CLOUD SECURITY POLICY

1. INTRODUCTION

Cloud computing offers many potential benefits, including scalability, flexibility, high performance, lower administration burdens along with cost efficiency, agility, flexibility, faster time to market, and new opportunities for innovation.

Understanding, managing and controlling those risks that primarily concern the confidentiality, security and resilience associated with adopting cloud services and/or delivery is critical to ensuring proper IT security management.

2. SCOPE AND FIELD OF APPLICATION

This document defines specific company policies, integral to the general SGI policy as defined by METEDA Management, in relation to the Cloud service, for the protection of global data, including personal data, applying the best practices defined by ISO 27017 and ISO 27018 standards.

The purpose of this policy, therefore, is to describe the general principles of security within those cloud services that METEDA has taken on, in order to ensure the security of information, stored and/or managed on public cloud platforms, at a level that is as least equal to the general principles expressed in its policy and, in the presence of personal data, in compliance with current legislation.

3. ORGANISATIONAL SCOPE

This policy applies to all METEDA employees and to all those who collaborate with METEDA.

The policy also applies to all general processes and to all resources involved in the management of information handled by the company.

In the document, the terms “Cloud Service Provider” or “CSP” acquire a dual meaning depending upon the context. When the policy is applied to services for which METEDA is a customer, the above terms refer to the provider of such services. When it is applied to services provided by METEDA, it will refer to the company.

4. TERMS AND DEFINITIONS

Assets or Goods – Any resource that has a value for the organization, whether tangible or intangible (e.g. physical assets, software, information or data, etc.).

Cloud – A set of ICT services that are accessible on-demand and in self-service mode via Internet technologies, based upon shared resources, characterised by rapid scalability and timely measurability of performance levels, such that they can be paid for on a consumption basis.

Private Cloud– A Cloud-based platform managed internally to provide services and not open to the availability of third parties.

Public Cloud – A Cloud-based platform that provides services to multiple subjects that are not connected to each other.

Cloud Hybrid – A technology solution that provides for the combined use of a Public Cloud and a Private Cloud.

CSP – (Cloud Service Provider) An entity (private or public) that provides cloud-based platforms, infrastructures, applications, security services or storage services to another entity/organisation, usually paid for.

Availability – The property for which the information is made accessible and usable at the request of an authorised entity (ISO/IEC 13335-1:2004).

Hardening – A set of actions designed to analyse the functionality of an operating system/application in order to identify the optimal configuration that makes it possible to raise the level of security and reduce the residual risk associated with system weaknesses.

IaaS – (Infrastructure-as-a-Service) Infrastructure provided in service mode. Virtualized hardware resources are provided so that the user can create and manage their own cloud infrastructure according to their needs, without worrying about where the resources are allocated.

Integrity – Property for which the accuracy and completeness of assets is safeguarded (ISO/IEC 13335-1:2004).

Log - The log is a system for recording significant events. The files that contain these annotations are called log files and may also be identified as log files; the log is therefore nothing more than a log.

Data Processor - a natural or legal person, public authority, service or other body that processes personal data on behalf of the data controller; Confidentiality – Property for which information is not made available or disclosed to unauthorised individuals, entities or processes (ISO/IEC 13335-1:2004).

Snapshot – A copy of the state of a virtual machine at a given moment in time.

Data Controller - a natural or legal person, public authority, service or other body that, individually or together with others, determines the purposes and means of the processing of personal data; when the purposes and means of such processing are determined by the law of the Union or Member States, the data controller or the specific criteria applicable to its designation may be established by the law of the Union or Member States;

VM – Virtual machines are software created within a digital environment that provides the same functionality as physical computers.

5. REGULATORY CONTEXT OF REFERENCE

- ISO 27001:2013 – IT Security Management Systems – Requirements.
- ISO 27017:2015 – ISO / IEC 27002-based information security control practice for cloud services.
- ISO 27018:2019 – Code of practice for the protection of personal information (PII) in public clouds acting as PII processors.
- GDPR Reg. EU 679/2016 and national legislation.

6. CLOUD SERVICE MANAGEMENT SECURITY POLICY

METEDA delivers cloud computing services in Software-as-a-Service (SaaS) mode. The SaaS model is a method for software application deployment via the Internet, where cloud service providers host and manage such software applications in order to enable the same application to be used by all of your devices by accessing it in the cloud.

METEDA, in using the IAAS infrastructure to support its processes, takes on the role of Cloud Service Customer.

The METEDA Cloud offers to the end user of the DiaWatch application the following types of value-added services:

- Distribution of the application to be installed on your smartphone.
- Archiving of personal and clinical data.

CLOUD SECURITY POLICY

As part of the provision and/or management of METEDA cloud services, the requirements described below are taken into account:

- Cloud Management: moving data to the cloud may require a significant realignment of roles and responsibilities within the organisation and/or its suppliers. For this reason, it is necessary to define roles, both in terms of the supply of the service as well as the management of relationships with cloud service providers.
  Staff with direct responsibility for public cloud services are trained on cloud technologies and provisions concerning the processing of personal data.
- Virtualisation: In cloud computing, most of the logical separation controls are not physical (i.e. separate servers). Separation is forced through the use of virtual equipment and data segmentation and integrity is guaranteed through logical controls. METEDA operates to ensure, in the virtual environment, a level of security for the separation of systems that is at least similar to that of physical environments.
- Separation of environments: in the Public Cloud, physical infrastructures are shared with other users and with the platform manager. METEDA guarantees the correct separation of the various logical realities.
- Digital Identity Management: Managing digital identities is an essential component to ensuring data security in cloud computing. METEDA guarantees their correct management during the cycle.
- Log management: METEDA has the necessary monitoring log information and guarantees access only to authorised users.
- Web Application Security: the Cloud is typically an open environment. This aspect significantly increases exposure to attacks. For this reason, METEDA submits web applications that interface with public Cloud environments to supplementary controls.
- Disaster Recovery: METEDA performs timely checks on the data stored in the Cloud to ensure their availability even in the event of a disaster.
- Computer investigations: the competent authorities may request access to specific information in the context of investigation activities. As with data stored internally, when the data is stored by a CSP, it is necessary to have procedures that are shared with the supplier.
- Contractual requirements: before transferring the data to third parties, METEDA performs an analysis of the CSP and adopts specific contractual clauses.
- Personal data processing: the roles and responsibilities, in the context of the processing of personal data stored on a public cloud, are clearly defined.

The main activities necessary in order to implement the above requirements are described below.

7. MANAGING THE CLOUD

7.1 ROLES AND RESPONSIBILITIES FOR IT SECURITY

To enable effective management of cloud services, METEDA ensures that:

- Staff with direct responsibility for cloud services are trained in cloud technologies and the provisions concerning the processing of personal data.

- In the case of the acquisition of cloud services on the market, regarding the various roles and responsibilities of the staff responsible for managing the cloud service, Quality Technical Agreements are formalised in order to ensure the level of service provided, NDAs are also signed to guarantee the security and confidentiality of information.
- These roles are also shared with customers when METEDA operates as a CSP. In this case, an escalation process to the group responsible for managing cloud services is defined and shared with customers.

The identity of the Data Processor is as follows:

METEDA SRL

Address Via Antonio Bosio, 2 Int.10 - 00161 Rome (RM)

Administrative and Operational Office: Via Silvio Pellico, 4 - 63074 San Benedetto del Tronto (AP)

contact details: e-mail info@meteda.it Telephone: +39 0735 783021 Fax: +39 0735 83887

Control of the secure management of the Cloud infrastructure is ensured by a team of specialist technicians.

The company also appointed a DPO: Mr. Dino Costanza, Lawyer – privacy@meteda.it

7.2 GEOGRAPHICAL LOCATION OF DATA PROCESSING

METEDA's cloud services are hosted on Microsoft Azure VMs, which have one of the highest security standards available on the market and reside in server farms located in EU.

7.3 ASSET MANAGEMENT AND CLASSIFICATION OF INFORMATION

Access to the client's assets takes place in relation to the contractual provisions and in compliance with the legislative provisions.

To protect the rights of data subjects whose data are the subject of processing, METEDA undertakes to constantly inform its customers regarding the policies, practices and technologies of data security and privacy which are applied.

These commitments include:

- Access and ownership: the customer retains full control of their content. The ownership of the data remains with the customer.
- Disclosure of customer content: METEDA does not disclose the content of the customer unless required to do so by current legislation or binding orders issued by a state authority.
- Safety Checks: METEDA adopts policies, standards and guidelines concerning privacy and data protection such as to achieve the highest level of security and confidentiality.

7.4 USER ACCESS MANAGEMENT

The user's access to Cloud Services takes place through a process of registration and/or voluntary downloading of the app associated with the service.

The processed data refers to the identification data of the users and -depending upon the service - there may be management of the personal medical data of the subject, whether in transit or also with a repository function.

The Cancellation of the registration takes place at the request of the data subject, in compliance with the GDPR according to the methods described in the privacy information sheet.

The interested party, in the case of access to the service by downloading an app, may use the standard uninstallation procedure available to them through the mobile device.

8. VIRTUALISATION ON SYSTEMS ACQUIRED ON THE MARKET

Most logical separation controls are not physical (i.e. separate servers). Separation is forced through the use of virtual equipment and data segmentation and integrity is guaranteed through logical controls. METEDA operates to ensure, in the virtual environment, a level of security of the separation of systems that is at least similar to that of physical environments.

To enable effective virtual system protection:

- During the supplier evaluation phase, the security policies adopted are evaluated, paying particular attention to the adoption of recognised standards and best practices. The policies, by way of example, include the following aspects:
    - disabling (or removing) all interfaces, ports, services, and devices that are not strictly necessary.
    - configuring, using principles of information security, all virtual network interfaces and storage areas.
    - limits on the use of VM resources.
    - the hardening (adoption of security policies) of all operating systems and applications running within the virtual machine.
    - validation of the integrity of the cryptographic key management operations.
- The CSP adopts controls to ensure that only expected and authorised snapshots are taken and that the level of classification, storage location and encryption assigned to them is in line with the sensitivity of the processed data.
- The CSP also ensures that the following controls are applied:
    - access to the hypervisor's administrative access logs.
    - logging of all hypervisor logs.
- METEDA must support the use of VMs provided by the customer and considered reliable by the customer.
- In this document, METEDA identifies the complete list of its suppliers involved in managing the cloud for the provision of the contracted service. If there is also personal data (PII), METEDA shall ensure compliance with the provisions of current legislation regarding the processing of personal data. Any change to the above list that occurs during the period of validity of the contract will be promptly communicated by METEDA.

9. SEPARATION OF ENVIRONMENTS

The separation of the different logical systems that coexist on a Cloud infrastructure is one of the main measures to ensure the confidentiality and integrity of the stored data as well as the security of the entire service delivery infrastructure.

In the case of cloud services acquired on the market, METEDA guarantees the logical separation of the networks used by all its customers and, in addition, separation between the infrastructure management network and those networks intended for the provision of services.

The CSP must provide METEDA, if required, with all of the support necessary in order to verify that this segregation is guaranteed even when additional segregation elements are required in compliance with its own policies.

CLOUD SECURITY POLICY

10. MANAGEMENT OF DIGITAL IDENTITIES.

The management of digital identities must comply with the provisions of the document "*P0L01_Politica di gestione degli accessi"* [*P0L01_Access management policy].*

11. MANAGEMENT OF LOGS

When METEDA uses third-party Public Cloud services, it must comply with the provisions of the reference procedure for systems being managed and agree with the supplier concerning the characteristics of the necessary logs.

In the event that METEDA operates as a CSP, the service must guarantee its customers the possibility of defining monitoring requirements on time, in particular with regard to all operations that require administrative privileges

12. BACKUP

METEDA in data management in the cloud ensures the execution of georedundant backups with DB replication in a different geographic site than the one where it is installed. The Backup storage site is located in EU, and the policy provides for multiple backups at different time intervals.

13. WEB APPLICATION SECURITY

In the case of cloud services acquired on the market, METEDA has a team available to manage security incidents and to adopt guidelines for the development of web applications that guarantee at least the measures of procedure P 04CYB_ Security Development Requirements and P 08.2 E_IT Incident Management and Data Breach.

14. DISASTER RECOVERY

METEDA, for the purposes of disaster recovery management, has enabled a disaster recovery process for applications with geographical replication in EU location.

In the case of cloud services acquired on the market, the CSP must adopt processes for managing changes and responding to incidents in accordance with the provisions of procedure P 08.2 E_IT Incident Management and Data Breach defined by METEDA and consistent with the SLAs of the services provided.

Furthermore, the qualified provider for cloud services must define a Disaster Recovery plan that guarantees data recovery within the timeframes and with the contracted service level. This plan must be tested at least once a year and the qualified provider for cloud services, upon request by METEDA, must deliver a copy of the test report.

15. IT INVESTIGATIONS

Cloud service customers will be guaranteed maximum support, in compliance with current legislation, if they initiate investigations into the services acquired.

In the case of cloud services acquired on the market, in order to enable effective investigation activities, the method for requesting data necessary for internal investigations or following a request by the competent legal authorities must be agreed with the CSP.

CLOUD SECURITY POLICY

16. CONTRACTUAL REQUIREMENTS

Adoption of market cloud services may result in greater risks concerning data integrity, confidentiality, and availability. For this reason, contracts that have the purpose of providing services on a Public Cloud must at least include:

- An “NDA – Non-Disclosure Agreement” declaration.
- the express declaration that the customer will retain the "exclusive" right to ownership of the data for the entire duration of the agreement. The ownership includes all copies of the data available with the CSP, including any backup media copies.
- the express prohibition of the CSP to use data from state agencies for marketing and/or advertising or any other unauthorised secondary purpose.
- the indication of the country(s) in which it is acceptable for the data to be stored.
- that the applicable legislation concerning the protection of personal data complies with European legislation.
- the Service Level Agreement (SLA) of the service.
- the obligation on the part of the CSP to inform, without undue delay, of any confirmed or suspected data breach.
- the obligation for the CSP to completely eliminate any trace of data/information, at the end of the Agreement, from all of its systems.
- how the CSP will return the data at the end of the agreement.

The above requirements must also be met in the contracting of services when METEDA operates as a CSP to its customers.

17. PRIVACY AND THE PROCESSING OF PERSONAL DATA

In order to protect the rights of data subjects whose data are being processed, the Cloud service customer, as Data Controller or Data Processor, appoints the CSP, as Data Processor or Sub-Data Processor, by means of a formal deed.

METEDA is committed to constantly monitoring the ever-changing landscape of regulations and laws regarding privacy in order to identify changes and determine the tools that clients, depending upon their applications, may require for compliance needs.

METEDA undertakes to constantly inform its customers regarding applied policies, practices and technologies of data security and privacy.

These commitments include:

- Access and ownership: the customer retains full control of their content. The ownership of the data remains with the customer.
- Disclosure of customer content: METEDA shall not disclose the content of the customer unless required by current legislation or binding orders issued by a state authority.

Safety Checks: METEDA adopts policies, standards and guidelines concerning privacy and data protection such as to achieve the highest level of security and confidentiality.