# INFORMATION SECURITY POLICY

# IN THE MANAGEMENT OF CLOUD SERVICES

**Infoteam VAT 01538680685**
**Viale Pindaro, 14 - 65127 Pescara (PE)**

## SOMMARIO

# 1 CLASSIFICATION AND DOCUMENT REVIEWS

| **DOCUMENT CONFIDENTIALITY CLASSIFICATION** | | | | | |
|---|---|---|---|---|---|
| **Confidental** | | **Internal** | | **Public** | **x** |
| **REVIEW STATUS** | | | | | |
| **Rev. N°** | **DatE** | **Reason of the review** | **Processed** | **Verified** | **Approved** |
| 1 | 25/07/2023 | Issuance | IMS Manager | SC Manager | MGT |

# 2 INTRODUCTION

This policy summarizes the commitment, expressly declared by the organization, to satisfy the requirements of the standards UNI EN ISO 27001:2022, UNI EN ISO 27017:2015, UNI EN ISO 27018:2019, GDPR (UE Reg. 679/2016 and Italian legislation – D. Lgs. 196/2003 updated by the D. Lgs. 101/2018 e s.m.i.) and to integrate the general policy IMS-DOC-52-01 of the management system for information security, in the field of design, development, evolutionary maintenance, provision and support for IT infrastructures, applications and cloud services provided in Saas mode (software as a service), consultancy services for regulatory compliance and technical services for assistance and IT security.

# 3 AIM

This document defines, in coordination with the general policy IMS-DOC-52-01, issued by Infoteam Management, the general directive criteria relating to the cloud services provided in order to protect the data processed and stored therein, including personal data.

The criteria established therein derive from the best practices referred to in the reference standards (ISO 27017:2015 and ISO 27018:2019).

# 4 APPLIED POLICY

## 4.1 Overview

The information generated through cloud services reside in the logical infrastructure that makes up the Saas services (IAAS infrastructure, operating system, middleware,

application and database).
This information can be traced back to the following types:
a) Structural elements of the cloud and their support.
b) Configuration of the logical environments assigned to customers.
c) Information and application data of the customers.

Infoteam employees and collaborators have access exclusively to the information referred to points a) and b), while they have no possibility of accessing type c) elements unless explicitly authorized by the customer for assistance, maintenance or update reasons.
Access to the information referred to points a) and b) above, for the execution of administrative operations, is possible exclusively for Infoteam technicians (to be understood as developers and systems engineers) via protected and encrypted connections (SSH / SSL).
Access to the information referred to point c) is possible, where provided for by the contract conditions, only for Infoteam technicians and always via protected and encrypted connections.
The security (confidentiality, integrity, availability) of the data is guaranteed to both external (e.g. cyber attacks) and internal threats (e.g. unfaithful employee).
The end customers are responsible for the contents of the data inserted in the cloud services provided and for all activities attributable to their accounts. They are also responsible for using the SaaS services offered adopting all the most suitable measures for security, protection and saving of their accounts and contents.
For each cloud service Infoteam undertakes to ensure the security of the operating environment (operating system, middleware etc...), of the application and of the database and therefore of the confidentiality, integrity and availability of the data.
To this end, safety practices and procedures have been planned and provided. They are independently validated through third-party assessments. Furthermore, they are aimed at ensuring the continuous verification of the security posture as well as the monitoring of events and results in a documented and, therefore, demonstrable way.

#### 4.1.1 *Control programs*

Infoteam identifies and defines the necessary control programs based on certifications, laws and regulations.
The Certifications / attestations are issued by a third-party audit body. Laws and regulations are specific to the industry or function performed.

The infrastructure and services are approved for use to guarantee the aforementioned compliance. For this reason the cloud environment is subjected to continuous checks.
Among the main standards taken into consideration for compliance and the planning of the control programs, there are:
ISO 27001:2022 - It is a widely adopted global security standard that defines the requirements for information security management systems. It guarantees a systematic approach to the management of the company and the customer data based on periodic risk assessments;
ISO 27017:2015 - It provides guidelines on cloud computing cyber security aspects and recommendations about the implementation of cloud-specific information security controls. It complements the guidelines of ISO 27002 and ISO 27001. This code of practice provides guidelines on the implementation of information security controls that specifically refer to cloud service providers;
ISO 27018:2019 - It is an international code of best practices focused on protecting personal data in the cloud. It is based on the ISO 27002 information security standard and provides guidelines for implementing ISO 27002 controls that apply to personal information in the public cloud.
Infoteam compliance demonstrates the availability of a system of controls specifically aimed at protecting the privacy of the contents entrusted by the customers.

### *4.1.2 Data security with respect to hardware failures*

The logical infrastructure that allows the management of the information described in points a), b) and c) is created according to functional models of high reliability and redundancy on distinct and independent devices, which guarantee copy and replication of the data according to specific policies.
This is possible thanks to the choice of ISO 27001 certified cloud data center sub-suppliers and therefore able to demonstrate the reliability and compliance of the respective ICT infrastructures, all equally equipped with high security and redundancy standards.

### *4.1.3 System security against intrusion*

The physical infrastructures used for hosting the cloud services provided by Infoteam belong to ISO 27001 certified sub-suppliers chosen according to certification, reliability, performance and security requirements.
These infrastructures meet the physical security criteria referred to in ISO 27001 and therefore guarantee the adoption of the measures necessary to protect the

environments from intrusion, as well as the measures aimed at separating the networks, systems and data of the different tenants that use the infrastructure.
Infoteam technicians do not access the data centers. The access is reserved only to authorized technicians of cloud providers.

#### *4.1.4 Data security*

The data managed by Infoteam on behalf of customers can be replicated on distinct physical infrastructures in independent and geographically different data centers.
This is to guarantee redundancy and timely resumption of services in the event of any interruption.

#### *4.1.5 Safety of operations*

Internal staff with access to cloud services for assistance/maintenance/administration reasons is prohibited from:

- keeping access sessions to the infrastructure open during their absence
- storing in any form (e.g. on file, on browser, written on paper) the access credentials to the infrastructure outside of the company password manager.

#### *4.1.6 System security against Malware*

The software installed on the cloud systems are only those serving the applications (e.g. nginx, apache etc...), downloaded from authenticated and official sources after checking the correspondence between the available package and the downloaded package (via hash).
Only Infoteam system engineers are authorized to carry out such installations safely. The possible presence of malware or other vulnerabilities is periodically checked through the Vulnerability Assessment process

### ***4.2 Data management***

Infoteam customer digital data can be divided into two categories:

- Platform data
- Application data

#### *4.2.1 Content security*

Infoteam pays extreme attention to the privacy of its customers. The customer always remains the owner of his contents and also retains the possibility of encrypting them,

moving them and managing their conservation.
Infoteam does not disclose the customer content, except where required by applicable legislation or binding legal orders issued by a public authority.
The data centers of the cloud providers used by Infoteam are located in Italy, thus allowing compliance with privacy and cyber security regulations (e.g. the Cybernetic National Security Perimeter Law).

#### 4.2.2 *Types of data and related regulations*

##### 4.2.2.1 *Resources assigned to the customer*

This category includes information relating to the resources defined in the contract stipulated between Infoteam and the customer and the technical characteristics that make up the service, such as:

- Ip
- Cpu
- Memory
- Disk space
- Etc…

##### 4.2.2.2 *Login data*

Infoteam's technical operators (systems engineers and developers) have access to the cloud environment for administrative or maintenance/assistance reasons and, consequently, to personal and sensitive data internal to the customer's virtual machines or databases, as defined in the contract and in the appointments pursuant to GDPR.
In particular:

- Access credentials must be changed periodically and refer to nominative users
- Credentials must be stored on Passbolt.
- Only authorized users can access the resources with the aforementioned credentials, and only for service reasons and according to their specific skills.

##### 4.2.2.3 *Log data*

Cloud services generate numerous types of logs, which are essential both for operational/performance reasons and security reasons (webserver logs, system logs and so on).
Infoteam technical staff can access the logs of the various cloud instances for the sole purpose of monitoring their correct functioning and consequently of analyzing and

resolving any anomaly.

#### 4.2.3 Application data management

Infoteam technicians may have access to the data generated/processed through the applications developed and contained in the databases only for maintenance and support reasons and as strictly provided for in the contracts.
This access occurs exclusively for release reasons (updates and bugfixes), support and evolutionary maintenance. The data are in no way analysed, used or extrapolated.

#### 4.2.4 Operational continuity

The cloud infrastructure provides a high level of availability with continuous capacity control; systems are designed to tolerate hardware or system failures with a minimal impact to the customer.
In particular:

- The resources and related loads are constantly monitored via the administration panels provided by the cloud providers used and via Zabbix.
- Computational and storage capacity is controlled and increased where necessary.
- The data, in particular the databases, are subject to daily backup and this allows the service to be restored in the event of a fault or other disaster that affects the cloud infrastructure.
- We rely on different cloud providers, so we can restore services in different organizations and geographical areas.

### 4.3 Termination of the employment relationship of Infoteam employees and/or collaborators

Upon termination of the activity, the employee or collaborator is required to maintain confidentiality regarding the information acquired during the employment relationship, according to the commitment signed during the hiring and onboarding phase.

### 4.4 Controls

The following checks are carried out periodically:

- Controls on the visibility of the platform data by each operator
- Control over the correct use of the centralized password manager (Passbolt)
- Controls on virtual machine firewalling policies
- Control of the software installed on systems
- Control of the logs

- Verification of backup results.