Cerved Group S.p.A.

Information Security Policy

Approved on July 1, 2022

Version 005

Index

1 Objective and scope of application

1.1 OBJECTIVE

The objective of this document is to define the information security policies of Cerved Group (hereinafter the Group), in terms of principles, guidelines and rules to be applied for the definition, management and governance of the security of information systems. In particular, this document represents the preferential tool in order to raise awareness among employees and collaborators of the company regarding the rules that must be respected in the management of corporate information assets, with the aim of ensure the security of the computer system and the protection of the image of all Group companies.

1.2 SCOPE OF APPLICATION

The security policies defined in this document must be applied to the entire set of organizational structures and technologies that make up the information systems of all Group companies.
The infrastructure that the company provides for its internal (employees, consultants) and external (customers, suppliers) services is structured as follows:

- *Application systems:* applications and databases that support business processes;
- *Processing and storage systems:* systems that provide information processing and storage services, such as mainframe, file servers, Storage Area Networks etc.;
- *Infrastructure systems:* systems that provide network services (for example domain controller, Proxy, Mail, DNS, Firewall etc.);
- *Telecommunication systems:* devices that provide telecommunication services, such as routers and switches, as well as telephony equipment connected to the company data network (for example, smartphones);
- *Workstations:* fixed and mobile workstations through which users access company information resources.
- *Cloud Services*: services designed to provide easy and cost-effective access to applications and resources, without the need for internal infrastructure or hardware. It is specified that even security policies for which there is no explicit cloud reference section are also applied to Cloud services.

1.3 RECIPIENTS

The security policies defined in this document must be observed by all company personnel belonging to the Group and by the personnel of any external suppliers who carry out activities on behalf of the Group.

2 Riferimenti

2.1 DOCUMENTATION

The security policies defined in this document have been structured on the basis of the international standard ISO 27001. The UNI CEI ISO / IEC 27001: 2013 Standard (Information technology - Security techniques - Security management systems of information - Requirements) is an international standard that defines the requirements to define and manage a Management System of Information Security (ISMS or ISMS from Information Security Management System) regarding logic, physical and organizational security.

The standard was created and published in October 2013 for certification purposes, so as to constitute a complete system to guarantee the security management in information technology: with its publication it replaced the British standard BS 7799 which up at that time it represented the main reference standard for the application of an information security management system.
The setting of the ISO / IEC 27001 standard is consistent with that of the ISO 9001: 2015 Quality Management System and Risk management, based on a plan-do-check-act (PDCA) model.
The goal of the standard is to protect data and information from threats, in order to ensure their integrity, confidentiality and availability, and provide the requirements for adopting an adequate information security management system.
ISO 27002: 2013 is a collection of "best practices" that can be adopted to meet the requirements of the ISO standard 27001: 2013 in order to protect information resources.
This document has been defined also taking into consideration:

- the specifications and requirements defined in the EU Regulation 2016/679 - GDPR and subsequent regulations issued by the Authority for the Protection of Personal Data.
- the specifications and requirements defined in ISO / IEC Standard 27017, clarifying the roles and responsibilities for cloud service providers and their customers with the goal of ensuring that data stored in the cloud is safe and secure;
- the specifications and requirements defined in ISO / IEC Standard 27018 [Code of Practice for the Protection of Personally Identifiable information (PII) in Public Cloud Services for Cloud Providers] to be understood as a guideline for public cloud service providers on improving the management of personal data in order to provide a structured, privacy-by-design based way of handling personal data in distributed computing infrastructure (public cloud).

Refer to document CG_D_0255 - “Mappa normative applicabili alle società del Gruppo Cerved” as regards the regulatory framework applied to the various companies of the Group.

The ISO/IEC 27017:2015 standard, part of the ISO/IEC 27001 standards, defines specific controls for providers and customers of cloud services with the aim of precisely delineating the roles and responsibilities of the various actors involved to ensure the security and protection of personal data stored in the cloud. This standard provides guidance for cloud services in addition to what governed by ISO/IEC 27002, focusing on new additional aspects:

- division of responsibilities between provider and customers of cloud services;
- monitoring of customer activities within the cloud environment;
- alignment of virtual and cloud environments;
- administrative activities and procedures related to the cloud environment;
- protection and separation of virtual environments;

- Virtual Machine configuration;

The ISO/IEC 27018:2020 standard defines a set of specific countermeasures based on international privacy principles for the proper design, development, implementation, monitoring and measurement of privacy policies in cloud computing services.

3 Information security policies

The Group has defined the security policies described in this document, in line with the needs and business objectives, security requirements and the corporate organizational structure. The main objectives of the IT security policies are listed below:

- ensure that the information and IT assets are adequately protected against the risks of compromise;
- establish and maintain a structured process for the identification and assessment of IT risk, with the aim of applying the appropriate controls and verifying its effectiveness and efficiency with a view to continuous improvement and reduction of the level of risk identified;
- ensure compliance with legal, regulatory and contractual requirements relating to information security

The security policies defined in this document have been structured on the basis of the following areas:

1) international standard ISO 27001: 2013 (described in paragraph 2.1 - Documentation):
   - *Organization of security:* definition of roles and responsibilities to promote conduct and controls for the purpose to guarantee IT security;
   - *IT asset management:* technical and / or organizational criteria for the management of IT equipment and rules for assigning an information risk profile;
   - *Personnel security:* rules of conduct that the personnel must follow;
   - *Physical and environmental safety:* protection for personnel, for technological components, for premises and paper archives;
   - *Operational and telecommunications security:* controls on processes and operational activities such as data protection transmitted, and access control to IT services and systems available on the network;
   - *Access control:* control of logical accesses to the information system, according to precise pre-established methods;
   - *Management of cryptographic keys:* rules for the management of cryptographic keys (creation, distribution, storage, period of use, backup, disposal, destruction, protection)
   - *Acquisition, development and maintenance of systems:* rules for the management, modification, testing and production of application programs, basic software and hardware components;
   - *Management of IT security events and incidents:* procedures to ensure the timely management and resolution of incidents and malfunctions that may have an impact on IT security;
   - *Business continuity management:* rules for governing the process of providing the service even in the face of an interruption due to a critical event;
   - *Compliance with laws and regulations:* criteria and procedures necessary for the fulfilment of the laws and regulations in force.
2) International Standards ISO 27017:215 and ISO27018:2020 (described in section 2.1 Documentation) with specific reference to Group companies using cloud computing services.
   - Cloud Computing Services: criteria, processes and activities related to cloud computing services such as description of the structure, definition of obligations and rights of the cloud service provider and Cerved Group companies.

3.1 SECURITY ORGANIZATION

3.1.1 Internal organization (roles and responsibilities)

The Group must establish an IT security management process based on the identification, assessment and management of business and IT risks inherent to information security. This process must be oriented towards continuous improvement in order to check and periodically review the security of the Group's IT system.
The implementation of the security policies defined in this document requires an organization of resources and processes that promote actions, behaviours and controls.
To this end, the Group must equip itself with suitable organizational structures for the governance, operational management and control of information security. In particular, the structures responsible for the governance and control of security must carry out the following activities:

- coordination with operational structures;
- periodic information on the evolution of threats and related security solutions;
- periodic monitoring of the operational effectiveness of the controls implemented to ensure the security of information.

The structures responsible for the operational management of IT security must take care of the design, implementation and maintenance of the technical and organizational solutions necessary to ensure an appropriate level of information security within the technological and application platforms in use by the Group companies. To this end, adequate segregation of roles and related responsibilities must be ensured between security governance and control activities and the operational management of IT solutions.

The main corporate structures competent in the field of safety are:

- *the Board of Directors*: establishes the safety objectives, the acceptable risk levels, the prevention and mitigation strategies and approves the investment plans for the implementation of the identified strategies;
- *the Security Committee*: has the task of evaluating, validating and proposing the company's safety strategies, authorizing the publication of policies and operating procedures, periodically checking the state of safety and promoting the culture of safety among staff;
- *the IT Area*: has the task of identifying, designing and implementing, through the technical structures involved, the organizational and technological security measures. It also has the task of managing the operational aspects of the security of information systems, in compliance with the policies and operating procedures defined;
- *the Managers of all company areas*: they have the task of supervising and monitoring the application of the policies and operational procedures defined in their structures;
- *Internal Audit*: has the task of checking the application of the rules and monitoring the level of security in the various business areas.

3.1.2 Management of Third Parties

The purchase on the market of services of a different nature (consulting, programming, general services, outsourcing, etc.) involves the possibility of direct access by third parties to the corporate information assets. It is therefore essential to establish the security requirements that must be respected for the contractual and managerial regulation of relations with Third Parties who, in order to provide the agreed services, need to access company resources. In the case of IT services managed in outsourcing, the Third Party companies must guarantee the adoption of adequate security measures, at least equal to those adopted by the Group.

Agreements with third parties must contain the Group's data protection requirements. In particular, third parties must be available to submit, upon request, their security plan, the security measures implemented and allow for IT security checks by the Group. In particular:

- the approach to be adopted for the management of collaborations with third parties must foresee the acceptance by the contractor of the company policies and procedures in force and of all the operating procedures and requirements specified in the rules of engagement and in the contract stipulated with the Third Party;
- confidentiality or non-disclosure agreements must be signed valid before, during and after the engagement based on the criticality of the information and services involved;
- the roles and responsibilities for the safety of third parties must be defined and documented;
- Agreements must be established for the exchange of information and software between the organization and third parties;
- it must be monitored and verified that the supplier provides adequate resources for the provision of services based on contractual requests, in particular with regard to IT security

3.2 IT ASSET MANAGEMENT

3.2.1 IT asset governance

All IT assets must be identified in terms of their physical location (for example, offices, branches, data centres and warehouses where are hosted) and owned. Their value must be evaluated in order to provide an adequate level of protection (for the value information refer to paragraph 3.2.2 Classification of information).
Responsibilities for the use and management of all IT devices must be defined in order to ensure correct and safe operation from a perspective of managing the risks associated with human errors, theft of assets, attempts at fraud or improper use of corporate resources. Furthermore, a registry of the equipment (assets) and devices assigned to users must be maintained. In the case of IT assets supplied to external entities of the Group (such as agents, service providers etc.), the minimum security requirements must be defined, which must be guaranteed by the owner of the asset. Furthermore, periodic audits must be carried out in order to verify that the methods of management and use of the equipment and devices supplied are in line with business needs and established practices.
IT assets must be stored according to the manufacturer's instructions and in compliance with internal and external regulations (see paragraph 3.13 Compliance with regulations).
During maintenance, change of use, change of ownership and disposal, mechanisms must be provided to guarantee the confidentiality of the data contained within the assets and, if necessary, mechanisms must be provided to prevent unauthorized recovery of data (including secure deletion of data).

With regard to cloud services, the assets of Cerved Group companies located on the premises of the cloud service provider must be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.
Group companies must request a documented description of the service termination process covering the return and removal of Group company assets, followed by the deletion of all copies of those assets from the cloud service provider's systems.

3.2.2 Information classification

Information, understood as structured aggregations of data, is an integral part of the Group's assets and requires precise information management rules to ensure their adequate protection. In order to protect this asset and make the best use of it in the interest of the corporate mission, it is necessary to define a classification model of the types of information in relation to their criticality, establishing the guidelines for their correct management in all available, tangible and intangible.
The classification of corporate information is a preparatory activity for the implementation of suitable solutions aimed to protect the data and related information associated with them: these solutions must be adequate to the level of criticality that the data assume in the corporate context. The implementation of specific security solutions, based on the level of criticality of the data, makes it possible to ensure greater protection of data and related information and not to waste resources in the protection of data that are instead easily available even outside the perimeter corporate.

The classification of company data consists in assigning a level of criticality to each data product, processed or stored within the company perimeter. In particular, the level of criticality must be assigned in relation to the importance to follow the Group's business objectives, as well as the economic, image or legal impacts resulting from a violation of their confidentiality, integrity and availability properties.

The classification of information must be carried out at the time of creating a category or instance of the data, in order to be able to adopt the appropriate protection methods.
To determine the level of safety to be followed and maintained, an analysis and classification of risks must be performed in order to define what will be the appropriate safety mechanisms, such as to balance costs and benefits.
An "owner" must be identified for each class of information, application, process, system or IT infrastructure. The owner is responsible for assessing the risk associated with failing to meet safety requirements and for assigning an appropriate safety rating.
The level of data protection must be commensurate with their degree of confidentiality and relevance for the Group. Based on ratings regarding the criticality of the data, the information must be classified according to the following scheme:

- *public information*: information in the public domain and data intended for disclosure to subjects external to the Group, subject to restrictions regarding the content;
- *information for internal use*: data used in the performance of ordinary work activities, intended for disclosure within the company perimeter whose eventual leakage does not compromise the position of the company and / or its image, if not marginally. All information that has not obtained approval for free disclosure outside the Group is defined for internal use;
- *information for corporate use only*: data that provide an advantage resulting from the know-how gained by the Group, the release of which may lead to an increase in operating activities to restore the competitive position or a loss of image that requires economic investments to be restored;
- *strictly confidential information*: data that provides a competitive advantage whose leakage can result in a considerable decrease in the Group's competitive position or compromise its image.

It is important that access and sharing of information take place following specific security measures and on the basis of the necessary authorizations. Furthermore, based on the data class and therefore on the level of criticality for each security objective, it is necessary to implement suitable security measures. In particular, adequate protection measures must be identified in the event of:

- paper and electronic archiving;
- paper and electronic distribution;
- disposal of information and supports;
- making paper copies.

3.3 PERSONNEL SECURITY

Group employees, as well as all collaborators, must comply with precise rules of conduct in order to ensure a homogeneous level of safety, reducing the risks associated with human errors, in compliance with company procedures (as a result of inexperience and misinformation) or wilful misconduct.

In order to have adequate guarantees that the internal and external personnel have their responsibilities clear, have been selected and appointed in accordance with the role assigned to them and have the necessary skills to carry out the tasks assigned to them, the Group must prepare appropriate safety measures during the entire corporate life cycle of personnel. In particular:

- when selecting personnel, verification checks must be carried out on candidates, in proportion to the classification and corporate role, in compliance with the relevant laws and regulations;
- when the personnel signs a contract with the Group in compliance with their contractual obligations, they must accept and sign the terms and conditions regarding their responsibilities, also with reference to IT security aspects;
- during the normal operations of the personnel, it must be verified, through periodic audits, that all users apply the security measures provided for by company policies and procedures;
- when the collaboration relationship with the Group ends, as specified in paragraph 3.2 Management of IT assets.

The concrete implementation of a system for the protection of corporate assets is also achieved thanks to the promotion of a related corporate culture, achieved through information activities and the implementation of specific training plans. All Group employees and, where appropriate, collaborators and third-party users, must therefore receive adequate training in order to be made aware of the risks affecting data and other corporate assets, on the countermeasures available to prevent harmful events, on the resulting responsibilities and on the methods of updating the security measures adopted by the Group.

Particular attention must be paid to the choice and designation of system administrators, in consideration of the access privileges to the company IT system. For the assignment of the functions of system administrator, internal or external, the experience, ability and reliability of the designated person must be assessed, who must provide a suitable guarantee of full compliance with current safety provisions. In particular, the designation of system administrators must take place on an individual basis and, at the same time as the assignment of duties, each person must be provided with a detailed list of the permitted areas of operation.

3.4 PHYSICAL AND ENVIRONMENTAL SECURITY

The Group is responsible for defining, by means of an appropriate risk analysis and with the support of the relevant company structures, criteria and requirements for physical and environmental security in order to prevent and / or limit the loss of data and critical resources due to vulnerabilities in the physical domain scope.

The devices for controlling access to the offices and related premises are established according to the risks and the nature of the information contained. Access to the premises where the processing tools and segregated paper archives are located must be allowed only to appointed and authorized personnel.

Access to company offices must be allowed only after identifying the person who needs to enter by badge or other mechanisms of equal reliability. In particular, all accesses to the premises deemed critical must be recorded, automatically or manually, both at entry and exit.

The areas hosting the most critical systems must be located in safe and protected areas in order to minimize the risk of loss or damage and improper and unauthorized use. This objective must be pursued through the adoption of the principle of security-in-depth: progressive security techniques in order to mitigate the risk of a level to be compromised or bypassed.

The premises hosting the electronic computers must have devices that allow:

- segregate and track the accesses made by authorized personnel;
- monitor attempts of unauthorized access or break-in into the premises;
- monitor the level of temperature and humidity present in the premises;
- counteract harmful events such as floods and / or fires through suitable environmental control tools;
- ensure the provision of the service in the absence of primary electricity through the implementation of appropriate compensatory solutions;
- report any malfunctions to an operations centre.

Authorizations relating to access to the premises hosting the computers must:

- be approved by the appropriate structures prior to release;
- revoked in the event of termination of the employment relationship or change of job;
- reviewed and evaluated on a regular basis.

In addition, all employees must be trained on prevention and behavior in the event of security incidents that may affect the premises hosting the systems.

3.5 OPERATIONAL AND TELECOMMUNICATIONS SECURITY

3.5.1 Operational Security

The IT infrastructure and its main components must be adequately protected and their effectiveness and efficiency must be maintained over time. Therefore:

- the operating procedures, the defined architectures, the applied configurations, must be documented and kept up to date to ensure the correct and safe use of IT resources;
- IT documentation classified as company confidential use must be adequately kept and accessible only to authorized personnel;
- the necessary measures must be planned and implemented to guarantee an adequate level of efficiency and performance of the IT systems, the prevention of the risk of malfunctions or degradation of the security functions applied. Furthermore, such measures must be able to ensure:
    - ✓ maintaining the efficiency of the systems and their regular maintenance, also in consideration of the criticality level of the information they process;
    - ✓ that access to the systems for administration and maintenance purposes is allowed only to authorized and authorized personnel;
    - ✓ that the software installed is licensed, compliant with applicable legal regulations and provides the required level of service.
- a company-wide prevention policy must be identified against malicious software (computer viruses, worms, etc.). This policy must provide for clear and effective security measures, the use and maintenance and timely updating of appropriate software tools and specific controls in order to ensure and maintain the security of the corporate network and of the information shared through it. In particular, the effectiveness and update of these programs must be verified, automatically, on a periodic basis.
- the use of IT resources must be monitored and the processing capacity needs must be planned to minimize the risk of inadequate performance, malfunctions and degradation of established service and safety levels.

The operational processes of IT resource management must be structured and controlled in order to guarantee security computer technology. In particular:

- the hardware systems and the connected peripheral units must be controlled and be subject to a level of maintenance that is adequate for the Group's business continuity needs;
- maintenance operations on hardware systems must be carried out, as far as possible, with timing compatible with the processing for business processes, in order to minimize interference;
- in addition, measurements of the processing capacity of the systems must be carried out periodically in order to adequately meet the needs of the business processes (capacity planning);
- the evaluation of new products, replacing or integrating the basic software must include checks on the safety, reliability and availability characteristics, with a view to reducing the probability of harmful events and improving the level of security.

3.5.2 Telecommunication security

The design of the security of a computer network must consider the following aspects:

- *segregation:* mechanisms for separating and filtering traffic between subnets within the corporate perimeter;

- *monitoring:* methods and tools to be used to control the traffic in transit on the networks, with the aim of identifying any deviations from the defined operations;
- *availability:* methods and tools to ensure continuity in the provision of network services.

The configuration of the security of a computer network must address the following aspects:

- *addressing:* rules for assigning the network addresses of the equipment and systems connected to the networks;
- *routing:* technical solutions adopted to avoid unwanted routes, given the destination of the information to be transmitted;
- *access to network equipment*: mechanisms for controlling and restricting access to network equipment that make up the telematics infrastructure.

Therefore, technical and procedural criteria must be adopted in order to ensure that only authorized users can access the individual IT systems or services, via the telecommunications network. Similarly, the telecommunications network must ensure that the messages and data transmitted over the network are not altered or deleted and that there are sufficient protections in order to prevent fraudulent data from being entered.

The components of the telematics network must be protected through specific measures:

- the network equipment must be located inside suitably protected cabinets. Access to these cabinets must be allowed only to internal and external technicians responsible for managing maintenance;
- network devices considered critical must be duplicated to manage any malfunctions of them;
- Network diagrams must be drawn up and kept constantly updated. These diagrams must be treated as confidential information.

The following countermeasures must be adopted in the management of security related to remote accesses:

- remote access to systems must be allowed only with prior authorization and on the basis of reasons that justify it;
- the entrance lines to the Group network used for traffic must be managed by special equipment that allows control and ensures protection from unauthorized access;
- the use of telematics equipment connected directly to the Group's network computers must be granted only with prior authorization and with proven justification.

Connections between the Group network and the Internet must only take place through devices that have technological requirements capable of ensuring protection from unauthorized access (firewalls, routers, proxies).

Internet access by employees and company collaborators must be granted according to the needs of users, limited to the performance of specific activities and tasks.

The management of the Group's network infrastructure must include monitoring devices capable of examining network traffic, verifying the correct functioning of safety devices and providing timely alarm signals in the event of an attack on the protection systems.

3.5.3 Backup and management of storage media

Backup operations make it possible to ensure the availability of information and systems even following IT security incidents or disaster events. In particular, as part of the Group infrastructure, the following must be subjected to a backup and archiving procedure:

- the data necessary and sufficient to guarantee the complete recovery of the applications considered critical and of the related databases;
- the data and programs that make it possible to satisfy subsequent requests for restoration by internal or external control units, in accordance with the retention times defined in line with the regulations to which the Group is subject (see paragraph 3.12 Compliance with regulations).

During all stages of the backup management process, the confidentiality, integrity and availability of the data processed must be guaranteed. To that end:

- appropriate backup frequencies, backup techniques and backup copies preservation methods must be agreed and implemented, in line with the requirements to ensure the complete restoration of critical applications and related databases;
- adequate checks must be carried out to restore the data (partial and total) backed up, in order to ensure the effectiveness of the procedures.

The security measures taken to protect the backup data must comply with the criticality level of the information contained in the backup itself. In particular:

- physical access to the premises hosting the backup system must be allowed only to authorized personnel;
- logical access to backup systems must be controlled and allowed only to authorized personnel;
- any access by other parties for the performance of activities other than those of ordinary management of the backup systems must be authorized in advance;
- any exceptions must be agreed with the security structures in charge.

Backup operations must be documented in order to facilitate any requests for details regarding data backup activities. Furthermore, the storage media used to make the backups must be chosen based on the backup recovery times and must be managed in compliance with the following constraints:

- the storage media must be stored in a place other than that in which the original data reside;
- access control measures must be implemented that make it possible to limit logical and physical access to the media and data contained therein to only those in charge of backup activities. The control measures must be correlated to the criticality of the data they contain;
- the data on the storage media must be deleted using secure erasing methods (for example, specific algorithms for the secure erasing of data);
- backup media no longer needed must be destroyed in ways that do not allow subsequent access to the data contained in the media;
- backup media must never be left unattended and must always be stored in adequately protected places, such as for example, fireproof lockers and / or safes;
- the storage of removable backup media must provide with the correct labelling.

3.5.4 System log management

The tracing and subsequent consultation of the logs represent essential elements for monitoring and guaranteeing the security of the company IT system, as they allow processing and analysis (both in real time and at different times) on the activities carried out on the information systems. In particular, the tracking allows to support and optimize the following activities:

- reconstruction of events;
- attribution of responsibilities;
- analysis and understanding within the Group of who uses the systems and the type of use made;
- compliance with laws, regulations and standards.

The integrity, availability and confidentiality of the logs over time must also be guaranteed in order to ensure effective management of the service for the purpose of reconstructing an event. Users of the IT system must be aware that the use of company systems is subject to systems for tracking and consulting logs (in compliance with the regulations in force reported in paragraph 3.13 Compliance with regulations).

3.5.5 Cloud services security

Multi-tenant cloud allows Cerved Group companies to share data in a public or private cloud. Each tenant's data must be isolated and inaccessible to other customers.
Group companies define the requirements for network segregation to achieve tenant isolation in the shared environment of a cloud service and verify, with the support of the cloud service provider if necessary, that these requirements are met, including:

- The separation of resources in use by Cerved Group companies in multi-tenant environments;
- the separation of the internal administration of the cloud service provider from the resources in use by Group companies.

When configuring virtual machines, Cerved Group companies and cloud service providers must ensure the proper implementation of technical measures (e.g., anti-malware and log collection) for each virtual machine used.
In addition, Cerved Group companies must ensure that:

- an information security policy for the virtual network configuration is defined and documented, consistent with the information security policy for the physical network;
- appropriate logical segregation of Cerved Group companiesdata, virtualized applications, operating systems, storage and network is applied;
- risks associated with the execution of software provided by Cerved Group companies within the virtual machines offered by the cloud service provider are considered.

3.6 ACCESS CONTROL

Access to information must comply with the "need-to know" principle, i.e. the sharing, access and communication of information must be guaranteed only to personnel who, previously identified and authorized for a specific period of time, have actual need for the performance of their work duties.
Access to the systems must be allowed following identification through a user identification code (user id) and following authentication using a password. These mechanisms must be accompanied, if necessary, by additional authentication tools (strong authentication systems).
The safety rules set out in this section apply, except in special cases to be assessed if necessary, to all types of users who use the Group's technological infrastructure.

3.6.1 Users management

The entire life cycle of access authorizations to IT systems (creation of user accounts, modification of user accounts and the removal of the user account), must be defined and formalized in order to reduce the risk of unauthorized access to information. In particular, in order to ensure the security of information, the following constraints must be met:

- the request for the creation of a new user and the relative generation must be carried out only by the personnel in charge;
- the user id must be created following a nomenclature standard such as to:
  - not provide information on the type of activity that is carried out by the person to whom the user refers;
  - not provide information on the privileges associated with the user.
- as far as possible, the creation of multiple users assigned to the same person for access to the same system must be avoided and in case of actual need these users must be authorized and appropriately registered and documented;
- the persistence of the validity of the users must be checked periodically by the structures in charge;
- the modification of a user must only be carried out by the personnel in charge, upon explicit request by authorized figures. Particular attention must be paid in the event of a change in the user's use so that, at the end of the change, the authorizations related to the previous authorization profile do not remain;
- the users of the internal employees of the Group must be deactivated at the end of the employment relationship with the Group Companies or if the collaboration relationship is temporarily suspended. Any exceptions to this general rule must be formally documented and authorized;
- the users assigned to personnel outside the Group must be deactivated in the event of withdrawal from the service contract or in the event of termination of the employment relationship with the external company by the employee or temporary suspension.

The creation of service users must be limited, especially where used by several individuals. If it is necessary to create service users, they must respect the following constraints:

- obtain approval from the relevant Security structures;
- assign and formalize the responsibility of the user to a single individual;
- define the methods for management, extension to other users, tracking over time, monitoring and constant updating of assignments;
- allow, where possible, access only from certain workstations.

As for cloud services, Cerved Group companies must verify that the cloud service provider's procedure for assigning authentication information meets the same requirements.
In addition, Cerved Group companies must formalize an access control policy that defines the requirements for the Group companies users' access to each cloud service; while the cloud service provider must provide Cerved Group companies with user registration and de-registration functions and specifications for the use of these functions.

3.6.2 Authentication techniques

In order to ensure that access to information is allowed only to authorized personnel and only for the permitted purposes, measures must be activated to limit access to the Group's IT systems. In particular:

- identification and authentication mechanisms must be in place that allow the control of logical access to IT resources, in order to ensure that these resources are accessed and used only by authorized personnel;
- systems and procedures must be established for the safe use of the services provided by the Group (e-mail, Internet access, ...) and of the applications and related operating systems.

With specific reference to the Cloud services:

- authentication techniques have to be used to authenticate the users of Cerved Group companies accessing Cloud resources. Specific care has to be paid on the authentication techniques for system administrators;
- Cerved Group companies must ensure that access to information in the cloud can be restricted in accordance with the access control policy and that such restrictions are enforced. This includes restricting access to cloud services, cloud service functions, and data maintained in cloud services. In particular, specific controls to mitigate the identified risks must be in place, whether such controls are provided by the Group companies or by the cloud service provider;
- The cloud service provider must ensure that any use of utility programs capable of circumventing normal operational or security procedures is strictly limited to authorized personnel, and that the use of such programs is reviewed and monitored regularly.

The user systems must be set up in such a way as to comply with the following security requirements on how to manage the password:

- provide the mandatory change of the initial password on first use;
- provide the choice of a secure password that complies with the applicable legislative requirements in terms of length and complexity (see paragraph 3.12 Compliance with regulations);
- provide the periodic change of the password by the user;
- provide automatic user blocking mechanisms following a limited number of access denied attempts;
- mask the password characters while typing;
- prevent unauthorized access to the user management systems and related passwords.

3.6.3 Management of roles and privileges

The definition of roles must only be carried out by the responsible corporate structures. In order to carry out this activity, the corporate structures in charge must evaluate at least the following attributes for the users associated with internal employees of the Group:

- the Group Company and the Organizational Unit to which the user belongs;

- the professional figure (defined by duties, role and company position within the Organizational Area to which they belong) associated with the user;
- any particular responsibilities additional to those envisaged by the professional figure (replacements, delegation of certain decision-making or authorization powers, etc.).

To define the roles to be assigned to the users associated to external personnel, at least the following attributes must be evaluated by the company structures in charge, based on the supply contract:

- the external company to which they belong;
- the reference to the supply contract, in particular the period of validity of the contract itself;
- the internal reference manager employed by the external company.

In defining and assigning roles, at least the following elements must be taken into consideration:

- the principle of separation of duties (Segregation of Duties);
- the principle of minimum privilege (Need to Know);
- compliance with security restrictions and any obligations of legislative or contractual origin (see paragraph 3.13 Compliance with regulations);
- compliance with the Group's organizational model in place.

The roles that regulate access to applications must comply with the following constraints:

- be defined according to an authorization model based on the level of responsibility assigned to each professional figure;
- provide for specific roles for authorization-type operations;
- the modification of the profiles must be tracked and a track must also be kept of who made the modifications on the profiles;
- the access profiles associated with the various users must be evaluated and reviewed periodically by the appropriate structures.

3.7 MANAGEMENT OF CRYPTOGRAPHIC KEYS

Cerved is responsible for managing the encryption systems adopted both for the provision of internal services and for customers, and must ensure that the implementation and operations relating to the encryption systems comply with the Cryptography and Key Management Guidelines.
A documented process for managing cryptographic keys should be established and include:

- Key generation using approved key lengths.
- Secure and approved methods for distributing, activating and archiving, retrieving and replacing / updating cryptographic keys.
- Immediate revocation (deactivation) of cryptographic keys, for example when an employee leaves the organization
- Immediate revocation (deactivation) of cryptographic keys, such as when an employee leaves the organization
- Recovery of lost, damaged or expired cryptographic keys.
- Disposal of cryptographic keys that may have been compromised, for example by disclosure to an external party
- Backup / archive of cryptographic keys and maintenance of cryptographic key history (eg to allow access to backup or archived information).
- Definition of retention periods for cryptographic keys and key change processes;
- Processes for limiting access to cryptographic keys to authorized persons only.

Ownership of cryptographic keys should be assigned to key owners, who should be aware of their responsibilities in the use and protection of the keys (and where necessary to disclose the keys).
Cryptographic keys must be protected against access by unauthorized persons or applications, accidental or malicious destruction, and unauthorized copying.

3.7.1 Confidentiality, Integrity and Authentication

The data, depending on the type of information processed and in line with what is defined in the "information classification policy", must be subjected to evaluation by the same owner, in order to define the need for the adoption of encryption to ensure confidentiality.
Data integrity (including encryption keys) must be protected by encryption both during transmission and storage, in order to meet the principles of Security By Design and By Default described in the Security by Design and by Default Guidelines and Safe Software Development according to the risk associated with the type of information processed.
Use of cryptographic controls for authentication purposes must comply with authentication requirements, such as authentication method and protocol, storage and validity of authentication credentials. Therefore, cryptographic authentication credentials (for example, private keys) must be kept secret.

Insiders are those who can gain access to confidential data of Group companies, compromising their confidentiality, integrity and availability. The following are the main risks attributable to insiders:

- disclosure of sensitive data;
- theft of intellectual property;
- fraud;
- insider trading;
- violations of compliance with internal and external regulations.

It is the responsibility of Cerved Group companies to put operations in place in order to manage risks from insiders, based on the following principles of:

- transparency;
- configurability;
- usability.

3.7.2 Data retention

If media-level encryption is required, the storage media must be encrypted with full-disk encryption.
If file-level encryption is required, however, the following encryption methods are used:

- File-based;
- File compression tools (eg WinZip, etc.) compatible with FIPS 197, using the AES 256-bit method.

In some cases, both the media and the file can be encrypted simultaneously.

Regarding cloud services, the cloud service provider must inform Cerved Group companies of the geographical location and countries where data may be stored, even temporarily.

3.7.3 Data transmission

When encryption of the transmission is required, depending on the type of data transmitted, only the protocols present in the Guidelines for Encryption and Key Management 6.1 Annex A must be used. If the risk associated with the data transmitted is high, both the transmission and the files can be encrypted simultaneously.
In the case of sending emails outside the perimeter of the Company (for example Customers, Suppliers etc.) where encryption is necessary but not supported by the recipient, it is necessary to use alternative methods of secure data exchange (for example Winzip with password). Connections to customers and third parties must use appropriate encryption by default, where necessary.

3.7.4 Protocols and versions

You can only use the protocols and versions that meet the requirements, which are specifically described in the Cryptography and Key Management Guidelines document (paragraph 4.2.4 Protocols and versions and Annex A)
The protocol must be used to its maximum encryption capacity on all transmission components, in order to satisfy the principles of Security By Design and By Default described in the Security by Design and by Default and Secure Software Development Guidelines, and in any case depending on the type of data processed and depending on the evaluation performed by the owner of the data itself.

3.8 KEY MANAGEMENT PROCESS

A key management system must be used to centrally manage and secure cryptographic keys. Access to keys within the key management system is permitted only if necessary or requested by the requesting user's function manager. All access to the key management system and stored keys must be logged and monitored. The effectiveness of encryption depends on the correct management of the keys, which must be administered securely throughout their life cycle.

- **Creation of keys**

Cryptographic keys must be generated within a cryptographic module. Cryptographic modules Software and / or firmware-based must be at least FIPS 140-2 level 1 compliant. HSM cryptographic modules must be at least FIPS 140-2 level 2 compliant.

- **Distribution of keys**

A key management system must address the secure transmission of keys from their storage space to the device that requests them, in accordance with the encryption algorithms and the size of the keys. Key Wrapping should be used when keys are exchanged with symmetric encryption. Asymmetric private keys (to be used for signing or encryption) are not distributed. An inventory of all keys used must be compiled and maintained.

- **Memorization**

Where technically feasible, asymmetric private keys (to be used for signing or encryption) must be generated directly on the device where they must be stored and protected by a password or hardware token. Keys should never be stored in an unencrypted format. Keys stored in offline databases are encrypted with key encryption keys before exporting the master key, where possible. The length of the key encryption keys (and algorithm) must be equal to or greater than the length of the protected key.

- **Periods of use, rotation, storage and review**

The keys used for short-term or long-term data encryption should be stored according to local data retention needs and the business needs of the encrypted data. The Cerved IT area is responsible for defining and implementing the annual reviews of the algorithms and procedures relating to key lengths.

- **Update and renewal**

Each individual key subjected to a renewal process must have a security level equal to or higher than that of the original key.

- **Backup and restore**

Based on the types of data that Cerved wants to encrypt, it is necessary to determine the keys to be included in the backup process. A key recovery mechanism is provided to ensure access to the encrypted data in the event of the key being lost or damaged. This mechanism could include backing up keys or using a master key.

- **Disposal**

A key must be decommissioned when its validity period has expired or when it is suspected that the key has been compromised. The disposal keys must not be used and / or made available in production. While retention of the withdrawn keys may pose a security risk, the withdrawn keys must be prepared for destruction after it is determined that the key is no longer needed.

- **Destruction**

Keys must be securely destroyed when there is no need to keep secure data. Keys are destroyed in accordance with FIPS 140-2.

- **Protection**

Private keys must be protected by the key management system to prevent unauthorized use, disclosure, and modification. Public keys must be protected by the key management system to prevent unauthorized changes.

3.9 ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS

The Change Management process provides for the approval for each request for change that concerns the supporting IT infrastructure (software, hardware, network, etc.). The goal is to ensure that standard methods and procedures are used for an efficient and prompt management of all application and IT infrastructure changes, in order to minimize the impact and accidents involving the services provided.

3.9.1 Security rules relating to the Change Management process

The development and maintenance of information systems must be carried out in such a way as to minimize the risk of service interruption or malfunction, while ensuring the integrity and confidentiality of the information at the same time. In order to guarantee these properties, it is necessary to evaluate when opening new projects the execution of an analysis to evaluate any security implications. In particular, each new service that requires the implementation of a new application or modification to an existing one must provide for the execution of the following phases and compliance with the related security constraints:

- *definition of user requirements:* provides a clear definition of requirements through the identification of user requirements and security requirements;
- *technical* and economic feasibility: provides a technical and economic feasibility study by the structures involved, in collaboration with the IT Department. In particular, the costs and benefits deriving from the new application or modification will have to be analyzed.
- *functional* and technical analysis: provides a clear functional and technical analysis. This analysis must contain:
  - ✓ the input controls;
  - ✓ the output controls;
  - ✓ the identification and authentication mechanisms for accessing information;
  - ✓ a risk analysis where possible threats to the new application or modification are analyzed and the appropriate countermeasures are highlighted;
  - ✓ the security criteria to safely configure the application support platforms;
  - ✓ the requirements (methods and frequency) for saving data and restoring applications;
  - ✓ the architectural design that highlights the integration of new applications and services with the existing reference architectural context;
- *development and testing of applications or modifications*: the test activities must be exhaustive in order to verify the correct functioning of the application. Tests of applications or changes must be formally approved by the appropriate organizational structures involved;
- *transfer of programs to the production environment*: the transfer of a new application or an update from the test to the production environment must be approved by the appropriate organizational structures. In particular:
  - ✓ the transfer of a new application or an update from the test environment to the production one must be carried out by the appropriate structures;
  - ✓ the transfer of a new application or an update to production must be followed by detailed tests in order to ensure that there have been no errors regarding the information, with particular reference to the integrity of the data;
  - ✓ technical and procedural criteria must be adopted in order to keep track of the different versions of the applications in production so as to be able to easily trace back to previous versions in case of need.

- *emergency changes*: they must be allowed where there is a blocking criticality for the provision of the service in production. In particular, it has to be possible to document the reasons that led to the change. Once the emergency changes have been completed and the interrupted service provision has been restored, the structures concerned must be informed;
- *documentation*: the documentation on applications must be kept constantly updated. In addition to the project documentation, the following documents must be provided:
  - ✓ request;
  - ✓ evaluation of the request;
  - ✓ approval of the request;
  - ✓ outcome of the test activities and relative acceptance;
  - ✓ approval of the production release.

With regard to the cloud service, the change management process of the Group companies must take into account the impact of any change made by the cloud service provider, which is required to provide the Group companies with information regarding changes to the cloud service that may affect it, by means of a communication that includes at least the following:

- categories of changes;
- expected date and time of the changes;
- technical description of the changes to the cloud service and underlying systems;
- notification of the start and completion of the changes.

3.9.2 Systems Maintenance (Configurations and Patch Management)

All corporate infrastructure must be maintained and configured in order to reduce infrastructure vulnerabilities, applying all appropriate security measures based on the specific system. In particular:

- an analysis of the vulnerabilities that potentially affect the systems must be carried out, with information on their criticality, on possible impacts on operations and on applicable countermeasures for mitigating the risk associated with the vulnerability;
- systems identified as critical must be subjected to periodic vulnerability tests in order to identify possible security flaws in the system configuration;
- the identification of vulnerabilities must take place through the execution of selective Vulnerability Assessments on a single asset or on a wider perimeter (carried out internally or externally) or following the detection of attacks / reports coming from the Incident Management process (see paragraph 3.8 Management of IT security events and incidents);
- the identified vulnerabilities must be analyzed in order to implement the appropriate remedial activities for their resolution and mitigation. These actions must be implemented promptly and verified in order to validate their level of effectiveness;
- mechanisms must be implemented for the management of system configurations capable of keeping track of changes made to the systems themselves;
- the administration tools and commands must be able to be used only by users with an administration profile;
- secure protocols must be used for access to systems capable of guaranteeing the confidentiality and integrity of communications (eg. SSH, Https);
- the infrastructure must provide for the use of automatic filtering tools, in order to exclude the presence of viruses or other dangerous components and allow the reduction of risks associated with the use of e-mail and Internet services;

- on each system, where applicable, anti-virus software must be installed, which must be configured as follows or with more restrictive settings:
    - ✓ the software must not be able to be disabled by the user;
    - ✓ the software configuration must not be able to be changed by the user;
    - ✓ real-time file scanning must always be active;
    - ✓ the antivirus software must be updated periodically;
    - ✓ periodic automatic scans of the system must be scheduled;
    - ✓ the scan should include the memory of running processes and if possible all connected removable media.
- when installing and configuring the operating system and / or application software, system hardening procedures must be followed which include, among other things, the modification of the default credentials;
- the operating system and application software present in the systems must be updated with the security patches issued by the relevant suppliers whose compatibility with the operation of the systems themselves must be ascertained. The installation of the released security patches must be planned taking into account the severity of the vulnerability that is resolved by the patch and the operational needs of the Group;
- each vulnerability or patch found must be adequately analyzed and assessed from the point of view of the impacts it may have on the affected assets, with the assignment of the priority of intervention shared with the security structures in charge;
- if it is not possible to install the updates, it is necessary to keep track of the patches not installed and the reason why the installation was not carried out.

The checks carried out on the purchased software, on new versions and on security patches must include at least the following security checks:

- any presence of viruses or other malicious code on the storage media containing the software;
- vulnerability tests to identify any security flaws;
- testing to ensure that there are no incompatibilities that cause a negative impact on the organization's operations or safety.

The checks and security control carried out and the relative results must be appropriately documented.

3.9.3 Standard for secure code development

The security features of the software must ensure the confidentiality, integrity and availability of the data and information processed according to the relative level of criticality. The software must offer security event tracking and consultation capabilities.
An access control model to the software, its functionalities and the processed data must be implemented.
In the software development phase, the safety indications relating to the specific platform / programming language used must be considered. In particular:

- in the software development phase, no already developed codes (APIs, modules, macros, etc.) affected by known vulnerabilities or considered unsafe must be used;
- the software must include checks on the validity of the incoming data, which must comply with the type, format and content envisaged;
- the software must be implemented in a way to prevent unmanaged exceptions at runtime;

- in the event of an error during the execution of the software, generic messages must be displayed to the user (where possible), without technical details that may provide information on the technologies used and the software architecture, such as to jeopardize security;
- procedures and controls must be defined to check for the presence of potentially harmful or vulnerable code in applications;
- the software must ensure the separation of administrative functions from those of ordinary operations. The administration functions must be accessible following a specific identification, authentication and authorization process;
- any connections to databases must be made through accesses following the principle of separation of duties and the minimum privilege necessary for carrying out operations;
- in the source code of the software (including any comments to the code) confidential information must not be stored, understood as personal / sensitive data, critical data for the Group and / or information whose disclosure may impact on security.

3.10 MANAGEMENT OF IT SECURITY EVENTS AND INCIDENTS

The incident management process defines the methods for managing events that impact the normal execution of company activities. The primary objective of the process is to restore normal operations as quickly as possible and to minimize the impact on the operational activities of users of the information system, promptly and appropriately addressing incidents.
In addition, the following objectives must be achieved:

- ensure timely notification to company management of the opening and closing of any relevant event;
- safeguard the company assets;
- quickly identify an emergency situation, implementing the most suitable strategies to contain its consequences;
- reduce false alarms (called “false-positives”) as much as possible by identifying with certainty the circumstances of the emergency;
- collect the necessary information (evidence) to support any legal action;
- comply with industry best practices and current regulations;
- analyze the incident by identifying the errors, weaknesses and strategies adopted to manage it, improving the timeliness of intervention and the response to similar future events.

Reporting IT security errors or incidents must be timely enough to take appropriate countermeasures and limit the damage. A process must therefore be defined and implemented to define the methods of detection, classification, management, treatment and resolution of IT incidents, determined by the occurrence of events capable of compromising one or more security features in terms of confidentiality, integrity and availability of information processed by IT systems.
This process must include the definition of roles and responsibilities in reporting, escalation, containment and elimination of the threat.
To achieve proper IT incident management, possible critical events must first be identified and categorized, such as:

- unavailability of services;
- systems malfunction or overload;
- unauthorized variation of system configurations;
- hardware malfunction / break;
- theft;
- data loss;
- violation of company policies and procedures;
- violation of mandatory regulations;
- violation of physical infrastructure;
- access violation.

After returning to normal operation, the documentation of the accident and its solution must be prepared and the causes that produced the accident must be analyzed, identifying any vulnerabilities to avoid subsequent similar events.

It is also necessary that this process ensures the correct collection, management and historicization of the evidence and the main information, both for the need of internal company analysis and, if necessary, for investigative and / or legal needs.
Company management must be periodically informed with a summary of the relevant security incidents that occurred during the period.

3.11 BUSINESS CONTINUITY MANAGEMENT

Business continuity management provides the preparation of an emergency plan capable of ensuring the continuity of vital operations in the presence of events that compromise the functionality of the information system, in order to ensure the return to normal operations within an acceptable time. This process takes input from:

- identification of risks (for example natural disasters, unavailability of IT systems, etc.) conducted through Risk Assessment activities in order to determine the impact of any interruptions due to disastrous events;
- definition of critical processes, through the business impact analysis (BIA) which evaluates company processes / systems according to their criticality and provides an estimate of the maximum time of sustainable unavailability.

One of the key components for business continuity management is the Disaster Recovery Plan (DRP). This plan must consider the disastrous events capable of causing significant damage in the continuity of IT services in order to define the procedures for reactivating the IT services deemed critical within the acceptable recovery times. The elements examined by the DRP are made up of the resources of the computer system including hardware, software, connections, databases, IT personnel, documentation, alternative site and organization.

The following are the main requirements for developing, managing and maintaining a business continuity plan:

- involvement of top management in the preparation of the plan;
- identification of critical processes, for which high levels of continuity must be guaranteed;
- identification of the internal / external personnel to be involved in the plan since the role and individual or group responsibility to be covered must be indicated for each person or group involved in the provision of the service;
- identification and involvement of relevant suppliers and counterparties;
- identification of recovery times; it must be formally stated in how long (hours and days) the service will be restored;
- definition of the recovery strategies adopted according to the event and the technology used;
- drafting of operating procedures for the personnel involved;
- evaluation of the maximum time for which the service can be provided;
- identification of the assets necessary for the operation of the plan within the established times;
- data recovery methods (backup / restore);
- any insurance policy that covers the higher costs due to emergency operation and the loss;
- identification of logistical needs in terms of spaces and work places to carry out the operations considered vital for business continuity;
- guidelines for the conservation of paper documents and storage media;
- test of the plan;
- staff training;
- periodic updating of the business continuity plan.

3.12 COMPLIANCE WITH REGULATIONS

Compliance with laws, policies and company regulations that express IT security obligations must be ensured and a structured audit process for IT systems implemented. In particular, an IT Security Compliance process must be implemented that allows to direct and control over time the maintenance of compliance with the relevant IT Security obligations deriving from:

- national and international laws;
- directives of the Authorities;
- sector specific regulations;
- business requirements;
- contractual obligations;
- service agreements;
- reference standards.

This process aims to allow the company to manage IT Security Compliance needs, as part of the corporate compliance management process, by identifying and harmonizing compliance obligations, requirements and security measures. The process must also define the monitoring needs for maintaining compliance over time by implementing procedures and tools to perform compliance checks based on the collection and storage of evidence.

Regarding cloud service, Group companies must ensure that the cloud service provider provides a process for responding to requests from authorities (e.g., subpoenas, official investigations or legal proceedings) and respective ways of sharing information to support investigations and forensic activities.

4 Glossary

System administrator	The professional figure in charge of the management and maintenance of a processing plant and / or its components.
Asset	Tangible and intangible value belonging to a property.
Authentication	Process through which the veracity of the identity declared by a person is verified.
Backup	Copies of a set of data made with the aim of replicating information avoiding accidental loss in the event of breakdowns or tampering.
Confidentiality	Guarantee that data and information are accessed only by authorized personnel.
Personal data (pursuant to Regulation 679/2016 -GDPR)	Any information relating to an identified or identifiable natural person ("data subject"); it is considered identifiable the natural person who can be identified, directly or indirectly, with particular reference to an identifier such as the name, an identification number, location data, an online identifier or one or more characteristic elements of his physical identity, physiological, genetic, psychic, economic, cultural or social;
Availability	Feature according to which a data is always accessible and usable according to the times and methods provided.
Incident	Unwanted and / or unforeseen security events that have a significant likelihood of compromising operations, threatening information security.
Integrity	Characteristic of a data with respect to its authenticity and completeness.
Log	Chronological recording of certain events that occur on a system.
Threat	Possible cause of an unwanted accident, which can cause damage to a system or organization.
Segregation of Duties	Fundamental principle within the corporate IT organizational model. Responsibilities must be defined and duly distributed avoiding functional overlaps or operational allocations that concentrate activities on a single subject in order to avoid operational risks and / or any conflicts of interest.
Computer system	Installation of Information Technology consisting of several hardware and software components in a known and defined operating context, aimed at satisfying the requirements of specific groups of users (for example: a data center, a LAN, a PC or stand-alone WS, etc.) .
Third Parties	Partner, IT Service Provider, Customer, Supplier.