting these principles should be maintained. Security should be treated as an integral part of a system design reducing risk to an acceptable level.

5.2.6 Secure development environment

The purpose of this control is to ensure that system development environments are secured and protected including all the involved people, technology and processes. The security controls to secure a development environment should depend on the associated risks affecting it and the sensitivity of the specific development activities. External regulations and internal policies requirements should be considered and the existing controls to protect the development environment should be reviewed. If the development is going to be partly or fully outsourced, the

security requirement should be defined in the agreements. Access to the environment should be controlled and data movement from and to the environments should be controlled and monitored.

5.2.7 Outsourced development

This control ensures that the organization constantly monitors and supervises the outsourced development not just for performance but also for security arrangements and controls. The underlying agreements should define and enforce the security requirements of the organization for secure design, coding, and detesting practices. The protection of data is very important as it could be residing outside the organization premises especially the newly developed data. The property of this data should be clearly defined and ways to ensure intellectual rights protection should be applied.

5.2.8 System security testing

This control necessitates that security testing of software and systems should be performed during development to ensure that issues are managed before being put into operation. Both in-house and outsourced developments should be tested for security vulnerabilities and ensure that data is protected. Testing activities should simulate how the software of a system would behave under attack which gives the developers insights into what they need to improve. Testing and verification activities should be scheduled stating what the testing criteria inputs and expected outputs are. After the development team has performed its tests an external independent test should be performed which provides an unbiased assessment and could cover areas which the initial tests failed to check. The level and scope of the tests should be proportional to the type of the system., its importance to the organization and the criticality of the data that the processes transmits or stores.

5.2.9 System acceptance testing

This is the last control. Before a new system is finally moved into operation or a new upgrade being rolled out and acceptance an acceptance testing should be performed which ensures that the system is acceptable by the organization. Information security requirements should be evaluated as part of the acceptance testing where the system is evaluated according to business requirements. A system should pass through all the testing criteria before it is made ready for end users, customers, or any business unit in an operational environment. The organization should use tools that would automate the testing such as vulnerability assessment tools or code analysis tools. The tests should be performed in environments that emulate a real operational environment to ensure that the tests are reliable and can perform under real conditions.

5.3 Test data

This is the third category, and its objective is to ensure test data is protected from unauthorized access and manipulation. This category has one control which is the last control.

5.3.1 Protection of test data

This control ensures that this data is controlled and properly selected to ensure optimum results. The selection of data becomes critical when testing on operational data is important to the success of the test. In such cases the inclusion of personally identifiable information should be avoided. When using operational data for testing an authorization should be obtained and documented each time data is transferred to the test environment. Access control rules should be applied to test data in a similar manner to operational data depending on its sensitivity and based on the information classification scheme. After a test is conducted and finished all operational data should be deleted immediately and this procedure should be documented and logged.

6. Supplier Relationships

6.1. Information security policy for supplier relationships

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Information and communication technology supply chain includes cloud computing services.

6.2. Monitoring and review of supplier services

Organizations should regularly monitor, review and audit supplier service delivery. The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

6.3. Managing changes to supplier services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

7. Information security incident management

7.1. Responsibilities and procedures

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.

7.2. Reporting information security events

Information security events should be reported through appropriate management channels as

quickly as possible.

All employees and contractors should be made aware of their responsibility to report information

security events as quickly as possible. They should also be aware of the procedure for reporting

information security events and the point of contact to which the events should be reported.

7.3. Reporting information security weaknesses

Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

All employees and contractors should report these matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible and available as possible.

7.4. Assessment of and decision on information security events

Information security events should be assessed and it should be decided if they are to be classified as information security incidents.

The point of contact should assess each information security event using the agreed information

security event and incident classification scale and decide whether the event should be classified as an information security incident. Classification and prioritization of incidents can help to identify the impact and extent of an incident.

7.5. Response to information security incidents

Information security incidents should be responded to in accordance with the documented procedures. Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organization or external parties. Post-incident analysis should take place, as necessary, to identify the source of the incident.

8. Information security aspects of business continuity management

8.1. Information security continuity

An organization should determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process. Information security requirements should be determined when planning for business continuity and disaster recovery. The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

8.2. Verify, review and evaluate information security continuity

The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

8.3. Redundancies

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements. Organizations should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures should be considered. Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

9. Compliance

9.1. Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

9.2. Identification of applicable legislation and contractual requirements

All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization. The specific controls and individual responsibilities to meet these requirements should also be defined and documented.

9.3. Intellectual property rights

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences. Proprietary software products are usually supplied under a licence agreement that specifies license terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only.

9.4. Protection of records

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

9.5. Privacy and protection of personally identifiable information

Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

9.6. Information security reviews

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

10. Access control

The purpose of this policy is to promote confidentiality, integrity and availability of the company's data.

10.1. Business requirements of access control

Management is to restrict access to information and information processing facilities to only authorized members of staff using a policy that states the rule of access control, access rights and the security requirements of the company. Sensitive information should have stricter controls and access should be closely monitored. Access control should be regularly reviewed and assessed, and should be revoked when the need for it is over.

Users and service providers should be given a clear statement of the business requirements to be met by access controls. Users should only be provided with access to the network and network services that they have been specifically authorized to use. This policy covers the means used to access networks and network services (e.g. use of VPN or wireless network).

10.1.2. Access to networks and network services.

Granting access to users should be based on strict requirements. Formal authorization procedure should be followed, and approval obtained from the relevant entities before access is granted. Access should be made secure by using user's authentication, passwords, VPNs, encryption, and other measures. Wired connections access to the network should be secured to avoid unauthorized plug-ins and access. It is important for guest users to have limited or no access to the company's network, if guest's access is granted, it should be limited, controlled, and monitored. Access granted to third party staff to provide maintenance and other short-term services should be revoked at the end of such services.

10.2. User access management

A formal user registration process should be implemented to enable assignment of access rights using certain implementation guidance such as unique user IDs to enable users to be linked to and held responsible for their actions. Shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented. Assess rights should be periodically reviewed to ensure the needs to such assess still exist, otherwise a formal de-registration of the assess right for all user types to all systems and services should be done.

10.3. Management of privileged access rights

Privileged access rights should be granted with more care because of its sensitivity and significant impact on the associated systems and assets. Access control policy should be taken into account, and after sufficient business deeds has been presented, an authorization process has to be completed before granting privilege access to an employee. A good record of all granted privileges should be maintained and once the business need no longer exit such privilege rights should be revoked and the record should reflect such change. Account with privilege access should not be used for personal activities because this increases the risk of creating a problem or compromising the company's data. Employees with access privileges should be educated on the risks associated with such access and disciplinary actions that follow when any misconduct is detected and the competencies of those employees should be constantly evaluated.

10.4. User responsibilities

Users should take responsibility for safeguarding their authentication information. A rule of not sharing company's information with anyone such as friends, family members should be enforced. Being careless with secret information should be prohibited and when information is suspected to be compromised, it should be changed. Rules for passwords creation should be done securely by complying with password policy. users should be advised to keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority and also that they should avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved.

10.5. System and application access control

The company must prevent unauthorized access to systems and applications while handling the technicalities of access control efficiently. Information access restriction control should be in accordance with the access control policy and its implementation guidance ensures that restrictions to access should be based on individual business application requirements.

Users' access to utility tools should be highly restricted. Unsupervised manipulation of some of those tools (like the antivirus or the operating system firewall or the system's file manager) could lead to high risk and should be prohibited. Access control to program source code should also be prohibited with the source code and the program listings stored according to a managed and controllable manner. Centralized storage should be used to obtain a high level of control as all access can be controlled to one location. A backup of the source code on a physical medium or on the cloud should be done to ensure uninterrupted availability of information.

11. Cryptography

11.1. Policy on the use of cryptographic controls

A policy on the use of cryptographic controls is necessary to maximize its benefit, which is, protecting the confidentiality, authenticity, and integrity of information. To minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use should also be considered. Cryptography and Encryption are necessary measures to protect stored and transmitted data preserving its integrity and confidentiality. Hence, specialist advice should be sought in selecting appropriate cryptographic controls to meet the information security policy objectives. The policy should define what level of protection is needed in accordance with the information classification scheme and the importance of the data to the organization.

11.2 Key Management

The management of cryptographic keys is essential to the success of cryptographic operations, hence a policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through the whole lifecycle of the keys. In order to reduce the likelihood of improper use, activation and deactivation dates for keys should be defined so that the keys can only be used for the period of time defined in the associated key management policy.

Remote access to the organization's assets should be encrypted and the users responsibilities to the management of the secret information should be defined in relation to the access control policy mentioned above.

A policy that deals with the secret key use and protection should be defined. Secret keys go through a lifecycle from being generated to eventually being discarded. The policy should cover the security of the keys throughout their life cycles with specific measures applied at each stage. After the management has decided on the strength of the security keys, a particular technical detail of the key generation should be decided and mentioned, such as the used algorithms and key length. Once generated, secrete keys should be secured from unauthorized access, change or coping. The tools used to generate the key should be secured physically and logically as well. Procedures on how to generate keys should be defined; how to distribute them, how to store them, how to update them, how to revoke them, and how to archive and recover them. The management of public keys and the obtaining of public certificates should be maintained and this should cover both liability and reliability issues.

12. Physical and environmental security

This class has two categories and 15 controls. The organization should put into consideration to secure its information both physically and environmentally.

12.1 Secure areas

This category has six controls concerned with physically securing the information facilities. The first control is called physical security perimeter and its purpose is to define measures that help to ensure the physical security of the surroundings of information facilities. The protection level depends on the criticality of the facility. The organization should know on which areas its assets are located and the perimeters that surround these areas. The perimeter should be properly surveyed, and it should be ensured that any gap allowing the breaches followed.

The second control is called physical entry controls. All entries to an organization secure facility should be identified and properly secured. Similar to logical restrictions on access points to an organization's information systems and networks, physical entry points could pose a serious threat to an organization's assets if not controlled. All entry points to secured areas should be monitored and secured. Only authorized personnel should be allowed access to the organization's facilities. Firewalls and other security facilities should be in place to secure all assets holding sensitive data.

Securing offices, rooms and facilities is another control. This control includes protection of rooms and offices where information or information facilities are being hosted. Control should be based on a proper risk assessment. Key facilities where critical information is being processed should be identified and warning signs should clearly state that unauthorized access is prohibited.

The fourth control the organization should put in consideration is called protecting against external and environmental threats. The purpose of this control is to have enough measures to protect against environmental disasters and physical malicious accidental or deliberate attacks. The organizations should seek advice from specialists that have experience in designing and implementing measures against natural disasters.

Working in secure areas is another control. Based on this control a set of procedures should be established to regulate working in the secure areas. Any work to be performed in a secure area should be authorized. In more critical areas work must be supervised to ensure the safety of the assets and facilities and to protect from any malicious attempt.

The last control is called delivery and loading areas. Those areas when they exist in an organization are considered as entry points and should be controlled and secured. There are additional measures that should be implemented in regards to delivery areas as new material will enter into the organization and presumably to secure areas. All deliveries should be scheduled

and authorized to avoid confusion and many malicious acts. Only authorized personnel should be allowed access and they should be attended to during their delivery. The delivery area should not allow access to other parts of the organization which is unauthorized to the delivery personnel.

12.2. Equipment

The organization should have strong control mechanisms ensuring that the equipments are secure.

12.2.1. Equipment siting and Protection

The equipment should be placed in a manner that maximizes the security and allows for better protection. The information facilities should be strategically positioned, especially critical facilities to minimize unauthorized access. Equipment storage areas should have a similar positioning consideration to avoid asset theft or damage. Personnel's behavior in the proximity of critical equipment should be regulated. Eating and drinking should be prohibited to avoid equipment damage.

12.2.2. Cabling Security

To protect equipment, utilities have to be secured, constantly maintained and monitored. Utilities management should be as specified by the manufacturer's specification and recommendation. Back-ups arrangement should be in place to ensure constant availability of utilities. Utility monitoring and control systems should be used to measure consumption and performance. Alarm should be set when performance and consumption limits have been reached. When new equipment or additional components are added, the utility performance has to be checked to ensure that it can handle the extra requirement. Emergency procedures and measures should be planned in case an unexpected disaster happens. Such measures include; having a redundant network connectivity through another provider or being able to shut things down manually.

Another control is called removal of assets. This control concerned with moving and taking equipment, information and other assets of premises temporarily. Assets can be taken for specific purposes such as for maintenance and testing or for temporary needs in other locations. These purposes need to have valid business objectives and subsequently authorized by appropriate management. Details about the removal of assets should be recorded such as the time of removal and returning.

Security of equipment and assets off-premises is the sixth control . there is a higher security risk of assets being compromised outside the organizations premises so it should be managed and controlled. Having taken authorization to talen an asset off premises an employee should ensure the security of these assets by using it in safe environments with appropriate environmental conditions.

Security disposal or reuse of equipment is another control which concerns equipment that has storage components and might be storing media on them. It has to be ensured that any stored media on this equipment can not not be retrieved and it has to be totally physically destroyed. Stored media has to be permanently deleted, destroyed or written over in a way that makes retrieving the original data impossible.

Unattended user equipment another control with the purpose to ensure the assets and equipment are secured when benign unattached to. Employees should be educated on how and why they should keep their equipment safe even when they are not being used. An unsecure and unattached equipment can cause serious risk if not managed when an employee leaves his computer unattended. He must ensure that it is locked or atleast has an active session that he is using closed. Unneeded services should be terminated. Devices should be locked by using key lock or a biometric

The last control is called d´clear desk and clear screen policy. A clear desk means that any sensitive information and storage and removable media should not be placed on an employees desk in a way that makes them easy to read and grab. Such items can be placed safely on a lockable drawer or cabinet. The organization should make the employees know and understand the sensitivity of the document or data stored on a media device. Highly critical diócument should be kept safe and accessed only when it is needed. Additional restrictions should be applied to reproduction of these documents. A clean screen means that when an employee is going to leave his device unattended he should lock it. Depending on how long the employee is going to be away for his device the employee should consider terminating any further log in sessions that he has initiated on his device.

Reference

[1] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-based access control models," in *Computer*, vol. 29, no. 2, pp. 38-47, Feb. 1996, doi: 10.1109/2.485845.
[2] J. H. Seltzer and M. D. Schroeder, "The protection of information in computer systems," in Proceedings of the IEEE, vol. 63, no. 9, pp. 1278-1308, Sept. 1975, doi: 10.1109/PROC.1975.9939.