Technical and Organizational Security Measures

Information security procedures

Internal organization

Separate roles and responsibilities have been defined for information security and have been assigned to those responsible for processing activities within the company (hereinafter also referred to as "users") in order to avoid conflicts of interest and prevent improper activities.

Human resources security

Mobile devices and teleworking

There is a security policy for the use of all company devices, in particular mobile devices, and appropriate controls are in place.

Termination or changes in the employment relationship

Upon termination of a user's collaboration with the organization or in the event of a significant change in their role, access permissions are immediately updated, while business tools are physically and logically reset and reset.

Enterprise resource management

Responsibility for the company's resources and assets

All company tools and assets are carefully inventoried and their allocation to the various users responsible for their security is monitored. A policy has been defined for its correct use.

Information classification

All information is classified and cataloged by the respective users, according to security requirements, as well as processed appropriately.

Storage media management

Information stored on storage media is managed, controlled, modified and used in a manner that does not compromise its content and is erased appropriately.

Access control

Access control requirements

The company's organizational requirements for monitoring access to information resources are documented in a policy and implemented in practice through an access control procedure; meaning that network access and connections are limited.

User Access Management

The allocation of user access rights is controlled from the initial registration of the user to the removal of access rights when they are no longer needed, including special restrictions on privileged access rights and the management of "secret authentication information", and is subject to periodic reviews and verifications including an update of access rights when necessary. In access management, the criterion of minimizing access rights is used, as they are issued to grant the user only access to the data necessary for their function and business activity. Additional access rights require specific authorization.

User Responsibility

Users are also aware of their responsibilities in maintaining the effectiveness of access controls, and must, for example, choose complex passwords, whose complexity is verified by the system, and keep them confidential.

Access control systems and applications

Access to information is subject to restrictions in accordance with the access control policy, through a secure access system and password management, as well as controls on privileged users and limited access to all source code.

Encryption

Cryptographic control

There is a Policy in place regarding the use of encryption of storage media and user data. Authentications are encrypted.

Physical and environmental security

Physical and environmental security measures are in place to prevent unlawful or accidental access, loss or dissemination of data.

Secure areas: Data center

The company's services are provided and hosted in several neutral national Data Centers, made available by suppliers in the service provision format. All Datacenters within the supply chain offer complete redundancy of all electrical, cooling and network circuits. All Datacenters have perimeter lighting, as well as a presence detection system with CCTV cameras, providing private security for the building, with a security team present 24 hours a day, 7 days a week, in the Datacenters.

Physical access is regulated and controlled by authorization, recognition and registration procedures and is limited, thanks to the access control system, to the areas for which authorization exists.

Equipment

There is a policy for disposing of unused equipment in order to securely destroy any information that may be contained therein.

Operations security

Operational procedures and responsibilities

IT operational responsibilities are documented and changes to IT facilities and systems are controlled. Development systems, verification systems, and operating systems are separate.

There are users responsible for the proper functioning of the procedures. On the other hand, the management of the logical security of the operating systems and applications installed by the customer is the responsibility of the customer for the individual services provided by the Company (hereinafter also referred to as the "customer").

Malware protection

Virus and malware control is active on company devices and there is appropriate user awareness.

With regard to Virtual Server or Dedicated Server services, the customer is responsible for installing antivirus and antimalware software and - if the related service has not been purchased - a firewall. Regarding the hosting service, there is real-time protection on the frontend machines.

As far as the email service is concerned, email traffic is analyzed in real time, both incoming and outgoing, to detect viruses, malware and to identify and filter spam. The analysis is automated and is based on the nature of the content, the interrogation of international databases and the reputation acquired due to a series of parameters.

Backup

Periodic backups are performed, excluding services for which the customer has not subscribed to a backup service and is therefore responsible for maintaining and managing their backups. For hosting services and

of mail, periodic backups are performed which, for hosting services, can also be accessed by the customer. Additional backups, not accessible by customers, are performed for the sole purpose of disaster recovery.

Authentication and Monitoring

Authentication and Synchronization

All activities and events related to information security, carried out by system users and administrators/operators, occur after the insertion of their authentication credentials or identity certificates. The clocks on all equipment are synchronized.

Operational software control

The installation of software on operating systems is controlled and monitored.

Regarding Virtual Servers and Dedicated Servers, the operating systems available to customers are provided with updated installation images. It is also the customer's responsibility to update any applications or software installed by them.

Communications security

Network Security Management

Online networks and services are also secured through separation and segregation. The network is monitored 24/7 both in terms of metrics and automatic alarms.

Transfer of information

Agreements regarding the transfer of information to and from third parties are in place.

System acquisition, development and maintenance

Security in development and support processes

The rules governing the security of software and system development are defined in a Policy. Changes to the system (for applications and for operating systems) are controlled. The security of the system is tested and eligibility criteria, which include security aspects, are defined.

Relationship with suppliers

Information security in relationships with suppliers

There are contracts or agreements that aim to protect and regulate the processing of information from the organization and customers accessible to third parties operating in IT and to other subcontracted suppliers that are part of the entire supply chain.

Management of services provided by suppliers

The provision of services provided by suppliers is monitored and verified against the contract or agreement. Service changes are verified.

Incident management for information security

Information security incident management and improvements

There are specific responsibilities and procedures that aim to manage in a coherent and effective manner all events and incidents related to information security (for example, the so-called procedure

of data breach).

Information security aspects related to business continuity

Redundancies

All major IT facilities are redundant to meet availability requirements. Where such redundancy is not in place, appropriate measures are in place to ensure continuity of service or minimize data loss.

Accordance

Compliance with legal and contractual requirements

The company identifies and documents its obligations to external authorities and other third parties regarding information security, including intellectual property, accounting documentation and privacy information.

Safety information review

The organization's information security-related projects and security policies are reviewed and corrective actions are taken when necessary.