Secuoya
content group

Information Security Policy

Code	PO.00
Title	Information Security Policy

Rules for the use, access, and distribution of the document

Any copy of this document shall be considered an unofficial copy, and it is the responsibility of the holder of such copy to verify its validity.

Any person, other than authorised personnel, who finds this document is required to send it to: Avenida de España, 4, 28760 Tres Cantos, Madrid or https://secuoyacontentgroup.com

Contents

1. INTRODUCTION

Information is a strategic asset for the companies that comprise the Secuoya Group (hereinafter referred to as "Secuoya"), as their main activities are framed within the provision of audiovisual services. Secuoya depends on Information Technology (IT) systems achieve its strategic objectives. These systems must be managed with diligence, taking appropriate measures to protect them from accidental or deliberate damage that could affect the availability, integrity, confidentiality, authenticity, or traceability of the information processed or the services provided.

The objective of information security is to guarantee the quality of information and the uninterrupted provision of services by acting proactively, monitoring daily activities, and responding promptly to incidents.

IT systems must be protected against rapidly evolving threats that have the potential to impact the availability, integrity, confidentiality, authenticity, traceability, intended use, and value of the information and services. To defend against such threats, a strategy is required that adapts to changes in environmental conditions to ensure the continuous provision of services.

This implies that the security measures required by the Corporate Information Security Management System (ISMS) must be implemented. Secuoya continuously monitors the criteria and requirements set out by applicable legislation, such as Royal Decree 3/2010 of 8 January, which regulates the National Security Framework in the field of Electronic Administration (ENS), Organic Law 3/2018 of 5 December, on Personal Data Protection and the guarantee of digital rights (LOPDGDD), and the European Union Regulation 2016/679 on the protection of personal data processing (GDPR). Furthermore, continuous monitoring is conducted on service levels, reported vulnerabilities are analysed, and an effective response to incidents is prepared to ensure the continuity of the services provided.

Thus, we can identify three distinct roles:

- **Information Manager:** responsible for determining the requirements of the information processed.
- **Service Manager:** responsible for determining the requirements of the services provided.
- **Security Officer:** responsible for making decisions to meet the security requirements of the information and services.

Secuoya must ensure that information security is an integral part of every stage of the IT systems lifecycle, from their conception to retirement, including development or acquisition decisions and operational activities. Security requirements and funding needs must be identified and incorporated into planning, tender requests, and IT project outsourcing proposals.

2. OBJECTIVE

Secuoya establishes this Information Security Policy with the primary objective of ensuring the security of information and the continuous provision of the services it delivers, through preventive action, ongoing supervision of activities, and prompt response to any incidents that may arise.

This Policy is intended to lay the foundations for securely accessing, using, protecting, and safeguarding the information assets on which Secuoya depends to perform its functions, ensuring compliance with security guarantees in various dimensions:

- **Availability:** The property or characteristic of assets that ensures authorised entities or processes can access them when required.
- **Integrity:** The property or characteristic that ensures the information asset is not altered in any unauthorised manner.
- **Confidentiality:** the property or characteristic that ensures information is not made available or disclosed to unauthorised individuals, entities, or processes.
- **Authenticity:** the property or characteristic that ensures an entity is who it claims to be or guarantees the source from which data originates.
- **Traceability:** the property or characteristic that ensures the actions of an entity can be attributed solely to that entity.

In line with these principles, the specific objectives of Information Security at Secuoya are as follows:

- Ensuring the security of information across the dimensions.
- Conducting effective management of incidents that affect information security.
- Developing, maintaining, and testing availability and continuity plans for the various services provided by the organisation.
- Ensuring that all personnel are fully informed of security requirements and promoting best practices for the secure handling of information.
- Ensuring the agreed-upon levels of security when sharing or transferring information assets with third parties.
- Complying with applicable regulations and standards.

The Information Security Policy:

- Shall be formally approved by the Security Committee and presented to the Board of Directors.
- Shall be regularly reviewed to adapt to new technical or organisational circumstances, and to avoid obsolescence.
- Shall be communicated to all employees and external companies working with Secuoya.

3. MISSION

The purpose of this Information Security Policy is to protect the information and services of Secuoya.

- Secuoya expressly recognises the importance of information, as well as the need for its protection, as it constitutes a strategic and vital asset. The total and irreversible loss of certain data could jeopardise the continuity of the organisation or cause significant damage.
- Secuoya implements, maintains, and monitors the controls set out in its statement of applicability and the processes of its ISMS, in accordance with ENS standards, GDPR, LOPDGDD, ISO 27001, and ISO 20000-1, and complies with all applicable legal requirements.
- Information and services are safeguarded against losses in availability, integrity, confidentiality, authenticity, and traceability.
- Service requirements regarding information security and information systems security are fully met.
- Controls shall be proportionate to the criticality and classification of the assets being protected.
- The responsibility for the security of information involved in the provision of services within the scope lies with the Security Committee, which will provide the necessary resources. Nevertheless, employees and users are expected to assume their share of responsibility regarding the resources they use, as set out in the policies, regulations, and supplementary procedures.
- Those responsible for Information Security and related administrative functions will manage security.
- Information owners have been identified and shall promote the establishment of controls and measures aimed at protecting the data they manage, particularly personal or critical data.
- The necessary and appropriate means have been established and made available to protect individuals, data, software, equipment, facilities, documentation, and other media containing information, and in general, any asset of Secuoya.
- Specific aspects related to personal data are governed by the set of rules included in this security document and by internal or other applicable regulations referenced herein.
- Individuals who fail to comply with these rules and supplementary procedures may be subject to disciplinary action in accordance with labour law and the applicable collective agreement, or in the case of non-employees, sanctions as stipulated in their contracts and applicable legislation.
- Regular risk assessments are conducted, and based on identified weaknesses, implementation or reinforcement plans for controls may be developed.
- The dissemination of information and security training for employees and collaborators is encouraged to prevent errors, omissions, fraud, or criminal activity, and to detect any such occurrences as early as possible. In the event of incidents, investigations are conducted with highly restricted dissemination.
- Secuoya personnel must be familiar with the rules, regulations, standards, and procedures related to their position, including their roles and responsibilities, as well as the segregation of duties and independent review of records where necessary, to ensure accountability regarding who performed what action, when, and from where.
- Security incidents are properly reported and addressed.

4. SCOPE

This Security Policy applies to all companies within the Secuoya group, as well as to their information systems and assets, including:

- All departments, both management and employees.
- Contractors, clients, and any other third party with access to the organisation information or systems.
- Databases, electronic and paper-based records, processing activities, equipment, media, software, and systems.
- Information generated, processed, and stored, regardless of its medium or format, used in operational or administrative tasks.
- Information provided within an established legal framework, which shall be considered as proprietary solely for protection purposes.
- All systems used for the management and administration of information, whether owned, leased, or licensed by the organisation.

This Information Security Policy is designed to support the information systems that underpin management processes and audiovisual services, including:

A. Production and post-production of audiovisual content and information for television.
B. Production and audiovisual services: advanced experiences (augmented and virtual reality) and innovative content for brands.

This policy applies in accordance with the current statement of applicability and covers the activity centres and permanent locations of the following entities:

- CBM SERVICIOS AUDIOVISUALES, S.L. (B18911651)
- CBM MEDIA SERVICIOS DE PRODUCCIÓN, S.L. (B18893164)
- CBM SERVICIOS DE TELEVISIÓN, S.L. (B73881716)
- SECUOYA NEXUS, S.L. (B18950642)

5. REGULATORY FRAMEWORK

The control of regulations and applicable legislation for this security policy, which is included within the Information Security Management System, refers to, among others, the following regulations and laws:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, regarding the protection of natural persons regarding the processing of personal data and on the free movement of such data (GDPR).
- Organic Law 03/2018 on Data Protection and the Guarantee of Digital Rights (LOPDGDD).
- Law 31/1995 of 8 November on the Prevention of Occupational Risks and Royal Decree 39/1997 of 17 January, which approves the Regulation of Prevention Services.
- Law 34/2002 of 11 July on Services of the Information Society and Electronic Commerce (LSSI-CE).
- Royal Decree 3/2010 of 8 January, which regulates the National Security Framework (ENS) within the field of electronic administration).
- Criminal Code (Organic Law 10/1995 of 23 November), which includes provisions related to data protection and privacy offences.
- The Criminal Procedure Act, particularly relevant for its content in Book II, Title VIII, Chapter III, which includes common provisions on the interception of telephone and telematic communications, the capture and recording of oral communications using electronic devices, the use of technical devices for tracking, location and image capture, the search of mass information storage devices, and remote searches on computer equipment.

6. CONTENT

6.1 Regulatory Governance

Secuoya establishes a regulatory framework around Information Security to enable the deployment of all necessary regulatory resources, ensuring operational capability and legal protection to meet the objectives set by the Security Committee.

To achieve efficiency, a system is structured into three main functional levels: strategic, tactical, and operational. Additionally, a technical level is introduced to adapt regulations to the evolving technologies of Information Systems.

The following are the three levels present within a planning system, alongside the technical level adapted to Information Systems resources:

6.1.1 Strategic or Superior Level

This level corresponds to planning aimed at achieving the objectives of the organisation and serves to establish action plans for company operations. It focuses on setting company goals, defining resources to be used, and establishing policies for acquiring and managing this resource.

This level establishes the general, though not detailed, framework for the functioning of Secuoya.

The Security Committee leads and approves the strategic level. Final approval and validation of the documentation rest with the Board of Directors.

6.1.2 Tactical or Intermediate Level

This level involves detailed planning for each area within Secuoya, based on the framework established at the strategic level.

It is drafted, approved, and validated by the Security Committee.

The primary difference between the strategic and tactical levels is that the strategic level covers company-wide policies over an extended period, while the tactical level focuses on specific standards for products, services, general operations, quality metrics, or other offerings, with clearly defined timelines and deadline.

6.1.3 Operational or Lower Level

This level involves internal regulations that enable the coordination of tasks across the various departments of Secuoya. It is developed from the guidelines provided by the strategic and tactical levels.

This level is created and approved by the Security Committee.

Those responsible for drafting this documentation must adhere to higher-level regulations and comply with rules precisely defined by the other two levels. The internal regulations at this level apply to specific time periods for each process.

6.1.4 Functional or Technical Level

This level includes technical documentation that enables employees to use a tool from the Information Systems of Secuoya to perform their functions.

The creation of this documentation depends on a designated responsible party, and its publication should only occur within the internal systems of the organisation.

6.2 Regulatory Structure

The following regulatory framework is established, ranked from highest to lowest level:

- Upper or Strategic Level:
    - Corporate Policy

- Middle or Tactical Level:
    - Corporate Regulations

- Lower or Operational Level:
- Corporate Procedures

- Technical Level:
    - Technical Guides
    - Internal Manuals
    - Manufacturer Manuals

6.3 Policies

Secuoya must be prepared to prevent, detect, respond to, and recover from incidents, in accordance with the established policies and the service level agreements committed to clients and users.

Furthermore, this document addresses how we approach Information Security policies, how we organise security within the corporation, how we ensure and protect personal data, risk management, and the development of the Information Security Policy.

6.4 Prevention

Secuoya commits to employing all means at its disposal to prevent or, at the very least, mitigate any harm to information or services caused by security incidents. To this end, the necessary security measures, as determined by applicable legislation, will be implemented, along with the controls deemed necessary by the ENS, ISO 27001, and ISO 20000-1, as well as any additional controls identified through threat and risk assessments.

To ensure compliance with this policy, Secuoya will deploy the necessary organisational and technical resources to:

- Authorise systems prior to operation.
- Regularly assess security, including evaluations of routine configuration changes.

- Ensure that risks affecting Secuoya are identified and maintained within acceptable levels.
- Ensure that the services provided by Secuoya to its clients, along with the activities developed for their provision, possess an increasing level of security and have undergone the necessary testing to ensure an acceptable level of risk.
- Develop and implement all necessary policies, controls, and standards in information security to ensure compliance with business requirements, service level agreements, and stakeholder expectations.
- Request periodic third-party reviews to obtain an independent evaluation.

6.5 Detection

Since services can degrade rapidly due to incidents, ranging from simple slowdowns to full-service stoppages, continuous monitoring of operations is necessary to detect anomalies in service performance levels and act accordingly.

Monitoring is particularly relevant when lines of defence are established. Mechanisms for detection, analysis, and reporting will be set up to ensure that deviations from predefined normal parameters are communicated to the responsible parties both regularly and when a significant deviation occurs.

6.6 Response

- Mechanisms are established to effectively respond to security incidents, managed by the Security Committee.
- A contact point is made available to clients and users for reporting incidents detected in their operations (incidencias@secuoyacontentgroup.com), and an internal HelpDesk tool is also available (https://helpdesk.secuoyacontentgroup.com).

6.7 Recovery

To guarantee the availability of critical services, continuity plans for ICT systems have been developed as part of a general service continuity plan and recovery activities.

7. SECURITY ORGANISATION

Secuoya defines the following committees and general roles in relation to their participation in the management and oversight of information security:

- Security Committee
- Crisis Committee

7.1 Security Committee

The Security Committee is established as a collegiate body to lead and coordinate information security within Secuoya, ensuring the governance and management of cybersecurity risks, and taking actions to safeguard and mitigate these risks.

7.1.1 Mission

To support the goals and objectives of each company within the group, providing leadership to ensure legality, confidentiality, integrity, availability, and traceability of its information resources, as well as ensuring that third-party (client) assets accessed through Secuoya information systems (whether on-site or remotely) remain uncompromised.

Information is understood to include:

- Information itself, such as data managed within systems, transmitted through digital processes (networks, applications, or any mechanism used for interoperability with target systems), or stored on storage devices, whether owned by Secuoya or third parties.
- Processes, applications, and information systems that support the information and are part of Secuoya activities.

In essence, the Security Committee is responsible for raising awareness among all Secuoya employees about cybersecurity risks, protecting Secuoya information resources, investigating potential misuse of systems, monitoring compliance with all established policies, procedures, and rules regarding the acceptable and appropriate use of resources, as well as governing security mechanisms implemented to protect and defend target systems from technological threats that could jeopardise Secuoya or third-party business.

The Security Committee is part of the management and cross-functional services that Secuoya provides to all the companies and divisions within the group and is responsible for formalising cybersecurity policies and objectives aligned with the company strategic goals.

7.2 Roles and Responsibilities

A Security Committee within the Corporate Security Policy of a corporate group has key roles and responsibilities to ensure the protection of the physical, digital, and human assets of the organisation. While functions may vary depending on the company, they generally include:

i Development of Security Policy:
  - Drafting and updating security policies, ensuring they comply with legal regulations and industry standards.

- Regular review of these policies to adapt them to new threats or changes in the business environment.

ii Risk Assessment:

- Identification and evaluation of potential risks that could impact the security of the company, both physical and digital.
- Continuous monitoring of emerging threats and vulnerability analysis to prioritise preventive actions.

iii Planning and Strategy:

- Designing security strategies to protect infrastructure, data, and personnel.
- Developing incident response plans and emergency procedures.

iv Supervision and Coordination:

- Overseeing the implementation of security measures across all areas of the company.
- Coordinating with other departments (IT, Human Resources, Legal) to ensure comprehensive protection of data and assets.

v Training and Awareness:

- Organising training and awareness programmes for employees on optimal security practices.
- Promoting a security culture throughout the organisation to foster safe behaviours.

vi Incident Management:

- Managing security incidents, from identification to resolution and documentation of lessons learned.
- Post-incident evaluation to improve and adjust existing security strategies.

vii Audits and Compliance:

- Conducting internal security audits and verifying compliance with policies.
- Ensuring adherence to external regulations and industry standards, such as ISO 27001, GDPR, etc.

viii Reporting and Communication:

- Providing regular reports to management on the state of security and any relevant incidents.
- Maintaining effective communication channels for security alerts and policy update notifications.

ix Continuous Improvement:

- Ongoing assessment of security processes to identify areas for improvement.
- Incorporating new technologies and protection methods in line with advancements and best practices.

In summary, the Security Committee acts as the primary body for control and decision-making in security matters, playing an essential role in protecting the integrity, confidentiality, and availability of the assets of the organisation.

7.2.1 Governance and Organisation

The Security Committee is established as a collegiate body, reporting to the Management Team and structured as follows:

- Head of Purchasing and Internal Audit
- IT Director
- Data Protection Officer

Depending on the subject matter:

- Business Operations Director
- Manager of the affected/compromised service
- Other specific profiles

Activities:

- Establishing security policies and objectives that are compatible with the organisation policies and strategic goals.
- Integrating the security management system requirements into the company processes.
- Ensuring the availability of necessary resources.
- Establishing effective communication policies related to cybersecurity practices within the organisation.
- Conveying cybersecurity requirements to projects.
- Communicating the development, documentation, and maintenance of cybersecurity risk management plans.

7.3 Crisis Committee

The Crisis Committee is essential for making key decisions in managing any crisis arising from a severe security incident.

In this committee, decisions are made regarding the actions to be taken and the steps required to resolve the issue, as well as managing communication with all parties involved.

7.3.1 Objectives and Functions

The objectives include:

- Unified management of a crisis.
- Defining key scenarios to consider and appropriate responses.
- Accelerating the decision-making process to resolve incidents and crises by setting priorities, strategies, and tactics to follow.

Functions:

- Deciding whether a crisis exists and determining its level or degree based on the alert system and pre-established severity levels.
- Determining the appropriate course of action in response to the issue.
- Establishing and implementing the necessary measures to resolve the problem.
- Allocating responsibilities within the relevant areas to facilitate resolution and ensure coordination among all involved parties.
- Protecting the public image and reputation from the potential negative impact of the situation.
- Establishing a comprehensive information policy during the crisis.
- Continuously evaluating the strategy being implemented, along with its actions and results.
- Detecting and anticipating events and steps to take based on the unfolding situation.
- Centralising information both internally and externally.
- Ensuring coherence and unity across all actions at various levels of intervention.
- Appointing internal and external spokespersons.

7.3.2 Governance and Organisation

The committee may be convened at the request of management or by a responsible individual within the organisation. It should include representatives from various Secuoya departments:

- General Management
- IT Systems Management
- Legal Management
- Human Resources Management
- Communications/Marketing Management
- Data Protection Officer (DPO)

Depending on the crisis, the committee may be assembled with specific individuals as required, without the participation of all its members.

8. PERSONAL DATA

The LOPDGDD and the GDPR seek to guarantee and protect, regarding the processing of personal data, the public freedoms and fundamental rights of individuals, particularly their honour, personal and family privacy. These regulations apply to personal data recorded both electronically and on paper.

The privacy policy of Secuoya, which governs data protection regulations, is published at https://secuoyacontentgroup.com/en/privacy-policy/

All information systems of Secuoya shall comply with the security levels required by the regulations concerning the nature and purpose of the personal data collected for processing.

To ensure such protection, security measures have been adopted in accordance with the requirements set out in applicable legislation.

Any internal or external user who, by virtue of their professional activities, has access to personal data is obliged to maintain confidentiality regarding such data. This obligation shall remain in force indefinitely, even beyond the termination of the professional or employment relationship with Secuoya.

9. RISK MANAGEMENT

All systems subject to this Policy must undergo a risk analysis, evaluating the threats and risks to which they are exposed. This analysis shall be reviewed:

- Regularly, at least once a year.
- When the information being handled changes.
- When the services provided change.
- When a serious security incident occurs.
- When serious vulnerabilities are reported.

To harmonise risk analyses, the Security Committee shall establish a reference valuation for the different types of information handled and the various services provided. The Committee shall facilitate the availability of resources to meet the security needs of different systems, promoting horizontal investment strategies.

10. DEVELOPMENT OF THE INFORMATION SECURITY POLICY

10.1 Information Security Management System

For the proper management of the Information Security Management System (ISMS), we adhere to the ISO 27001 standards and the National Security Framework, with the aim of ensuring the correct application of periodic review controls, establishing maturity levels, and developing implementation and improvement plans.

Established Maturity Levels:

- Level 0 Non-existent: The organisation does not have effective implementation of controls or associated processes.
- Level 1 Initial: The organisation implements and achieves the objectives of the processes.
- Level 2 Repeatable but intuitive: The organisation manages controls and processes, and the results of activities are established, monitored, and maintained.
- Level 3 Defined and implemented process: The organisation uses controls and processes adapted based on standards. The processes are described according to standards, procedures, tools, and methods through adaptation guides.
- Level 4 Managed and measurable: The organisation quantitatively manages the associated controls and processes.
- Level 5 Optimised: The organisation continuously improves processes, based on a quantitative understanding of common causes of variation, to meet the objectives of both information security and the business.

10.2 Information Systems Usage Policy

The internal policy for the use of Information Systems is communicated by the HR department when a new employee is registered in the organisation and can be requested at any time. This information aims to regulate the use of Secuoya information systems provided to its employees and users, ensuring the security, legality, performance, integrity, and privacy of the information, preserving the privacy and security of staff, and in general, ensuring the effective fulfilment of activities and other tasks strictly within the scope of employment.

The following are not considered acceptable:

- Creating, using, or transmitting material that infringes data protection or intellectual property laws.
- Installing, modifying, or changing the configuration of software systems (only system administrators are authorised to do so).
- The use of the internet for personal purposes (including web-based personal email) will be limited to authorised break times. Any personal electronic transaction conducted will be under the responsibility of the user.
- Deliberately providing access to facilities or services to unauthorised individuals.
- Wilfully wasting network resources.
- Intentionally corrupting or destroying the data of other users or violating their privacy.
- Introducing viruses or other forms of malicious software intentionally. Before using any information storage media, it must be checked to ensure it is free of viruses or similar threats.
- Voluntarily revealing passwords or access credentials.

- Using the equipment for personal profit.
- Creating, using, or transmitting offensive or obscene material or material that could cause discomfort or offence.
- Sending excessively large emails or sending emails to many recipients (which could saturate communications).
- Failing to ensure that emails are virus-free.

10.3 Security in Human Resource Management

Personnel security is essential to mitigate the risks of human error, theft, fraud, or misuse of facilities and services.

A confidentiality agreement shall be required as part of the contract signing process for all employees to prevent the disclosure of confidential information.

All security policies and procedures shall be communicated regularly to all employees and external users, where applicable. Upon the termination of employment or contractual relationships with employees or external personnel, their access permissions to facilities and information shall be revoked, and they shall be required to return any information or equipment provided to them for the completion of their tasks.

10.4 Physical and Environmental Security

For logical security to be effective, it is essential that facilities maintain proper physical security to prevent unauthorised access as well as any other form of external damage or interference.

10.4.1 Secure Areas

Secuoya shall take the necessary precautions to ensure that only authorised individuals have access to its facilities.

All Secuoya facilities have the necessary physical barriers in place to safeguard the resources they contain, and personnel shall be accompanied during their time within the premises.

10.4.2 Equipment Security

IT equipment is a critical asset on which the continuity of operations depends and must therefore be adequately and effectively protected.

The IT equipment of Secuoya is protected against potential power failures, including laptops with batteries, uninterruptible power supplies, and similar protective measures.

The equipment shall be properly maintained to ensure its correct functioning and optimal condition, in order to maintain the confidentiality, integrity, and above all, the availability of information. To achieve this, the equipment must undergo the revisions recommended by the supplier. Only authorised personnel shall have access to the equipment for repair purposes. It shall also be necessary to take the required precautions when equipment is removed from the premises for maintenance purposes.

10.5 Communication and Operations Management

10.5.1 Operational Procedures and Responsibilities

Secuoya shall control access to services on internal and external networks and shall ensure that users do not compromise these services. To achieve this, appropriate interfaces must be established between the network of Secuoya and other networks, along with suitable authentication mechanisms for users and devices, and access controls for each user of the information system.

To prevent malicious use of the network, mechanisms shall be implemented to limit the network services that can be accessed, as well as authorisation procedures to define who can access which network resources, and management controls to protect network access.

All employees authorised to handle automated information must be registered as domain users. Every time they access the information system, they must validate their identity using their unique and non-transferable username and personal password. This password shall expire periodically.

To ensure the correct and secure operation of information systems, operational procedures shall be appropriately documented and implemented according to these procedures. These procedures shall be reviewed and updated as necessary when significant changes occur in equipment or software.

In some cases, it will be necessary to logically separate different areas from the rest to prevent unauthorised access.

10.5.2 Protection Against Malicious Code and Mobile Code

The installation of any software that is not authorised and necessary for work purposes is strictly prohibited for Secuoya personnel.

All software acquired by the organisation, whether by purchase, donation, or transfer, shall remain the property of the institution and shall retain the intellectual property rights granted by law, with careful monitoring of the different types of licences.

Any software that requires installation to operate on the network must be evaluated by the Security Committee.

The System Administrator shall install appropriate software tools to protect systems against viruses, worms, trojans, and other malicious code. Users must follow the instructions provided to protect the equipment, applications, and information they work with.

10.5.3 Security Copies

Data shall be saved according to the standards established in the information systems usage policy to ensure availability.

10.5.4 Network Security Management

Network components (such as switches, routers, and similar equipment) shall be kept out of reach of unauthorised personnel to prevent malicious use that could compromise system security.

10.6 Media Management

Users shall apply the same security measures to media containing sensitive information as those applied to the files from which the information was extracted.

10.6.1 Information Exchange

Procedures shall be established to protect information exchanged through any means of communication (electronic, verbal, fax, and others).

10.6.2 Monitoring

Where necessary, mechanisms shall be implemented to detect unauthorised information processing activities. This shall involve conducting tasks such as system log inspections and activities to test the efficiency of data security and data integrity procedures to ensure compliance with the established policy and operational procedures, as well as recommending any necessary changes.

10.7 Access Control

10.7.1 Service Requirements for Access Control

Information shall be protected against unauthorised access. The service manager shall define access requirements for information at two levels: for the entire area and for each user within the area. Access shall only be granted to the information necessary for the work to be carried out.

10.7.2 User Access Management

The system administrator is responsible for providing users with access to IT resources, as well as specialised logical access to resources (servers, routers, databases, and others) connected to the network.

Each user shall be associated with a profile, based on the tasks they perform within the organisation, as defined by their direct supervisor. Each of these profiles shall have specific permissions and restricted access to information and systems that are not necessary for the job functions of the user.

10.7.3 User Responsibilities

Workstations shall be kept clear of papers and other information storage media to reduce the risk of unauthorised access and other potential damage. These items should be stored in appropriate locked spaces, especially outside working hours.

10.7.4 Network Access Control

Access to the network, systems, applications, or information shall not be permitted for any user who is not formally authorised to do so.

In the case of service providers or external entities that need access for a justified reason, they are required to sign confidentiality agreements with Secuoya and must be informed of the security policies, standards, and procedures they must adopt to maintain the same level of security as Secuoya employees.

The use of free or third-party VPN services to access the company information systems is not recommended.

Whenever possible, access to information systems shall be restricted from anonymisation networks (such as TOR, I2P) and other services commonly used for illegal activities that aim to conceal the true origin of connections.

10.7.5 Mobile Computing and Remote Work

When equipment or information owned by Secuoya is taken off-site, the employee using it must take appropriate measures to prevent theft or damage during handling, transport, and storage.

10.8 Incident Management

Cybersecurity incidents observed or suspected by any employee must be reported to the Security Committee through the designated communication channels, primarily email.

Other security incidents, whether physical (such as fire or water damage) or related to support services (such as communications, electricity, or similar services), must also be reported immediately to the Security Committee so that appropriate measures can be taken and the incident recorded. Depending on the severity, priority will be given to phone communication over email.

Responsibilities and incident management procedures will be established to ensure a rapid, effective, and orderly response to security-related events

Incident logs will serve as the basis for identifying new risks and for verifying the effectiveness of the implemented controls.

10.9 Service Continuity

It is essential for Secuoya to establish guidelines to follow in the event of an interruption of activities due to serious security failures or disasters of any kind.

To ensure continuity of operations in such cases, Secuoya will establish contingency plans that enable the recovery of activities to at least a minimum level within a reasonable timeframe. Service continuity management will include various controls for identifying and mitigating risks, and a procedure that limits the harmful consequences of such risks and ensures the resumption of essential activities as quickly as possible.

The service continuity strategy will be documented, based on the identified risks and the controls defined accordingly, and must be tested and updated regularly to ensure its suitability.

Service continuity management will be integrated into Secuoya processes and will be the responsibility of one or more individuals within the organisation.

11. STAFF OBLIGATIONS

All members of Secuoya are required to understand and comply with this Information Security Policy, and it is the responsibility of the Security Office to provide the necessary means to ensure that information reaches those affected.

All members of Secuoya will receive security training and awareness at least once a year. A continuous awareness programme will be established to ensure that all members of Secuoya, particularly new employees, are adequately trained.

Those responsible for the use, operation, or administration of IT systems will receive training on the safe handling of these systems as needed to perform their job functions. This training will be mandatory before assuming any responsibility, whether it is their first assignment or a change in job role or responsibilities.

12. THIRD-PARTY ENTITIES

When Secuoya provides services to other entities or organisations, or manages information on their behalf, those entities will be made aware of this Information Security Policy, channels for reporting and coordination with the respective Corporate Security Committees will be established, and procedures for responding to security incidents will be put in place.

When Secuoya utilises third-party services or transfers information to third parties, these third parties will be informed of this Security Policy and the related Security Regulations applicable to those services or information. These third parties will be subject to the obligations set out in those regulations and may develop their own operational procedures to meet them. Specific procedures for reporting and resolving incidents will be established. It will be ensured that third-party staff are adequately aware of security matters, at least to the level set out in this Policy.

Where any aspect of this Policy cannot be met by a third party, as required in the previous sections, a report will be required from the Security Officer outlining the risks involved and how they will be addressed. Approval of this report will be required from the information and service managers before proceeding.