Information Security Policy: OpenNebula Systems

1. Introduction and Motivation

Information is the fundamental asset for the activity of OpenNebula Systems and must be properly protected against possible threats. In an increasingly interconnected environment, ONS recognizes that traditional security models based solely on perimeter trust are no longer sufficient.

OpenNebula Systems assumes the responsibility of safeguarding information throughout its entire life cycle—from creation and processing to storage and eventual destruction. This policy aims to minimize the risk of unauthorized manipulation, loss, or destruction, ensuring the **Confidentiality, Integrity, and Availability** of all data related to the e-infrastructures we manage.

2. Declaration of Principles and Objectives

OpenNebula Systems is committed to becoming a benchmark for best practices in information security. Our security framework is guided by the following principles:

- **Asset Protection:** Information and communication systems are critical assets that must be protected against threats such as fraud, sabotage, service interruptions, and natural disasters.
- **Risk-Based Approach:** Security measures are applied in accordance with the value and criticality of the information, determined through formal risk assessments.
- **Standards Compliance:** This policy is developed in alignment with the **ISO 27001:2022** standard and the **National Security Framework (ENS)** requirements.
- **Shared Responsibility:** All ONS personnel, as well as authorized external users and suppliers, have a responsibility to protect the assets entrusted to them.

- **Life Cycle Management:** Security is integrated into the information life cycle, including its communication, transport, and dissemination to third parties.

3. Scope and Compliance

This policy applies to all assets managed by OpenNebula Systems, including:

- Information storage systems.
- Data processing environments.
- Communication methods and networks.

OpenNebula Systems reserves the right to take corrective actions in case of breaches to ensure the global security of our services.

4. Security Organization and Internal Regulations

To ensure these principles are upheld, ONS maintains a robust internal governance structure:

- **Security Committee:** A dedicated committee is responsible for the control, monitoring, and continuous improvement of the security policy.
- **Roles and Responsibilities:** Specific security roles are defined internally to ensure accountability across all organizational units.
- **Internal Regulations:** Detailed operational procedures are maintained internally covering areas such as physical security, access control, incident management, disaster recovery, and remote work.
- **Documentation Management:** ONS maintains a comprehensive set of internal handbooks and "Changelogs" to ensure that all security processes remain up-to-date and are reviewed on a regular (quarterly or annual) basis.

5. Information Classification

All information within the organization is classified according to its level of sensitivity and confidentiality. This ensures that sensitive data is subject to stricter access controls and handling procedures, while company-wide information is managed with appropriate transparency.

6. Legal and Regulatory Framework

OpenNebula Systems operates within a strictly defined legal framework. We undertake to comply with all applicable regional and international legislation regarding data protection, privacy, and information security to ensure full legal compliance in all our activities.

Last Updated: May 2025 **Compliance:** ISO 27001:2022 | ENS