Information Security Policy for Suppliers

CENTRIC

Information Security Policy for Suppliers

SCOPE

The purpose of this document is to define the information security requirements in relationships with Suppliers, in order to mitigate the risks associated with access to IT CENTRIC assets by external parties.

INFORMATION SECURITY POLICY

IT CENTRIC S.p.A. implements and maintains an Information Security Management System in accordance with the requirements specified in the ISO/IEC 27001 standard and in EU Regulation 2016/679, in order to guarantee:

1. **Confidentiality:** ensuring that the information is accessible only to duly authorized individuals and/or processes and that the information is not made available or disclosed to unauthorized persons or entities.
2. **Integrity**: safeguarding the consistency of the information from unauthorized modifications and guaranteeing that the information does not undergo modifications or deletions following errors or voluntary actions, but also following malfunctions or damage to technological systems.
3. **Availability:** ensure that authorized users have access to information and associated architectural elements when they request it.
4. **Control:** ensure that data management always occurs through safe and tested processes and tools.
5. **Authenticity:** guaranteeing a reliable provenance of the information.
6. **Privacy:** guarantee the protection and control of personal data.

The lack of adequate levels of information security may lead to damage to IT CENTRIC's business, lack of customer satisfaction, the risk of incurring sanctions linked to the violation of current regulations as well as economic, financial and image damage to the company. company and the underlying supply chain. The Management of IT CENTRIC is strongly committed to making all the people who work for and with the company highly responsible in guaranteeing the rigor of their work to fulfill the assigned tasks with the utmost attention.

For these reasons, the IT CENTRIC Management promotes all the necessary actions so that the processes and activities are oriented towards achieving the following objectives:

- Identify security needs through risk analysis, in order to gain awareness of the level of exposure to threats of your information system.
- Implement the actions necessary to mitigate the identified risks and the most suitable security measures.
- Guarantee maximum security of customer information, in terms of confidentiality, availability and integrity.
- Provide operational continuity to critical services even following serious accidents.

- Protect the rights and interests of all those who interact with the company (customers, employees, collaborators, third parties, etc.).
- Safeguard the interests of investors and partners.
- Ensure an excellent level of service.

Suppliers must ensure that all staff work to achieve the aforementioned security objectives in information management and use the most appropriate technologies to ensure compliance with this policy.

SECURITY REQUIREMENTS FOR THE TRANSMISSION OF INFORMATION

The exchange of documents and information between IT CENTRIC and the Supplier must take place in a controlled and secure manner in accordance with the classification and labeling system adopted by the company and to which the Supplier must adapt. This system provides in particular the following levels of classification of information:

1. in the public domain (does not require any labelling)
2. for internal use
3. reserved (or confidential)
4. strictly reserved.

If confidential information is to be discussed or exchanged between IT CENTRIC and the Supplier, or between a Supplier and third parties, the parties must first ensure that they have signed a confidentiality or non-disclosure agreement.

For digitized information, transmission must take place in an encrypted manner via FTPS, email or PEC using the TLS protocol; in the body of the email message there must be a standardized header warning of the confidentiality/confidentiality of the message; e-mail attachments can be encrypted with a password to ensure greater protection for the Confidential Information deemed most critical (e.g. particular personal or judicial data).

Confidential information that is communicated in verbal form must be considered as such when the person communicating it indicates it as "confidential" to the other party.

The supplier is committed to implementing solutions to protect information from fraudulent activities, contractual disputes, disclosures and unauthorized modifications. In the event of a need for access to IT CENTRIC assets by the Supplier, the same must be authorized in advance and informed of the methods of use of the same, which must be scrupulously followed and will be subject to the controls provided for by IT CENTRIC security policies.

For Suppliers associated with ICT supply chain services and products, the Supplier must undertake to comply with IT CENTRIC requirements to address information security risks by requesting a copy of the applicable policies in advance from IT CENTRIC.

MONITORING AND REVIEW OF THE SERVICES PROVIDED BY THE SUPPLIER

In order to ensure control over all security aspects relating to critical information or information processing facilities, IT CENTRIC monitors the performance levels of the service provided and

received by the Supplier. This process verify compliance with the agreements. Audits may be conducted on your Suppliers, together with the review of supply relationships.

MANAGEMENT OF ACCESS TO THE NETWORK AND NETWORK SERVICES.

If the service requested from the Supplier requires operating within the IT CENTRIC network, access will be provided in the following ways and only for the services for which they have been specifically authorized by individual agreements with IT CENTRIC:

- The Supplier must communicate the names of the operators who will be previously approved by IT CENTRIC
- They will be assigned an authentication credential consisting of userID and password to be changed upon first login.

CONTROL OF LOGS The user (operator of the Supplier) is subject to control of the Logs by IT CENTRIC ICT staff.

PASSWORD MANAGEMENT

Users (operators of the Supplier) undertake to respect the criteria for creating, storing and managing access credentials indicated in this document.

Passwords must be at least eight characters long, must not contain references relating to private or professional life that can easily be traced back to the user, must contain a combination of numbers and/or special signs, letters, uppercase and lowercase, must not be the same as precedents.

The password must be changed every six months; in the case of processing of particular personal data and judicial data, the frequency of the change must be reduced to three months.

The password is strictly personal and must not be communicated and/or shared with any other person inside or outside the organization. Users must pay attention to providing their access credentials, responding to suspicious emails and/or clicking on links while browsing the web or from the same email message received, in order to combat possible IT fraud (e.g. phishing, theft of identity, etc.).

Each user is responsible for all actions and functions performed by his account. If there is reasonable certainty that the assigned credentials have been used by third parties, the user must report it to IT CENTRIC staff. For the safe storage of access credentials, it is advisable to avoid storing them on paper documents or in files kept within the workstation.

PHYSICAL ACCESS

IT CENTRIC has set up a perimeter control system for access to the headquarters, offices and rooms where information is processed. Access is permitted only to authorized personnel, so if the Supplier needs to access the offices or premises of the IT CENTRIC headquarters, they must have specific authorization and comply with the physical and environmental security measures applied.

SAFETY EVENT COMMUNICATION

Every report of vulnerabilities, events and security incidents detected during the activities carried out by the Supplier must be formally communicated also by email to the IT CENTRIC contract contact person for the subsequent management and resolution of the problem.

SANCTIONS

Failure or delayed compliance with the provisions of this company policy and/or the contract stipulated between the parties, which causes economic, financial and image damage to IT CENTRIC and the underlying supply chain, will result in the consequent obligation of compensation in favor of IT CENTRIC, in addition to any administrative pecuniary and/or criminal sanctions provided for by the GDPR Regulation 2016/679 and/or by current legislation.