Information security policy for third parties

Objective

The purpose of this policy is to establish information security requirements for Zelestra Group third parties who can access information, information systems, operation assets or resources of Zelestra during their relationship with the company.

In this regard, third parties to which this security document is provided have the responsibility of communicating it to their personnel assigned to Zelestra and obtaining their written commitment. The policy reflects legal and ethical requirements, both for the informal activities of the employees of the third parties that work for Zelestra, and for the conduct of their operations.

Suppliers and third parties that provide services or supplies to Zelestra must comply with the security measures specified in this document.

Provision of services or supplies

Third parties may only perform activities for Zelestra that are covered by the respective contract for the provision of services or supplies. The activities carried out by the personnel of the supplier companies will be made in accordance with the rules of the corresponding service or supply contract, as well as with the rules and procedures established between Zelestra and the respective supplier.

All external personnel working for Zelestra must comply with the organization's security policies. In the event of non-compliance with any of these obligations, Zelestra reserves the right to block the personnel who have committed the infringement, as well as to apply the corresponding sanctions in relation to the contracted company, which could even lead to the termination of current contracts with said company.

The supplier company must ensure that all its personnel receive the appropriate training to carry out the service provided, both in specific terms related to the activity associated with the provision of the service, and in general terms of information security. To this end, the provider company must guarantee, at least, that all personnel involved in the service or supply know and agree to comply with the established security policies.

Any exchange of information between Zelestra and the supplier companies will be understood to be carried out within the framework established by the corresponding service provision contract. Therefore, such information must not be used outside of said framework or for purposes other than those associated with said contract.

In general, assets include all forms of information, as well as the people and technology that support information/operation processes.

In any project or system design, as well as in the supply of communication equipment or its configuration, the minimum cybersecurity requirements attached to the contract must be considered

Information confidentiality

External staff who have access to Zelestra information must consider such information, by default, to be confidential. Only information to which the supplier has had access through the means of public communication of information provided for this purpose by Zelestra may be considered as non-confidential information. To this end:

- Unauthorized disclosure, modification and destruction, or misuse of the information will be avoided, regardless of the medium in which it is contained.
- Confidential information will not be transmitted without proper authorization and will be kept strictly confidential.
- The number of reports in paper format that contain confidential information will be minimized and kept in a safe place and out of the reach of third parties.
- In relation to the use of contact books, staff will only enter personal data such as name and surname, the functions or positions held, as well as the postal or electronic address and professional telephone number.
- No collaborator in projects, specific works, etc., must possess, for uses not within their responsibility, any material or information owned or trusted by Zelestra.

The present Policy was approved by the Chief Digital Officer, member of Senior Leader Team, on December 03rd, 2024 and it came into effect upon approval.

- In the event that, for reasons directly related to the job, the employee of the service providing company comes into possession of confidential information contained in any type of medium, it must be understood that such possession is strictly temporary, with an obligation of secrecy and without this conferring any right of possession, ownership or copy of such information.
- The employee must return the aforementioned media(s) immediately after the completion of the tasks that have led to the temporary use of the same and, in any case, at the end of the relationship with Zelestra. The continued use of the information in any format or medium other than that and without the knowledge of Zelestra will not imply, in any case, a modification of this point.

All these obligations will remain in effect after the end of the activities carried out by the external staff. Failure to comply with these obligations may constitute an offence of disclosure of secrets, which may give rise to the right to claim compensation.

To guarantee the security of Personal Data, staff belonging to supplier companies must take into account the following rules of action, in addition to the considerations already mentioned:

- Staff may only create files containing personal data when it is necessary for the performance of their work. These files must be destroyed when they are no longer useful for the purpose for which they were created.
- No personal data will be stored on the local disk drives of the user PC workstations.
- The transfer of computer media that contains personal data must only be authorized by the person responsible and in accordance with this policy.
- Computer media containing personal data must be inventoried and stored in a place with access restricted to authorized personnel.

Information distribution

The distribution of information, whether in digital or printed format, will be carried out using the resources established in the contract for the provision of services or supplies or with adherence to this policy, exclusively for the purpose of facilitating the functions associated with said contract. Zelestra reserves the right to implement control, registration and audit measures on these communication resources, depending on the identified risks and the scope of the service or operations.

Regarding the exchange of information within the framework of the service provision contract, the following shall be considered as unauthorized activities:

- Disguise or manipulate the identity of any person under any circumstances.
- Transmit or receive copyrighted material in violation of the Intellectual Property Protection Law.
- Transmit or receive any offensive material, discriminatory statements, or other types of statements or messages that may be considered offensive or illegal.
- Transmit or receive games and/or applications not related to the business.
- Participate in online activities, such as newsgroups or games, that are not directly related to the service provided.
- Carry out any activity on the Internet or other media that may harm the good reputation of Zelestra.
- In addition, any disclosure of information containing personal data, whether on computer, paper or e-mail, must only be made by authorized staff with due permission, in compliance with applicable laws.

Appropriate use of resources

The supplier agrees to use the assigned resources to provide the service in accordance with the established conditions.

The resources made available to external staff by Zelestra, regardless of their nature (computer equipment, data, software, networks, communication systems, etc.), are available exclusively to comply with the obligations and operational purposes established in the service provision agreements. Zelestra reserves the right to implement control and audit mechanisms that verify the proper use of such resources.

Any file introduced on the network or on any equipment connected to it, whether through automated means, the Internet, e-mail or other means, must comply with the requirements established in this policy, especially with regard to intellectual property, protection of personal data and virus control.

Upon termination of the contract, all physical assets must be returned to Zelestra, and information assets must be destroyed or returned without undue delay.

It is expressly prohibited:

- The use of resources provided by Zelestra for activities unrelated to the purpose of the service.
- Connecting equipment and/or applications to the network without the knowledge and approval of Zelestra.
- The introduction of obscene, threatening, immoral or offensive content into the company's information systems or network.
- The intentional introduction of any type of malware, logical device, physical device or any other script that may cause or is likely to cause alterations or damage to computer resources.
- Attempt to obtain rights or access other than those explicitly assigned.
- Attempt to distort or alter the activity logs of information systems.
- Attempt to decrypt without explicit authorization the encryption keys, systems or algorithms and any other security element used in telematics processes.
- Own, develop or run programs that may interfere with the work of other users or damage or alter the organization's computing resources.
- Attempt to destroy, alter, disable or damage the data, programs or electronic documents under the responsibility of Zelestra.
- Install on any Zelestra system any software that has not been previously authorized, whether licensed or freely distributed.

User responsibilities

Service providers must ensure that all personnel performing work for Zelestra comply with the following basic principles in their activity:

- Each person with access to Zelestra's information is responsible for the activities carried out with their user identifier and for everything derived from it. Therefore, it is essential that each person keeps the authentication systems associated with their user ID under control, ensuring that the associated password is known only to the user and not revealed to other staff members under any circumstances.
- Users should not use someone else's user ID, even if they have the owner's permission.
- Users must know and apply the established requirements in relation to the information handled.

Anyone with access to information under Zelestra's responsibility must follow the following considerations regarding password management:

- Select quality passwords.
- Ask for a password change whenever there is a possible indication of compromise of the system or passwords.
- Avoid including passwords in automated login processes, such as those stored in a function key or macro.
- Report any security incident related to the passwords such as loss, theft, or indication of loss of confidentiality.

Anyone with access to Zelestra information must ensure that equipment is protected when it is left unattended. At least the following clean desk measures should be adhered to, in order to protect paper documents and removable storage devices and reduce the risks of unauthorized access, loss and damage to information, both during normal business hours and outside of them:

- Store paper documents and computer media containing Zelestra information in secure furniture when not in use, especially outside working hours.
- Do not leave equipment assigned to critical Zelestra functions unattended and block access to it when necessary and the equipment is not being attended to.
- Protect information receiving and sending points (postal mail, scanning and fax machines) and duplication equipment (photocopiers, fax machines and scanners) whenever Zelestra information is used. The reproduction or sending of information using these devices will be the responsibility of the user.
- Immediately remove any confidential information once it has been printed.

User devices

Service providers must ensure that all computer equipment used by users to access Zelestra information complies with the following measures:

- When a workstation is left unattended for a short period of time, the system must automatically lock it.
- No user computer should have tools that can violate the security system and authorizations established in the organization's systems.
- User equipment must be maintained in accordance with the manufacturer's specifications.
- All user computers should be properly protected against malware, following these guidelines:
    - Antivirus software should be installed and used to reduce operational risk associated with viruses and other malicious software.
    - They must be kept up to date with the latest security updates available.
    - Antivirus software must always be enabled and properly updated.

Special attention must be paid to the security of all mobile devices used by users that contain Zelestra information or allow access to it in any way. This is achieved through the following measures:

- Verify that mobile devices do not contain more Zelestra information than is strictly necessary.
- Apply access controls to the information stored on such devices.
- Minimize access to information in the presence of persons not authorized to the service provided.
- Take additional precautions outside Zelestra facilities to prevent third parties from accidentally accessing confidential information

Equipment management

In case that Zelestra supplies equipment or other information assets, it is important for service providers to ensure optimal management of those used for the provision of services. To this end, it is essential to comply with the following measures:

- The provider must maintain an updated list of the equipment and users associated with such assets, or the designated responsible parties in case the assets are not for the exclusive use of one person. This list will be available to Zelestra at any time it is required.
- If a supplier wishes to remove a piece of equipment from the Zelestra asset list, they must return the asset so that its removal can be properly managed.
- If a supplier terminates the provision of the service, they must return all equipment provided in accordance with the corresponding service provision contracts. Only in the case of information assets, the provider may carry out their secure deletion, as long as they notify Zelestra of such deletion.

Access controls to networks and associated services

The access criteria meet the following guidelines:

- Users will only have access to authorized networks, network services and information assets based on their job responsibilities. Consequently, the supplier company must inform Zelestra in the event of any employee leaving or termination so that their access can be eliminated.
- It is required to obtain prior authorization to access networks and services.
- Security requires that access to networks and network services be constantly monitored.

If Zelestra domain accounts are created associated with providers, these will be kept for the time necessary to guarantee the traceability of the activity records linked with those accounts.

It is the responsibility of both parties to guarantee the security of the information, which implies the obligation to immediately report any incident or anomaly related to the security of the information systems/assets in operation that may be detected, such as viruses, deterioration of media, unauthorized access by third parties, among others. These communications must be made through the established communication channels.

It is crucial to protect the information flows between Zelestra's information systems and those of the provider, and it is mandatory to report any security incident that may affect the service provided.

Non-compliance

If a violation of the provisions of this policy is identified, Zelestra reserves the right to take the measures they deem appropriate in relation to the third party. These measures may include the termination of existing contracts with such supplier.

Update of the security requirements

Due to the evolution of technology, security threats and new legal contributions on the subject, Zelestra reserves the right to modify these requirements when necessary. Changes made will be disclosed to all third parties to which they apply using the means considered appropriate.

It is the responsibility of each company to ensure that its staff read and understand the latest Zelestra requirements.

Monitoring system

The approval of the Information security policy for third parties is the responsibility of Zelestra's Digitalization and Cybersecurity area, through its Chief Digital Officer, who is a member and part of the company's Senior Leader Team, which, either directly or through the Information Security Committee, will supervise it, ensure its compliance and periodically review it for its continuous suitability.

The Company will establish an internal monitoring system that allows the correct implementation of the Policy at all organizational levels.

Communication and stakeholder engagement

This Policy is communicated and understood within Zelestra and is available on the information and communication channels that the Company makes available to all its stakeholders.

This Policy is publicly available on the Zelestra website.

In order to make it easier for any person to confidentially and anonymously report any breach of the principles described in this Policy, Zelestra's Ethics Line (https://zelestra.integrityline.com/) guarantees independence, impartiality and the absence of conflicts of interest throughout the process of receiving, processing and resolving such reports.

Scope

This policy applies to all activities carried out by personnel who provide services or supplies to any of the Zelestra group companies but who belong to other companies, linked through the corresponding contract for the provision of services or supplies, regardless of the type of service provided, and that in the development of their functions may have access to information, information systems, assets in operation or resources of Zelestra.

The present Policy was approved by the Chief Digital Officer, member of Senior Leader Team, on December 03rd, 2024 and it came into effect upon approval.