Supplier Information Security

Edition: 1

indra

Contents

1 Purpose

The main objective of the Supplier Information Security Manual is to mitigate possible risks associated with access to Indra's information, information systems or resources by service providers, regardless of the type of service they provide and their relationship with Indra (legal, contractual or of any other non-employment type) with the aim of protecting the confidentiality, integrity and availability of information belonging to Indra and its customers.

Indra reserves the right to amend this policy whenever necessary. Any changes made to it shall be disseminated to all the service supplier companies to which it applies, using the means considered suitable. It is the responsibility of each supplier company to guarantee that all members of its staff have read and understood Indra's most recent security policies and obtain their commitment to comply with and respect these rules.

Should any of these obligations not be met, Indra reserves the right to adopt the punitive measures it deems appropriate in relation to the contracted company, which may result in the resolution of any current contracts with said company.

2 General security principles

Whenever required, service providers must provide Indra with a list of the people, profiles, functions and responsibilities associated with the provided service and report any changes (new hires, terminations, replacements or changes in functions or responsibilities) to this relationship.

Service providers must ensure that all their staff are suitably trained in the development of the provided service, both on the specific level in matters corresponding to the activity associated with the provision of the service and generally in relation to information security matters.

Service providers must at least ensure that all staff associated with the service are familiar with and committed to compliance with the provisions of this policy. Indra may request evidence of the corresponding information process at any moment.

Service providers must allow Indra to perform security audits on request, collaborating with the audit team and facilitating all evidence and records requested of them.

The scope and depth of each audit will be expressly established by Indra in each case. Audits will be undertaken in accordance with the schedule agreed in each case with the supplier of the service.

Indra reserves the right to perform additional extraordinary audits, provided that there are specific causes to justify them.

2.1 Information confidentiality

All information, documentation, programs and/or applications, methods, organization, business strategies and activities related to Indra or its business to which service providers may have access in the course of the provision of the service shall be considered to be confidential information. Accordingly, this information must always be accessed, exchanged and processed in accordance with the planned purposes described in the service provision contract and maintaining the corresponding obligation to secrecy throughout the duration of the service and following the conclusion of the relationship with Indra.

All resources and information that may have been accessed by the provider of the service or that may have been prepared, modified or copied for the correct performance of the service must be returned to Indra upon completion of the service. Indra may request the secure deletion of any devices that have had access to its information.

2.2 Intellectual Property

Compliance with legal restrictions on the use of all materials protected by intellectual property regulations must be guaranteed. Service providers may only use materials authorized by Indra for the development of their functions. The use of IT programs without their corresponding licenses in Indra's information systems is strictly prohibited.

Similarly, the use, reproduction, transfer, transformation or public communication of any type of work or invention protected by intellectual property is prohibited without due authorization in writing.

Indra shall only authorize the use of the materials it has produced or of the materials authorized or supplied to it by their owners in accordance with the agreed terms and conditions and the provisions of regulations in force.

2.3 Information exchange

All exchanges of information between Indra and service suppliers shall be understood to have taken place within the framework established by the corresponding service provision contract, in such a way that this information cannot be used outside this framework or for other purposes.

Electronic or physical information must be distributed using the resources determined in the service provision contract for this purpose and exclusively to facilitate the functions associated with the contract.

Indra reserves the right, in accordance with the identified risk, to implement control, registration and auditing measures in relation to these dissemination resources. In relation to exchanges of information within the framework of a service provision contract, the following activities shall be considered to be not authorized:

- The transmission or reception of materials protected by copyright that infringe intellectual protection legislation.
- The transmission or reception of all classes of pornographic or sexually explicit materials, racially discriminatory statements and any other types of statements or messages that can be classified as offensive or illegal.
- The transmission or reception of sensitive information, except when authorized in writing and electronically communicated in an encrypted manner.
- The transfer of protected information to unauthorized third parties.
- The transmission or reception of applications not related to the business.
- Participation in Internet activities such as news groups, games or other activities not directly related to the provision of the service.
- All activities that may damage Indra's image and reputation are prohibited on the Internet and in all other places.

2.4 Appropriate Use of Indra Corporate Resources

Indra corporate resources accessed by service providers must be used exclusively to comply with the obligations and purposes of the provision of the service.

Under no circumstances may they be used for activities not related to the purpose of the service or for the commission of activities that may be considered illicit such as damage to third-party intellectual property, breaches of data protection regulations, etc.

Service providers must undertake to use the Indra corporate resources to which they have access in accordance with Indra's security policies.

With the aim of ensuring the correct use of the aforementioned resources, Indra may implement the control and auditing mechanisms it deems suitable, either periodically or when suitable for specific security or service reasons.

If it is discovered that a service provider, or any members of its staff, has incorrectly used Indra resources or information, this circumstance must be communicated to the provider so that suitable actions can be taken. Indra reserves the right to implement all applicable legal actions to protect its rights.

Any files introduced into Indra's network or into any other equipment connected to it through automated media, the Internet, email or any other method must comply with the requirements established in these regulations and, especially, those that refer to intellectual property, personal data protection, and virus and malware control.

2.5 User Responsibilities

Service providers must ensure that all staff who in the performance of their functions for Indra may have access to Indra's information, information systems or resources respect the following basic principles in their activity:

- Everyone with access to Indra's information is responsible for the activity undertaken by their user identifier and everything arising from it. Therefore, it is essential for each person to control the authentication systems associated with their user identifier, guaranteeing that the associated code is only known by the user and is not disclosed to any other staff under any circumstances.
- Users must not use any other user's identifier even if they have the owner's authorization to do so.
- Users must be familiar with and apply all requirements and procedures related to the information they handle.
- All users with access to Indra's information must choose high-quality passwords (containing at least 8 characters, made up of upper case and lower case letters, digits and special characters, and not containing any type of information that can be easily guessed).
- All users with access to Indra's information must change their default and temporary passwords upon access to their first session and at least once every 90 days or when there is an indication that other users may know them.
- All people with access to Indra's information should ensure that their equipment is protected when unattended.
- All people with access to information must respect at least the following clean desk rules in order to protect paper documents, IT media and portable storage devices and reduce the risk of unauthorized access, loss or damage to information both during normal working hours and outside normal working hours (Store paper documents and IT media under lock and key, lock user sessions when left unattended, protect both information reception and transmission points, security remove, etc)
- People with access to Indra's information systems must never, without written authorization, perform tests to detect and/or exploit a supposed weakness or security incident.
- No person with access to Indra's information systems may attempt without express, written authorization to use any means to violate the security system and authorizations. It is forbidden for users to capture network traffic, unless it is for auditing tasks that have been authorized in writing.

2.6 Security Requirements for Devices

All devices with access to Indra's information, regardless of their ownership, must comply with the security policies established by Indra, placing special emphasis on the following considerations:

- Access to systems must always be gained in an authenticated manner, at least through the use of a personal identifier and associated password.
- All software installed or contained in devices must be licensed, within the life cycle of the product and in a state that is consistent with the license.
- Devices must be kept up to date with the latest available version of security patches for the installed software and operating system.
- Devices must be equipped with an anti-malware protection system that is active and up to date with the latest available version, both for the engine and the signature file.
- Screen locking must be configured to activate after 10 minutes of inactivity. Unlocking the device will require a password, unlocking pattern or an equivalent mechanism to guarantee that the device cannot be used by an unauthorized user.
- Devices must not contain any tools or files that contravene Indra's security policy or that may interfere with corporate software. This point includes all those that have the aim of discovering information other than that of the user or gaining unauthorized access such as sniffers, network scanning tools, password discovery tools, etc.

2.7 Communication of Security Incidents

Service providers must undertake to immediately communicate any incidents, weaknesses or threats (observed or suspected) detected in Indra's information systems or that may have affected information owned by Indra or its customers to the **Information Security Department** via email to the Indra CSIRT Generic User csirt@indra.es or through the person responsible for the service.

In the case of supplier staff posted to work at Indra's premises, any incidents, weaknesses or threats related to Indra's information or resources must be communicated through the Indra CSIRT Generic User csirt@indra.es or Indra's USC.

3 Specific security principles

3.1 Physical safety

Compulsory: All service providers whose services are provided from their site.

- Buildings or facilities must be physically solid (e.g. there should not be any gaps in the perimeter or areas that can be easily broken); the external walls of facilities should be solidly constructed.
- All external doors should be suitably protected against unauthorized accesses with control mechanisms such as bars, alarms, locks, turnstiles, surveillance cameras, etc.
- Wherever possible, it is advisable to establish physical barriers that require the identification of employees through a suitable identification and authentication method (identity cards, electronic cards, biometric identification, etc.) in order to prevent unauthorized physical access.
- Buildings and facilities should have automatic systems to detect and respond to adverse environmental conditions (mainly fire). When it is not possible to install an automatic fire extinguishing system, there must be manual extinguishing measures in place and all company staff must be familiar with their operation.
- Basic environmental conditions related to temperature, hygiene, electronic insulation, soundproofing and other similar measures must be established in accordance with the specific IT equipment requirements.
- If copies of information that is Indra's responsibility are kept, the systems that house and/or process this information must be located in a specially protected area that includes at least the following security measures:
    - There must be an access control system that is independent from the site.
    - An access log must be kept.
    - Access by external parties must only be granted when necessary and authorized and must always be subject to the surveillance of authorized staff.
    - External staff are not permitted to enter or work in especially protected areas without supervision.
    - There must be some form of protection against power failures.

3.2 Development security

Compulsory: All service providers who perform development work and/or application tests for Indra.

- The environments in which these activities are undertaken must be isolated from each other and also isolated from production environments.
- All accesses to information systems that house or process information should be protected by at least a firewall that limits their connection capacity.
- The entire outsourced software development process must be controlled and supervised by Indra.
- Application specifications must expressly contain the security requirements to be met in each case.
- Identification, authentication, access control, auditing and integrity mechanisms must be incorporated into the entire application design, development, implementation and operation life cycle.
- Developed applications must incorporate input data validations that verify that the data are correct and appropriate and prevent the introduction of executable code.
- Internal processes developed by applications must incorporate all the validations necessary to guarantee that information is not corrupted.
- Whenever necessary, functions to authenticate and control integrity in communications between the various components of the applications must be incorporated.

- The output information provided by applications must be limited, guaranteeing the provision of only relevant and necessary information.
- Access to the source code of applications must be limited to the staff of the service.
- Test environments must only use real data when they have been appropriately disassociated or whenever it is possible to guarantee that the applied security measures are equivalent to those in the production environment.
- Application tests must verify that there are no uncontrolled information leak channels and that only the planned information is offered via the established channels.
- Only applications that have been expressly approved can be transferred to the production environment.

3.3 System security

Compulsory: All service providers whose services are provided through the use of their ICT infrastructure.

3.3.1 Asset management

- Service providers must have an up-to-date record of their assets to identify all assets used to render the service.
- Service providers must inform Indra of the removal of any assets used for the provision of the service. If the asset contains Indra property (hardware, software or other types), it must be delivered to Indra prior to removal so that Indra can remove the assets it owns.
- Whenever an asset has contained information considered to be sensitive, service providers must guarantee the secure deletion of this information in their asset removal processes, applying secure deletion functions or physically destroying the asset so that the information it contained cannot be recovered.
- All assets used for the provision of the service should have a manager, who must ensure that these assets incorporate the minimum security measures established by Indra, which must at least be those specified in this regulation:
- Comply with the provisions of the point Security Requirements for Devices.
    - They must register the most significant events related to their operation. These activity records will be contemplated within the supplier's regulations on backup copies. Especially, all events undertaken with privileged permissions must be registered.
    - System clocks must be synchronized with each other and the official time.
    - Service providers must guarantee that the capacity of the systems is suitably managed, avoiding potential shutdowns or malfunctions of these systems due to resource saturation.
    - Errors and faults registered in the activity of the systems must be analyzed, adopting the means necessary to redress them.
- Suppliers must establish backup copy regulations that guarantee the safeguarding of all data or information relevant to the provided service on a weekly basis.

3.3.2 Continuity management

- Service providers must have a continuity plan and an IT recovery plan in the event of disasters that enable the provision of the service even in the case of contingencies. This plan must be developed in accordance with a risk assessment (at least once a year) to identify any risks that could interrupt operations and to ensure that appropriate controls are implemented to manage and control them.
- Service providers must test their continuity plan and recovery plan to confirm that the service can be recovered in the agreed periods. These tests must be performed on an annual basis or just after significant changes, improvements or amendments that affect the services have been made.

3.3.3 Network security

- All networks must be suitably managed and controlled, ensuring that there are no uncontrolled accesses or connections whose risks are not suitably managed by them, establishing suitable systems for the monitoring and auditing of security that are necessary to guarantee the security of the connections.

- The services available in the networks through which information circulates must be limited to the extent possible.
- The networks that enable access to Indra infrastructure must be suitably protected and comply with the following premises:
    - They must be communicated and authorized by the Information Systems Unit (IS).
    - Remote user access to the Indra network must be subject to compliance with IS procedures on prior authentication and access validation.
    - These connections must be undertaken for a limited time through the use of private virtual networks or dedicated lines.
    - These connections must not allow any type of communications equipment (cards, modems, etc.) that enable alternative uncontrolled connections.

3.3.4 Change management

- Service providers must guarantee that all changes to the ICT infrastructure used to provide the service are controlled and authorized, guaranteeing that no uncontrolled component forms part of the ICT infrastructure.
- It must be verified that all new components introduced into the ICT infrastructure used for the provision of the service work properly and comply with the purposes for which there were incorporated.
- All changes must be implemented in accordance with a formally established and documented procedure that guarantees that the appropriate steps are taken to make the change.
- The change management procedure must guarantee that changes to critical components are minimized and limited to those that are essential.
- All changes made to critical components must be verified to ensure that there are no adverse or unforeseen collateral effects to the operation of these components or their security.
- Any technical vulnerabilities presented by the infrastructure used for the provision of the service must be analyzed, informing Indra of all those associated with critical components with the aim of jointly managing these vulnerabilities.

Avda. de Bruselas, 35
28018 Alcobendas
Madrid, Spain
Phone: +34 91 480 50 00

indracompany.com