VIRTUALWARE

Information Security Management Systems (ISMS) Policy

2022

Content.

Introduction.

This Information Security Policy sets out the principles and guidelines by which Virtualware will protect its information, in accordance with the applicable regulations and its ethical values, as defined in the Code of Conduct and Responsible Practices (hereinafter, the "Code of Conduct") and other applicable internal regulations.

Virtualware will ensure the protection of information, regardless of the form in which it is communicated, shared, projected or stored. This protection concerns both information within the company and information shared with third parties as well as information on the platforms, services and projects offered by Virtualware.

In this sense, Information Security is understood as the safeguarding and protection of:

- **information owned by the Group, regardless of whether it is held on its own or third-party systems; and**
- **information owned by third parties and held in the Group's systems.**

For the purposes of this Policy, Information Systems are understood to be the set of technologies or technological means, whether owned or owned by third parties, that manage, store or transmit Information (including cloud or similar technologies).

Scope.

This Policy shall apply to the Company and its Group, and shall be binding on all of its personnel, regardless of their position and function. For these purposes, the Virtualware Group is defined as companies in which Virtualware owns, directly or indirectly, at least 50% of the share capital or voting rights.

The application of the Policy may be extended, in whole or in part, to any other natural and/or legal person linked to the Group by a relationship other than an employment relationship when this is possible due to the nature of the relationship and when it is appropriate for the fulfilment of the purpose of the Policy.

In accordance with the Policy, Virtualware may develop procedures and instructions to implement and comply with the obligations undertaken, as well as to adapt the Policy to the various local laws applicable to the Group.

Likewise, the application of this Policy is complementary to other mandatory internal rules, such as the Personal Data Protection and Privacy Compliance Policy, and those others that regulate issues related to the Company's information.

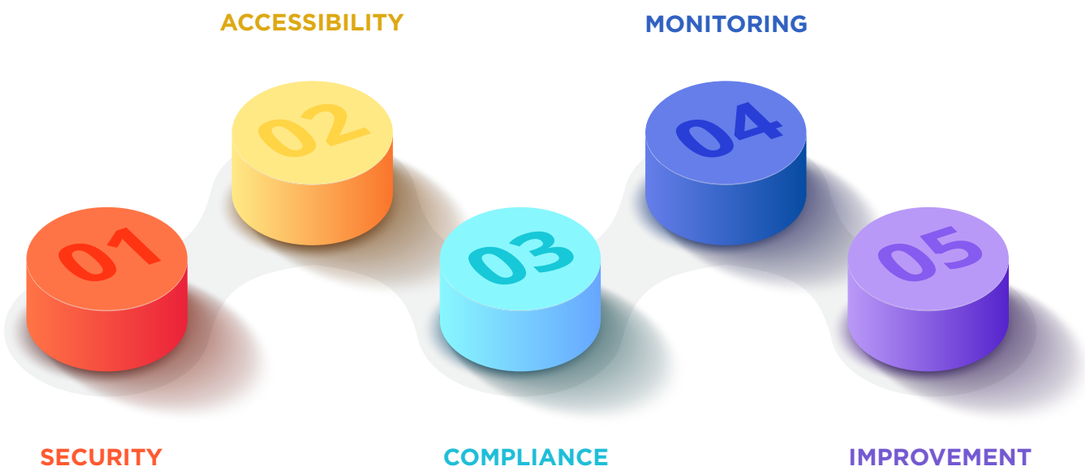
The Information Security Management System covers the following services:

- **Services to ensure the availability of the Logical Infrastructure for critical VRaaS (Virtual Reality as a Service) functionality.**
- **Development of digital content projects and applications (Apps) delivered in DEVaaS (Development as a Service) mode.**
- **Integration of technological solutions based on interactive digital content platforms.**

ISMS Pillars.

The ISMS is based on the following pillars

- Integrate the concepts of security by default and security by design in the approach to new development projects, as well as in all the services developed by Virtulaware.
- Ensuring accessibility of software in the operating environment
- Ensure compliance on all corporate processes and stakeholders in the operation and use of the VIROO platform.
- Active monitoring and operational control over security aspects and especially cyber security.
- Improved process governance, risks and controls transferred to third parties and especially to suppliers in the critical chain.



General principles.

The pillars described in section 3 are based on the following general principles:

Classification of Information.

Information shall be classified according to its value, importance and criticality for the business, so that the protection measures are adapted to the classification level of each information asset. Likewise, the classification of Information assets shall be carried out taking into consideration legal and operational requirements and the best practices and standards in this respect.

Use of the Information Systems.

The use of the Systems shall be limited to lawful and exclusively professional purposes, for the performance of job-related tasks. Consequently, these means and systems are not intended for personal use and may not be used for any unlawful purpose.

Segregation of duties.

Concentrations of risk arising from a lack of segregation of duties and single-person reliance on business-critical functions should be avoided. In this regard, formal procedures should be established to control the assignment of privileges to Information Systems, so that users have access only to the resources and information necessary for the performance of their functions.

Retention of Information.

Where necessary or appropriate, retention periods for Information by category shall be established in accordance with operational or regulatory compliance needs, as well as the corresponding procedures for the destruction of Information.

Access to Information by third parties.

Se desarrollarán los procedimientos de control de la puesta a disposición y acceso por terceros a la Información relativa a Virtualware o de cualesquiera otros terceros relacionados con el Grupo.

Information Security in Systems.

The development and production environments shall be maintained in separate systems. Likewise, the development and maintenance of the Information Systems must include the necessary controls and records to guarantee the correct implementation of the security specifications.

Continuity.

A continuity management procedure shall be established to ensure the recovery of critical information for the Group in the event of a disaster, reducing downtime to acceptable levels.

Compliance.

The Group's information and communications systems must be permanently adapted to the requirements of the legislation in force in all the jurisdictions in which it operates, as well as to the applicable internal development regulations.

Responsibilities.
(roles and authorities)

Responsibility for the protection of Information and the Systems that process, store or transmit it extends to all organisational and functional levels of Virtualware, each to the extent applicable to it, as detailed below:

1 Responsibilities of employees.

- All employees of the Group must know, accept and comply with the Policy, as well as the internal regulations on security and use of the Systems in force, being obliged to maintain the professional secrecy and confidentiality of the Information handled in their work environment and must communicate, as a matter of urgency and in accordance with the established procedures, any possible security incidents or problems that may be detected.

- Employees contracting services from third party companies or persons involving the use of or access to Information by third parties should understand the risks arising from the outsourcing process and ensure effective management of those risks.

- The use of digital systems or services by employees, including specifically e-mail and instant messaging services, shall be limited to lawful and exclusively professional purposes, for the performance of work-related tasks. Consequently, these means and systems are not intended for personal use and may not be used for any unlawful purpose.

2 Responsibilities in relation to suppliers and third parties.

- Contracts with third parties involving the use of or access to Information by the latter, including service provision or outsourcing contracts, shall include specific security requirements relating to the technology and activities of the third parties performing such services.

- In this respect, they must include provisions guaranteeing that supplier companies, subcontracted personnel or any external company that potentially or actually uses or accesses the Information (through the Systems or by any other means, as set out in section 1) must know and comply with the Policy insofar as it applies to them, and are obliged to maintain the professional secrecy and confidentiality of the Information handled in their relationship with the Group.

3 Information Security Officer.

The person responsible for Information Security shall exercise his/her control function independently and it is his/her responsibility to implement this Policy and monitor compliance with it, as well as with all requirements derived from applicable laws, regulations and good practices in the field of information security.

It is therefore responsible for:

1. **Implement an information security strategy** that ensures compliance with the basic principles of this Policy, and in particular that covers the following aspects:

    - Adequate access to Information, based on the principle of least privilege and the approval of the owner of the Information asset;
    - A proper segregation of roles and functions in Information Systems;
    - Proper configuration, administration and operation of the infrastructure, services and/or software used in the various business processes both inside and outside the Group's premises, from a security point of view;
    - A correct implementation of security requirements during the life cycle of the Information Systems that support the Company's processes.
    - Adequate protection of the systems and the information they support against physical or environmental threats, in accordance with their criticality, to identify, assess, prevent and respond to any risk that could compromise their security.

2. **Establish and review the corresponding controls to ensure compliance with this Policy and its implementing regulations**, including the organisational and technological mechanisms necessary to facilitate the continuous monitoring of the activities of access to and use of the Systems, services or Information managed by the Group.

3. **Prevent, detect and respond to any Information Security incident** and act in accordance with the "Information Security Procedure: Virtualware Group Incident Response Plan".

4. **Promote the regulatory development of this Policy**, by means of the procedures or instructions that may be necessary to define a global framework of action for information security in all its areas. Likewise, it must review, update and communicate any changes that result in variations to this Policy.

5. **Conduct training and awareness-raising activities** on Information Security processes.

6. **Establish a continuous improvement approach.**

7. **Ensure compliance with the legislation** in force within the scope of the competences attributed to it by this Policy.

4 Information Security Committee.

Virtualware has an Information Security Committee headed by a person responsible for the Information Security Management System and whose members are appointed by the Management team on an annual basis and whose objective, in compliance with the Regulations, is to:

- **Ensuring that security management best practices are applied effectively and consistently across the Group**. Among other functions, he/she is responsible for overseeing the information security strategy, including security spending, investment and resource plans, and coordinating the security needs of management, the business and geographies.

- **Report, at least annually, on the state of security**, the evolution of threats and vulnerabilities, the allocation of resources allocated to security and on significant incidents that have occurred. This committee will report to the Virtualware Management.

- **The members of the Committee are the joint owners of the Risks** and will jointly approve the risk action plan and the level of acceptable residual risk and put in place the necessary measures to keep the risks under control.

Implementation.

Virtualware is committed to allocating specific resources to ensure effective implementation of the Policy.

Control and audit.

Virtualware expressly reserves the right to adopt, with proportionality, the surveillance and control measures necessary to verify the correct use of the Systems that it makes available to its employees, including the content of communications and devices, respecting, in all cases, current legislation and guaranteeing their dignity.

The communication and acceptance of this Policy shall have the effect of prior notification to the employee.

The Group will undergo periodic reviews and controls, as well as internal and external audits to assess overall compliance with this Policy. The assessment of a possible breach of this Policy will be determined in the corresponding procedure, in accordance with the provisions in force, without prejudice to the legal responsibilities, including sanctions in the labour sphere, which, if applicable, may be demanded of the person who breaches it.

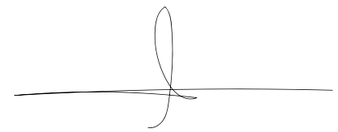
Policy Communication.

This Policy will be available to all employees and will be available to all stakeholders of the Company on the corporate website.

The Policy will also be the subject of appropriate communication, training and awareness-raising activities to ensure that it is properly understood and put into practice.

Policy update and review.

The Policy will be reviewed and updated as appropriate, in order to adapt it to changes that may arise in the business model or in the context in which the Group operates, ensuring its effective implementation at all times.



Unai Extremo Baigorri. (CEO)

Accelerating
VR adoption in the
enterprise.

#VRFORINDUSTRY

VIRTUALWARE®