INFORMATION SECURITY POLICY and NATIONAL

SECURITY SCHEME

TrustCloud's management, aware of the need to promote, maintain and improve customer focus in all of its activities, has implemented a Information Security Management System according to several internationally recognized standards, whose ultimate **goal is** to ensure that we understand and share the needs and goals of our customers, trying to provide services that meet their expectations working on continuous improvement. It expressly states its commitment to enhance the **security and cybersecurity** of the information of the service provided, and is committed to meet the needs and expectations of stakeholders, to keep our competitiveness high in the services of ***design, development and maintenance of applications, computer systems, professional cloud services and Integrated Trusted Services Provider.***

MISSION and OBJECTIVES*:*

- Promote continuous improvement of services and customer support.
- Continue to position **TrustCloud** as a benchmark in the sector.
- To provide customers with IT services with global solutions through the improvement of their information systems.
- To provide customers with the most professional human resources and to have at their disposal immediately and for as long as necessary highly qualified technicians, experts in the required disciplines, accustomed to working in teams
- *To* have a service delivery based on our commitment to the continuous improvement of our systems, with **security, cybersecurity and information continuity** as a central pillar.

Our **mission** and objectives will be achieved through:

- A system of objectives, metrics and indicators for continuous improvement, follow-up, measurement of our internal processes, as well as customer satisfaction. Establishing and supervising compliance with contractual requirements to ensure an efficient and safe service.
- Continuously training and raising awareness of our team to have the highest degree of professionalism and specialization possible, in addition to having our infrastructure in an adequate state and in accordance with the requirements of our customers.
- With a secure product procurement management procedure.
- Complying with the requirements of current legislation, especially with the **GDPR / LOPD** and compliance with our Security Documentation.
- Introducing continuous improvement processes that allow a permanent advance in our Information Security management.
- Managing and developing plans for risk management and treatment with a risk analysis and management methodology based on recognized and prestigious international standards.
- Managing internal and external communications and information stored and in transit.
- Ensuring interconnection with other information systems
- Managing and monitoring activity with log management
- With special focus on security incident management
- Ensure that our Assets and Services comply with ENS HIGH Level measures for the dimensions of Confidentiality, Integrity, Availability, Authenticity and Traceability.
- Ensuring business and service continuity and availability.

Likewise, these principles should be contemplated in the following safety areas:

- **Physical**: Comprising the security of premises, facilities, hardware systems, supports and any physical asset that processes or may process information.
- **Logic**: Including the protection aspects of applications, networks, electronic communication and computer systems.
- **Political-corporate:** Made up of security aspects related to the organization itself, internal rules, regulations and legal norms.

The ultimate purpose of information security is to ensure that an organization will be able to meet its **objectives** using information systems. The following basic principles should be taken into account in security decisions:

a) Integral security.
b) Risk management.
c) Prevention, reaction and recovery.
d) Lines of defense.
e) Periodic reevaluation.
f) Differentiated function.
g) Continuity

Security roles or functions
Responsible for the
information:
Determine the requirements of the information processed

- To implement and maintain the Information Security Management System, continuously improving its effectiveness.
- Implement and maintain the ENS by continuously improving its effectiveness.
- Supervise procedures and technical instructions.

- Follow up and verify the implementation and effectiveness of all established corrective and preventive actions.
- Ensure that the implemented system complies with the established standard.
- Analyze the data obtained in the Information Security Management System and ENS and propose improvements.
- Participate in management review decision making.
- Management of safety non-conformities.
- Participate in external audits.
- Responsible for the company's private data in terms of loss, theft and outdatedness.
- Comply with the manual of good information security practices.
- Communicate any fire, flood or HVAC equipment emergency that may activate the BCP.
- Prepares, reviews and approves the Business Continuity Plan.
- Maintains, updates and verifies the functioning of the Business Continuity Plan.
- Provides training programs to ensure that personnel know how to act in the event of contingencies
- Maintains updated means of contact with the authorities.
- Keeps the inventory of media containing personal data
- Supervises the recording of incidents in the data to which the high security or confidential level is applied.
- Analyzes the audit reports and submits the conclusions to the data manager.
- Monitors the security incidents that have occurred
- Convenes CSI meetings
- Generates risk management treatment plans and oversees their implementation
- Manages IS nonconformities, corrective actions and preventive actions.
- Updates risk analysis
- Oversees the collection of metrics
- Maintains IS and ENS documents
- Maintains and deploys the TrustCloud security policy as well as the rest of the policies to the personnel involved in each of them.
- Responsible for the management of the data protection and GDPR security audit.
- Performs IS security reviews
- Incorporates corrective actions in the incident log
- Supervises the LOPD tasks of the DPO.
- Create TrustCloud security documents
- Prepares agreements for the processing of data by third parties and monitors compliance with their services.
- Attends to incidents related to data protection.
- It is responsible for contacting the authorities if necessary.
- Enforcement and monitoring of compliance with IS policies.
- Maintenance and application of the IS Applicability Document and the ENS.

Responsible for systems:

- Responsible for data processing and logical access control.
- Responsible for logical monitoring of server capacity and communications.
- Systems Operator (trusted role)
- System Administrator (trusted role)
- Responsible for backups

Responsible for the service:
Determine the requirements of the services rendered

- Develop, operate and maintain the system during its entire life cycle, its specifications, installation and verification of its correct functioning.
- Define the topology and management policy of the System, establishing the criteria for its use and the services available in it.
- Define the policy for connection or disconnection of new equipment and users in the system.
- Approve changes that affect the security of the System's mode of operation.
- Decide on the security measures to be applied by the suppliers of System components during the development, installation and testing stages of the System.
- Implement and control the specific security measures of the system and ensure that they are properly integrated within the general security framework.
- Approve any substantial modification to the configuration of any element of the System.
- Carry out the mandatory risk analysis and management process in the System.
- Determine the category of the system according to the procedure described in Annex I of the ENS and determine the security measures to be applied as described in Annex II of the ENS.
- Elaborate and approve the security documentation of the System.
- Delimit the responsibilities of each entity involved in the maintenance, operation, implementation and supervision of the System.
- Ensuring compliance with the obligations of the IHR

LEGAL FRAMEWORK: Royal Decree 311/2022, of May 3, which regulates the National Security Scheme in the field of Electronic Administration.

- Investigate security incidents affecting the system and, if necessary, communicate them to the Security Manager or whoever he/she may determine.
- Establish continuity, contingency and emergency plans, conducting frequent drills to familiarize personnel with them.
- In addition, the system manager may *agree to* suspend the handling of certain information or the provision of a certain service if he/she is informed of serious security deficiencies that could affect the satisfaction of the established requirements. This decision must be agreed with those responsible for the affected information, the affected service and the security manager, before being executed**.**

Responsible for security:
Determine decisions to meet information security and service requirements

- To implement and maintain the Information Security Management System, continuously improving its effectiveness.
- Implement and maintain the ENS by continuously improving its effectiveness.
- Responsible for cybersecurity.
- Supervise the Safety Manual, procedures and technical instructions.
- Implement the measures indicated by the DPO.
- Overall responsibility for managing the implementation of security practices.
- Ensure that the implemented system complies with the established standard.
- Analyze the data obtained in the Information Security Management System and ENS and propose improvements.
- Participate in management review decision making.
- Participate in external audits.
- Responsible for the risk of physical intrusion of the company's devices.
- Comply with the manual of good information security practices.
- Segregation of tasks and environments.
- Communicate any fire, flood or HVAC equipment emergency that may activate the BCP.
- Review the Business Continuity Plan
- Verifies the functioning of the Business Continuity Plan.
- Controls the access of people to the premises where the systems are installed.
- Monitors the security incidents that have occurred
- Performs and safeguards backups
- Generates risk management treatment plans and oversees their implementation
- Updates risk analysis
- Oversees the collection of metrics.
- Performs IS security reviews
- Maintains the Business Continuity Plan
- Incorporates corrective actions in the incident log
- Enforcement and monitoring of compliance with IS policies.
- Maintenance and application of the IS and ENS Applicability Document.

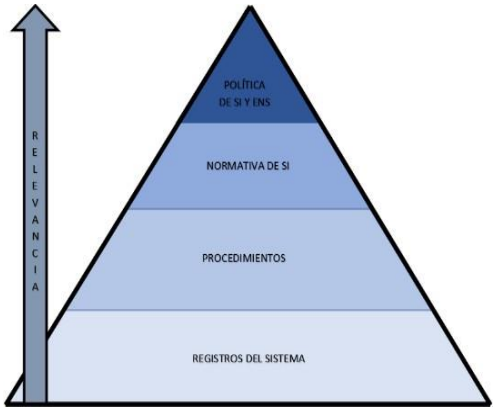
The **TrustCloud** Information Security Committee (ISC) reaches the entire company, is the mechanism for coordination and conflict resolution, among other functions:

- Designation and/or renewal of security positions, as well as their functions and responsibilities.
- Create, plan, implement and integrate the strategic direction of the organization and align it with the ISMS.
- Knowledge of the ICT market and new technologies and their application in the company.
- Management and supervision of the different security projects of the company.
- Participate in and promote compliance with the organization's information security policy.
- To ensure compliance with legal provisions and regulations of public administrations and internal rules related to information security.
- Approval of the ISMS, as well as its changes and new versions.

They make up the CSI:

- Address
- Responsible for the system
- Responsible for security

The system documentation follows the following structure:



The classification of system information is classified into the following categories, as established in the Asset Management procedure:

- Public Use
- Internal Use
- Confidential

Applicable legislation on the processing of personal data
With regard to the processing of personal data, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC and the corresponding national legislation shall mainly be taken into account.
The applicable legal and regulatory framework is described in the document TrustCloud Legal Requirements Identification and Assessment Register The risks arising from the processing of personal data are analyzed in the document LOPD Privacy Risk Management.

Considering these guidelines, this management reiterates its firm commitment to join efforts to achieve these objectives, so that this policy is understood, implemented and kept up to date at all levels of the organization.

Saioa Echebarria
Executive Director

E-SIGNED by Saioa Echebarria
on 2023-06-02 13:11:23 CEST