INFORMATION SECURITY POLICY

VERSION 12.0

1ST OCTOBER 2024

Author: IT Department

INFORMATION SECURITY POLICY

Version History				
VERSION	APPROVED BY	DATE REVIEWED	DESCRIPTION OF CHANGES	AUTHOR
1	N/A	September 2019	New Document	ISMS Manager
2	Management	October 2019	Document Approval	Management
3	N/A	12th November 2019	Include sections 4,5,6,7 to improve general policy.	ISMS Manager
4	Management	13th November 2019	Document Approval	Management
5	N/A	20th August 2020	Document periodical review and policies unification	ISMS Manager
6	Management	22nd October 2020	Document Approval	Management
7	N/A	26th October 2021	Document periodical review and policies. Added new providers ISO27001 compliance	ISMS Manager
8	Management	12th November 2021	Document Approval	Management
9	N/A	26th October 2022	Multiple modifications to adapt the General Information Security to the new ISO27001:2022	ISMS Manager
10	Management	16th November 2022	Document Approval	Management
11	N/A	25th October 2023	Document Review	ISMS Manager
12	N/A	1st October 2024	Revised and implemented new branding styles	ISMS Manager
13	N/A	28th October 2024	Added a new area to improve permissions assignment due to security incidence	ISMS Manager
14	N/A	22nd November 2024	Modified the policy according to the new CPD 7.2.4	ISMS Manager

1. DOCUMENT ORGANIZATION

2. OBJECTIVE

All information handled by a company can be exposed to changes, elimination, corruption, unauthorized disclosure, ... which can compromise its image or associated third parties if there are no appropriate mechanisms to ensure the confidentiality, availability, and integrity of data within the organization.

The company recognizes hence that information is a critical asset involved in all business processes and that this information must always be protected, no matter how it is shared, communicated, or stored.

In order to guarantee the correct fulfilment of its mission, company has implemented and maintains an Information Security Management System with the objective of:

- Comply with legal regulations and customer requirements related to information security.

- Satisfy the principles of information security by defining policies, procedures and rules that ensure confidentiality, availability, and integrity of information.

- Continuously improve procedures, processes, and policies.

- Minimize risks in critical areas of the organization.

- To guarantee the continuity of services.

- Protect all assets of the entity.

- Promote the culture of Information Security among its workers.

Being aware of information management criticality, company LIBNOVA has decided in addition to improve its Information Security Management System according to ISO27001:2022 and update and maintain its processes according to the latest version of that standard.

The purpose of this document is providing all staff a basic guide to mitigate risks associated with information systems inside Libnova.

3. SCOPE

The scope of this document is defined as the " Information Security Management System for the design, commercialization, deployment, operation and visualization of systems or processes for Digital Preservation and protection of Digital Assets."

The regulations will be applied to all the company's processes:

- Internal business processes

- Processes of rendering services to third parties

The application of the system will be extended to third parties as determined necessary.

This policy applies to all staff. It is **mandatory** and in case of non-compliance, sanctions might be carried out as specified inside **LIB-POL-020-Disciplinary Process**.

4. INFORMATION SECURITY OBJECTIVES AND PLANNING FOR EXECUTION

The objectives of information security are established in the necessary functions and levels, focused on improvement, and using as reference:

- Changes in stakeholder needs leading to an improvement in the scope of the system.
- Information security requirements and risk treatment results to guarantee confidentiality, integrity, and availability of information.
- Internal factors such as implementation of improvements in the organization that may benefit the ISMS or external factors such as technological advances or changes in legislation.
- Improvement in the effectiveness of training and awareness of personnel and that affects their performance in information security.

Likewise, the planning to achieve the established information security objectives will be carried out considering the following elements:

- What is going to be done.
- The necessary resources
- The responsible
- Timeframe for completion
- Indicators to assess outcome or compliance.

5. INFORMATION SECURITY FUNCTIONS AND RESPONSIBILITIES

Responsible of ISMS are:

- ISMS Manager: It will be responsible of notifying this policy to all employees of the company and inform them about any changes in it, as well as coordinating actions to implement, maintain and improve the ISMS of the company together with the Infrastructure Department that will oversee managing the technical security requirements of the information systems.

- Management: Responsible of reviewing and approve all policies and procedures and provide ISMS and Infrastructures Team with the appropriate resources to carry on with the ISMS improvement.

- Staff: all workers must observe this policy and all policies developed by the company.

6. ESTABLISHMENT, IMPLEMENTATION, MAINTENANCE, AND IMPROVEMENT OF ISMS

The deployment of the ISMS will start from the risk analysis that will determine the level of information security risk.

Security controls must be implemented, maintained, and continuously improved, and be available as documented information, reviewed and approved by the ISMS Manager and Management.

Documented information should be communicated to staff working in the company, who will be required to apply it during their working day.

7. GENERAL POLICY DEVELOPMENT

7.1 Introduction

This Information Security Policy is property of Libnova. It has **PRIVATE** classification, and its knowledge and execution are mandatory for all company workers.

7.2 Security Policy Development

7.2.1 General Information Security Policy

The management of Libnova, as a general company policy, guarantees the adequate management of the information security processed and/or hosted by the systems and services referred to in the scope area. To develop this policy, the management of Libnova is committed to:

- Ensure continuous confidentiality, integrity, and availability of the information by managing risks that may affect the information during normal operation.
- Perform periodical security risk analysis that allows maintaining an adequate overview of information security risks to which assets are exposed and develop the required mechanisms to reduce or eliminate discovered threats and risks.
- Provide with the necessary resources to develop all security mechanisms needed to decrease or eliminate risks and threats by implementing all required infrastructures and technologies to preserve information.
- Continuous improvement of the Information Security Management System to offer the best service for users and customers.
- Ensure the integration and compliance with the applicable ISMS requirements in the entity's processes.
- Ensure the establishment of this policy and all those resulting from risk analysis and information security objectives.
- Directing and supporting people to contribute to the effectiveness of the ISMS, promoting a culture in information security among the employees, training employees about information security requirements set by the company.
- Ensure that the ISMS achieve its intended results by performing periodical internal audits.

7.2.2 General Rules

As it has been established within the scope of this document, Security Policy applies to all staff working in Libnova and workers must know and accomplish it. In case of non-compliance, company might carry out different sanctions as specified inside **LIB-POL-020-Disciplinary Process**.

All staff, as Libnova workers that manages company information, must follow next procedures:

- Always protect information against non-authorized access or any other action that may cause information lack of confidentiality, integrity, or availability.
- Protect all information systems and networks against non-authorized access or use that may damage those systems or information that they contain or manage.
- It is a must knowing, accepting, and accomplishing this policy before accessing Libnova Information Systems.
- All employees are assigned to a specific area with the required permissions defined by their roles in the company. In case employees require extra access, an authorization must be addressed to their responsible and ISMS Management Team (generally by using the Support system)
- Additionally, all workers with specific responsibilities within scope indicated must ensure next rules accomplishment:
    - All development or implementation must incorporate mechanisms to ensure Information Security.
    - Secure and unique identification should be incorporated for the user's authentication.
    - Systems must be physically protected to guarantee information availability, integrity, and confidentiality.
    - It must exist a Business Continuity Plan to be able to restore in an orderly manner all systems that contain critical information. All workers involved in this plan must be trained on it.
    - Information confidentiality must be ensured, either if it is stored electronically or not.
- ISMS Manager is the responsible of managing Security Information.

7.2.3 Information Confidentiality

Information confidentiality can be defined as the warranty of information is not unproperly disclosed to entities or processes.

To preserve confidentiality:

- Information handled in the organization is confidential, owned by the company and must only be used for business purposes.

- All information by default, has a label with confidentiality level. In case one document is not marked by a confidentiality level, it will be considered as public.
- Users will protect information to which they have access against any action that can harm this information (such us modification, destruction…) or unauthorized disclosure.
- Information will be secure stored during an undefined period and will not be disclosed without owner authorization.
- Information will be saved in staff devices (such as laptops, mobiles, desktops, or storage devices) only during the time strictly necessary, and employees must upload it to approved media resources (Gdrive or company File Servers)
- It is strictly forbidden to use personal devices as USB, External Disks to keep company's data unless authorization is provided.
- Information will be stored only in approved media in the company (Local Servers, Gdrive) Paper format will be only used as temporary storage or in those cases that Public Administrations may require it. Information stored in paper will be scanned and safely kept in approved media.
- Confidential information managed by an employee cannot be shared under any circumstance outside the company or with other employees unless worker is authorized by information owner.

7.2.4 Physical access to Libnova facilities and working in secure areas

As part of the migration of our data center to EspacioRack, all physical assets transferred to their facilities are subject to the physical security measures established by EspacioRack. These measures are designed to ensure the integrity, confidentiality, and availability of the systems and data stored within their infrastructure.

7.2.5 Appropriate use of resources

Resources that company provides to workers, no matter the type of these resources, are only available to perform company processes. It is strictly forbidden:

- Use these resources to perform activities not related with company processes.
- Resources assigned to an employee are limited to business functions the employee oversees and cannot be shared without approval. It is not allowed to use these resources for personal use.
- The appropriation of information of the organization or its publication through any means without previous authorization.

- Try to scan or search systems vulnerabilities to explode them (except penetration testing and scan of vulnerabilities tasks)
- Use any system or application that do not belong to company infrastructure without authorization.
- Improper use of the company's resources such as playing games, mass mailings, attacks.
- Access to unauthorized, violent, racist, xenophobic, pornographic, or illegal content.
- Modifying any software installed by the company (e.g. Antivirus) or installing any kind of malware that may compromise information security or systems that contains it.
- Access to unauthorized information systems, as well as using any mechanism to break the system's security.
- Modify systems logs
- Try to unlock or decipher passwords, security mechanisms, encryption algorithms or any other security element.
- Store personal information inside company resources.

7.2.6 Malware Protection

To maintain systems free of malware or any other software that might affect information:

- Antivirus software must be installed in all servers and computers where it is possible.
- All security updates will be installed automatically or analyzed (Zoho)
- Antivirus will be always enabled.
- In those devices where use of an antivirus depends on the company, a centralized antivirus has been installed. Antivirus is based on a control panel where an administrator can control antivirus software's behavior. Only infrastructure and Management staff have authorization to access this control panel.
- In those services where antivirus installation or malware protection does not depend on the Company and is an external provider who guarantees services security, the Company accepts that the external provider protection is enough but

keeps a backup of the service just in case the provider is affected by any kind of virus or malware.

- All software used inside the company must be licensed or have GNU GPL (e.g. Linux or Unix-based components)
- Use of cracks or non-authorized software is strictly forbidden.
- Uninstalling or manipulating antivirus software (e.g. by stopping services, modifying critical configuration files…) is strictly forbidden.
- In case any malware is detected, ISMS Team will be informed, and system will be disconnected and isolated until problem is fixed.

7.2.7 Information exchange and sharing

Next rules must be followed:

- Users must never hide or manipulate their identity to access restricted information.
- Information distribution will be always performed by authorized and approved media (Gdrive, File Servers) when possible. If distribution is performed using paper, documents will be properly and safely stored during the minimal time they require to be scanned and stored in the right media. Use of encryption tools like AESEncrypt is highly recommended.

Next actions when sharing information are strictly forbidden:

- Send or receive information or material with copyright without authorization or breaking the laws.
- Send or receive information with sexual, pornographic, violent, racist … content or any other that may offend or illegal.
- Send confidential information or files to third parties without authorization.
- Provide with personal information under any circumstance except if proper authorization is provided and only by staff working in HR.
- In general, all activities that may harm company reputation through any media.

7.2.8 Mail proper use

Mail address is provided by the company and is understood as a working tool required for the normal workday.

Next criteria are assumed:

- Each company worker that may require an email address will be provided with it and will be the only user and responsible of this email account.
- Email will not be used under any circumstance except for working purposes and never as a personal tool or to send or receive improper content.
- Workers cannot use email address to send massive mails, publicity, …
- Email cannot be used to transfer confidential information unless authorization is provided, requester is properly identified, and information is encrypted.
- Business mail will not be forwarded to personal accounts without authorization.
- A secure password will be used to access the email.
- Authenticity of emails will be suspected by default. When a message presents changes in appearance, contains a "call to action" that urges us, invites, or requests us to do something unusual or requires credentials to access a website or application (bank account, ERP, ...) this mail will be discarded, and **ISMS Manager** will be informed (**support@libnova.com**)
- We will identify the sender before opening an email. If it is suspected that the sender has been impersonated, we will contact the sender by other means (e.g., by phone) before opening the mail.
- Attachments will be analyzed before opening. If their authenticity is suspected, content will not be either downloaded not opened. Contact **ISMS Manager** if you have any doubt.
- The links included in the emails will be checked before accessing. Contact **ISMS Manager** in case of any doubt.
- Spam mail will not be answered. Mail manager will be prompted to add the sender to a spam list and the mail will be deleted.
- Mails sent to multiple addresses will be sent with a BCC.
- As far as possible, accessing corporate mail, if connected to public (probably unsecured) networks, will be avoided.

7.2.9 Internet Connectivity

Internet use must be controlled with next rules:

- Internet is a working tool. All activities that require internet access must be related with company processes. Users must not navigate through sites not related with their normal workday.

- Access to internet and navigation will be performed through company infrastructures.

- Using internet to download any kind of information not related with business is strictly forbidden as well as using software as P2P and Torrents.

7.2.10 Users responsibility

All users must observe next responsibilities:

- Workplace must be kept clean and orderly.
- Eating and drinking in the workplace is not allowed.
- Each user will be responsible of its accesses, users, and passwords. Workers must never and under any circumstance share their user, passwords, and accesses with any other person.
- Users will be responsible of all actions recorded with their user in the systems (logs)
- Users must fulfil passwords use and protection requirements.
- Workers must ensure that computers are properly protected when they are unattended, as well as clean desktop policy, to protect documents, reports and any other media that may keep critical information, avoiding information unauthorized access or data integrity degradation.
- Information that is not being used must be stored in protected archivers.
- Information that is in use along the workday must be stored when employee leaves the workplace.
- When an employee leaves the workplace, the screen must be locked.
- Screen locker must be automatically active after 12 minutes of inactivity inside computer under domain.
- When printing or scanning any critical information, the document must be collected immediately.
- In case of security incident, employees must inform to ISMS Manager (support@libnova.com) or if they have any question regarding security matters.

7.2.11 Users and passwords

All employees are responsible to ensure that data, applications, and resources are used only for company processes matter. Systems are protected by a set of different protection mechanisms, being the main users and passwords protection. Regarding users and passwords, employees must ensure that:

- When an employee receives user and password to company systems, it is considered that Security Policy is accepted formally.
- Users must guarantee that their credentials remain confidential.
- Changing passwords without authorization is strictly forbidden.
- Passwords should mix numbers, letters, and special characters.
- Users must never use credentials of another worker even if they have been authorized to use them.
- User will only have access to the resources they need for their workday. Any other access must be requested to asset's owner and ISMS Manager.
- It is strictly forbidden to share personnel users and passwords or keep them in an unsafe location, being Bitwarden software the official passwords keeper.
- The Company uses Bitwarden (that provides a strong algorithm and checks whether this password is used in known passwords databases) to generate random passwords for new systems to comply with this policy and to share passwords among workers.
- If employees suspect that their credentials are being used by other user, they must modify credentials access and inform ISMS Manager.
- Devices inside Domain can be controlled by DC polices and fulfils the following requirements:
    - Passwords will have at least 6 characters.
    - Passwords must be changed every 200 days.
    - Two last passwords remember.
-

7.2.12 Software

Regarding software, next rules must be followed:

- All staff must only work with authorized versions of software, provided by the company.
- It is strictly forbidden the use of illegal software or modify legal software by using cracks.

- In case of any doubt regarding software (use or installation), employees can ask for help to ISMS Manager (support@libnova.com)

7.2.13 Network connection

Next rules have been determined for networking:

- Only company network infrastructure must be used for the normal workday.
- In case of punctual connection personnel devices can be used.
- Personnel network devices cannot be installed in the company infrastructure unless authorization is requested to ISMS Manager.

7.2.14 Access Control

Next rules must be followed to manage access control:

7.2.14.1 Physical Facilities Access

- Physical access must be requested in the main entrance, being necessary that people accessing facilities request an authorization managed by ISMS Manager or Management.
- Physical access can be revoked immediately if external staff do not accomplish company or supervisor instructions.
- Any external person must be companied by ISMS Manager, Management, Administration staff or resource access owner during tasks developed inside Libnova facilities.
- Physical access to infrastructures is controlled through a set of protection mechanisms (numeric keyboard, keys, and card readers)
- All infrastructure assets are protected against environment threats or disaster by using mechanisms such as fire extinguishing systems, temperature and humidity control, mechanical pollution, and alarms.
- All employees that detect a system failure in systems used to mitigate fire, temperature, humidity, alarm, or pollution must inform ISMS Manager or Management.

7.2.14.2 Systems Access

- Access is provided only when authorization has been confirmed.
- When tasks or roles that required access privileges end or change, authorization must be removed or changed accordingly.

- A record of access guaranteed is kept and reviewed.
- Access to all systems will be protected as a first security level by a username and password that are stored in **Bitwarden** that fulfils ISO27001 requirements. As a second security level, where available, a system of roles is established to guarantee a more controlled access (e.g. Administration Tools)
- Local assets (and VMs running inside them) are located inside the Company's Data Centre, hence, protected with the facilities protection mechanisms.
- External or cloud assets are protected by the provider's mechanisms. The Company transfers and accepts external access control mechanisms (services run inside secure and trusted data centers as company's providers comply with ISO27001 certification).
- Servers and computers inside local infrastructure are connected to a Domain (inherit Domain control and security mechanisms) except Test servers and Production Image Treatment servers.

7.2.15 Security Incidents

If any worker detects an incident related with Information Security:

- Worker must inform ISMS Manager as soon as incident is detected (using support@libnova.com)

7.2.16 Backup

Company sets backup mechanisms, fully developed inside **LIB-POL-070-Backup** policy.

7.2.17 Updates

The Company has set the following norms for update and maintenance:

- The infrastructure department is in charge to perform all preventive and corrective actions, and updates, except those that depend on external providers (e.g. ADMINISTRATION TOOL) or Development.
- Software and Hardware components have a preventive maintenance that guarantees their proper functioning at operating system level, programs, and hardware.
- Servers update and maintenance operations (no matter whether they are physical or virtualized or if they are local or cloud hosted) consists of:

- Operating system is manually updated following next strategy: Updates recommended by supplier are downloaded daily, but only updates that do not require a restart are installed, being manually update those that require a restart.

- Antivirus is daily updated.

- External tools in charge of infrastructure team are used to keep the servers updated and safe (Zoho)

7.2.18 Logs

The Company sets the following general norms for this policy:

- To have all logs with a correct data and time, clocks of all computers inside the domain are synchronized to a single reference time source (Domain Controller)

- In all application where log can be activated, log is kept.

- Firewall keep a log of activity and access that is exported to FortiGate cloud.

- Regarding servers:

  - All servers considered critical have an activity log activated, no matter if they are physical or virtual or if they are local or cloud hosted.

  - Operating system logs are stored inside each asset.

  - Servers hosted in external suppliers have their own log to which company has access.

  - Records are periodically reviewed during audits to check errors and intrusions.

  - As logs are kept inside servers, logs are protected from degradation by restoring servers from backup.

7.2.20 Classification and Labelling Information

Information managed within the company's environment must be classified according to its criticality and value to avoid information leaks due to staff neglect or carelessness. The Company has set certain norms and best practices to classify its assets that will be explained inside this policy.

- The Company's information is classified according to the kind of document and department that may access it.

- Documents are placed and stored inside the proper folders according point above.
- Main storage folders are Gdrive and local folders shared in File System Server.
- Documents must be labelled according to their confidentiality, being marked as **Confidential** those that cannot be published outside the company.
- Only personnel of each department can access documentation, being documents protected by:
    - Local Folders: Access is granted by Domain User accounts credentials.
    - Gdrive: Gdrive Accounts.

7.2.21 Teleworking

Teleworking is an option for employees in the Company. Due to the Company's activity, extra threats may affect data information. These threats have been analyzed, resulting in a set of protection mechanisms that must be applied.

- Teleworkers must be aware that, by teleworking, they must observe the same rules that apply in the office. Furthermore, teleworkers must be even more careful as they work with internal and critical documentation, but out of office.
- All devices used to telework must be protected by user and password
- Access to company resources will be always carried out through secure protocols (VPN or TeamViewer)
- Wire networks are the preferred connection method. In case Ethernet is not available only trusted WI-FI or 3G/4G connections will be used being strictly forbidden connect resources to untrusted or unknown WIFI networks.
- Employees that telework, must secure their router with all the mechanism offered by the device, such us MAC filter, disable SSID broadcast, strong WI-FI and admin password. Router features must be also kept protected by observing a maintenance policy (e.g. updating firmware) In case of any doubt they can contact **ISMS Manager.**

7.2.22 Cryptography

Regarding encryption requirements, users must comply with:

- Users should ensure that encryption meets or exceeds AES-128bit when dealing with critical data.
- AES-256 bit should be use where available.
- AES Encrypt is the preferred software to encrypt critical assets in the normal workday.
- Laptops taken out of the office and considered critical are encrypted with **Bitlocker**
- Where no encryption option is available, using **7-zip** software encryption tool as alternative way to encrypt sensitive data, is allowed (Note: AES-256 compliant)
- OFF-SITE storage: external providers fulfil ISO27001.
- Data transfer from external sources are encrypted, either by provider mechanisms (e.g. google that accomplish ISO27001 or SyncBackPro) or by FTPS (Data Vault Backups) or any other mechanism (such as PBS)
- Web applications use https with a self-signed certificate to secure connection by default.

7.2.23 Information Transfer

The following general guidelines must be observed before transferring any kind of information:

- Before transferring sensitive data, the responsible must obtain the corresponding authorization.
- Workers must not assume anyone that asks for information is entitled to access it.
- When dealing with third parties, we must consider whether there are sharing agreements or contracts that cover the transfer of data before transferring the information.
- Do not provide more information than necessary (e.g. do not provide a whole document if only a part is required)
- Before sending any sensitive data, identity of requester must be verified (e.g. asking for a confirmation mail, trusted email, personal meeting…)
- If there is any doubt about the requester's identity, **DO NOT** provide the requested information and contact with **ISMS Manager**.
- Email

- Subject line must not reveal the full contents of messages or disclose any sensitive personal data.
- Information sent must be enclosed in an attachment if possible.
- When sending attached files with sensitive data within an email, they must be protected by password or encrypted.

- Gdrive
  - Sensitive data can only be shared via Gdrive with collaborators that have been properly identified as **Trusted**, that is, people inside the Company and third parties than can ensure they are who they say to be.
- Removable Storage Devices
  - Sensitive data must be encrypted before sending Removable Devices to customers.
- Phone: Phone calls may be monitored or intercepted, either deliberately or accidentally, so:
  - Sensitive data must not be transferred or discussed over the phone unless identity of recipient has been confirmed.
  - Do not leave confidential messages or include any personal data within voicemail.
  - When listening to messages, ensure you do not play them in any areas where can be overheard.

7.2.24 Media storage

As a Digital Preservation company, Libnova workers must deal with a lot of storage media such as Hard Drives or USB.

Within this section the company defines a set of general norms that must be performed by all employees regarding all support devices, whether these are electronical devices (External Disks, USB…) or any other kind of asset that may support information (e.g. paper):

- Information supported by paper must be stored in secured archivers protected by a strong protection mechanism (e.g. keys or lockers)
- If information contained in papers is critical it must be digitized and stored in company servers

- Once one document is determined not to be used anymore and a digitized copy is safely kept (if so established) then it can be destroyed (e.g. paper destroyer)

- Personal data is not allowed to be stored within company's resources.

- Before retiring any data media an authorization is required from the Production department. A register of storage devices is maintained accordingly.

- During data media transportation, the authorized employee must observe a set of best practices, such as not leaving the media unattended, not leaving it to external staff or taking care of the devices to prevent accidents (crashes, fire, water…). Staff is trained in these best practices thanks to specific **trainings.**

- When an employee returns one storage device all information inside will be analyzed to determine whether a backup in company servers is needed or not. In the case a backup is required, it will be performed in company servers, being the device immediately formatted once backup is done (e.g. USB, external drives…) or stored or destroyed (e.g. CD-ROM)

- Obsolete devices (either by aging, or technology obsolescence) as well as damaged ones (broken devices, malfunctioning…) will be low-level formatted (if possible) and immediately physically destroyed.

- Storage devices with sensitive information must be properly backed up.

- Antiviruses must be executed over external and internal devices.

Destruction of devices or documents with critical information will be destroyed by a third-part company that ensures the complete and confidential destruction. This company sends administration department a certificate about destruction.

7.2.25 Portable Devices

Employees that may use any kind of portable device (such as mobile phones, laptops, or storage devices) must be aware of the information that is stored inside them in order to protect the devices against theft, loss or accidents.

To help employees to protect these devices, the Company sets the following mandatory guidelines:

1. All employees that own a portable device (mobile phones, laptops, or storage) must keep it controlled at physical level to avoid theft, loss, accidents (water, fire, fell, chemical products…)

2. Access control to devices will be controlled.

3. Manipulating hardware or software is strictly prohibited.

4. Prior to retiring a disk drive, an authorization is required.
5. A register of assigned equipment is maintained by Administration as well as an inventory of disks maintained by Production.
6. Devices must be protected with a strong enough password (laptops) and a PIN or Partner (mobiles)
7. Devices must be protected with an antivirus and malware.
8. Devices with critical information must be backed up.
9. Corporate information will not be stored in the storage devices or mobiles unless it is strictly necessary. Once information has been used it will be uploaded to company servers or Gdrive to keep it safe.
10. Devices will be periodically updated and reviewed by infrastructure personnel.
11. Ethernet is the preferred connection type for laptops. If cable connection is not available only trusted Wi-Fi will be used. If Wi-Fi is not secure or trusted, 3G/4G mobile connection will be used.
12. 3G/4G is the preferred connection for mobiles. If it is not available or a huge amount of data must be downloaded only Trusted Wi-Fi can be used (Private, not public)
13. Wi-Fi and Bluetooth will be turned off unless necessary.
14. In case there is a suspicion of virus, the user must contact the **ISMS Manager** to obtain instructions on how proceed.
15. In case of loss, theft or accident, the user will contact the **ISMS Manager** to get instructions.
16. Automatic lock for computers under AD is set.
17. Automatic lock is set within mobile phones.

7.2.26 Communication and awareness

To keep all employees informed of changes in ISMS, incidents that have affected or may affect the company, and to help them become aware of the ISMS, the company has determined the following set of rules:

- ISMS manager (or management) is the responsible to communicate workers about any incident or improvement regarding Information Security.

- ISMS manager (or management) will decide who will be the audience of communications keeping in mind restrictions and information usability.
- Email is the preferred method to publish basic communications (e.g. virus alerts)
- More complex communications (e.g. new policies or procedures, security incidents that must be treated in a proper way, set of new rules or policies to be applied) will be dealt with periodical meetings, trainings that will be documented.
- Communications will be performed periodically (continuous communication) and events based.

7.2.27 Extortion and Social Engineering

Extortion consists of forcing a person, using violence or intimidation, to carry out or omit a legal act or legal business for profit and with the intention of producing a damage.

As part of the Security Policy, employees are trained about extortion (what it is, how to fight against it, …), but as action policy these are the steps that must be followed in case an employee is victim of extortion:

- Never give up to extortion.
- Inform the direct superior about the fact to take proper actions.

Social engineering consists of obtaining confidential or critical information by manipulating legitimate users.

As part of the Security Policy, employees are trained about social engineering methods and how to fight against it, but as action policy these are the steps that must be followed in case an employee is victim of social engineering:

- Never provide any kind of information to untrusted people or systems.
- In case information has been provided, inform immediately to the support department in order to avoid intrusions.

7.2.28 Incident Management

- A Security event is defined as a set of non-expected incidents with a high probability of occurrence that may compromise business operation and threat information security.
- The Company has appointed a Security Responsible (**ISMS Manager**) that oversees managing security events.
- Employees must send **Security Event Template** (either Spanish or English, as preferred) filled with as much information as possible. In case template cannot be fulfilled, worker can inform ISMS Manager by any media available (mail, phone or whatever)
- The ISMS Manager will collect all Security Incidents, classifying them according to its characteristics and will solve them. In case template has not been sent by worker, ISMS Manager will create a new one and will store it properly.
- Incidents and their solution will be documented and stored for future use and audited.
- The Company is in contact with interest groups (INCIBE and HISPASEC) to improve ISMS.
- In case the event's severity is critical or could not be solved by the Security Responsible, he will inform authorities (Unidad de Delitos Telemáticos de la Guardia Civil and INCIBE)

7.2.29 Suppliers

- The Company considers critical suppliers those who store critical business information and customers' data.
- To verify a supplier is safe enough, the company has established that it must comply with **at least** one of these two requisites:
    - It accomplishes ISO27001 norm (or equivalent like NIST Cybersecurity Framework)
    - In case the supplier could not provide a valid and recognized certification, it must comply with some other security mechanisms as:
        - Infrastructure supported by a third-party that is ISO27001 (or equivalent) certified.
        - Communication Encryption (e.g. google encrypts all data transfers)
        - Two-factor authentication
- Here follows a list of suppliers considered as critical by the company:

-

SUPPLIER	PROVIDES	PROTECTION MECHANISM
GOOGLE	MAIL	ISO27001
	FILE STORAGE	ISO27001
AMAZON	FILE STORAGE	ISO27001
BITWARDEN	PASSWORD STORAGE	Supported by a third party (Azure)
VOXILITY	CLOUD SERVER FARM	Supported by a third party (Data Center ISO27001 Compliance)[1]
OVH	CLOUD SERVER FARM	ISO27001
DIGITAL OCEAN	CLOUD SERVER FARM	ISO27001
AZURE	FILE STORAGE	ISO27001
ARSYS	WEB SERVERS	ISO27001
	FILE STORAGE	ISO27001

7.2.30 Change management

The Company considers a change as any request for implementing a new functionality, interruption of service and repair or removal of existing functionality. They can be scheduled or unscheduled.

- Every change to any resource (Operating Systems, hardware, networks, applications, facilities…) must follow this policy.
- Support, Infrastructures and Management departments must be aware of any change that might be carried on.
- In case any of the workers require any change, they must inform the **ISMS Manager**.

[1] *Data Centers which store our servers are ISO27001 compliance (https://www.interxion.com/why-interxion/awards-accreditations-memberships, https://www.digitalrealty.com/data-center-solutions/security-compliance/compliance, https://www.coresite.com/data-centers/data-center-design/compliance)*

- The ISMS Manager will manage the incident deciding whether the change can be directly performed or not and if any other department assistance may be required (Infrastructures or Management)
- If possible, all requests will be scheduled to a low-activity frame time.
- A Change Management Log must be maintained.
- Proper testing should be performed before any change.

7.2.31 Network Services

Network services protection is a Must inside the Company. This policy deals with network configuration instructions to make Company networks and transactions secure.

- The Company owns a set of physical devices that use networks in a secure way (Routers, firewalls, switches…). All devices that support local network are protected against unauthorized access.
- Local network infrastructure is controlled and checked periodically by the infrastructure team in order to make it secure (checking accesses, logs and incidents that may affect the system)
- Staff accessing local resources uses VPN thought Remote Desktop connections.
- Network traffic to external providers (Google, Amazon…) for backup and storage purposes is performed through protection mechanisms of the providers that includes information strong encryption (e.g. TLS – 128 bits AES) as they comply with ISO27001
- None of the Company's software services uses public network as they all work in local mode.

7.2.32 Payment

Services that are hired to external providers must be reviewed and dated to avoid lack of payment that may imply a shutdown of the services provided.

- Services are configured to send a mail to services@libnova.com in order to inform about any remarkable information about the service (expiration date included).
- Each service has an owner described in the document above. Despite Administration and Support team reviewing and updating this document periodically, owners are responsible of taking care of each service that they are responsible.

- In case one service is near its expiration date, the owner will verify whether service is still needed or not. Administration department will ask the responsible if the service is still needed in case the owner does not contact with them before. In case the service is still required, administration will proceed with the payment.

7.2.33 Systems Monitoring

Critical systems must be monitored through Zabbix services (local and external infrastructures) and Veeam Alarms (local infrastructures) as reflected in **LIB-POL-100-Monitoring.**

7.2.34 Permissions Assignment

After permissions assignment for a user, these permissions must be reviewed before advising users they can work. In addition, an extra reviewing must be completed with the rest of the users already assigned.

Once reviewed, include new assignments into Netbox.

7.3 Control and monitoring

To ensure that company resources and procedures are being used properly, Libnova will verify either periodically or when security requires this verification, the proper use of company resources. In case some worker does not accomplish this policy, it will be informed about errors found and will be trained to solve them or to apply proper procedures in case of worker ignorance.

In case worker has violated this policy knowing that the actions performed were prohibited or with the intention of damage the company, sanctions will be carried out.

7.4 Security Policy Update

Security information is a living matter that changes every day and security policy cannot be consequently a static document. Company must update this policy periodically or when security information procedures, assets or threats change and will be also in charge of informing all staff about policy changes.

This policy is public for all employees and stored in a resource where all staff can access. Different versions are updated within this resource and when a major change is performed, ISMS Manager oversees explain new policy and ensure all staff knows and understand this document and updates.