Information Security Policy

Purpose

The purpose of this document is to demonstrate the management board's commitment to information security and to provide the over-arching policy statements to which all subordinate polices and control must adhere.

Policy

The Board of Directors and management of Confirmo s.r.l. located at Viale Volga c/o Fiera del Levante pad.129 Bari operates primarily in the business of Digital Signatures.
We are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information and information-related assets to meet the purpose and goals of the organization as summarized in 4.1 (Understanding the organization and its context).
Information and information security requirements will continue to be aligned with the organization's business goals and will take into account the internal and external issues affecting the organization and the requirements of interested parties.
Our ISMS Objectives are outlined and measured in accordance with the requirements of the ISO/IEC standard 27001:2022.
The ISMS is intended as a mechanism for managing information security related risks and improving the organization to help deliver its overall purpose and goals.
The online platform environment including our approach to risk management provides the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS.
The approach taken towards Risk Assessment and management, the Statement of Applicability and the wider requirements set out for meeting ISO 27001:2022 identify how information security and related risks are addressed.
The ISMS Board is responsible for the overall management and maintenance of the risk treatment plan with specific risk management activity tasked to the appropriate owner within the organization. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks, for example during special projects that are completed within the context.
Control objectives for each of these areas are supported by specific documented policies and procedures in the online environment and they align with the comprehensive controls listed in Annex A of the ISO 27001:2022standard.
All employees and relevant Interested Parties associated to the ISMS have to comply with this policy. Appropriate training and materials to support it are available for those in scope of the ISMS and communication forums such as the ISMS communications group as per clause 7 (Leadership) are available to ensure engagement on an ongoing basis.
The ISMS is subject to review and improvement by the ISMS Board which is chaired by the Senior Information Risk Owner (SIRO) and has ongoing senior representation from appropriate parts of the organization. Other executives/specialists needed to support the ISMS framework and to periodically review the security policy and broader ISMS are invited in the Board meetings and complete relevant work as required, all of which is documented in accordance with the standard.
We are committed to achieving and maintaining certification of the ISMS to ISO27001:2022 along with other relevant accreditations against which our organization has sought certification.
This policy will be reviewed regularly to respond to any changes in the business, its risk assessment or risk treatment plan, and at least annually.

Definitions

In this policy and the related set of policies contained within the online environment that incorporate our ISMS, 'information security' is defined as:
preserving
This means that all relevant Interested Parties have, and will be made aware of, their responsibilities that are defined in their job descriptions or contracts to act in accordance with the requirements of the ISMS. The consequences of not doing so are described in the Code of Conduct. All relevant Interested Parties will receive information security awareness training and more specialized resources will receive appropriately specialized information security training.

the availability

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The environment must be resilient and the organization must be able to detect and respond rapidly to incidents or events that threaten the continued availability of assets, systems and information.

confidentiality

This involves ensuring that information is only accessible to those authorized to access it and preventing both deliberate and accidental unauthorized access to the organizations and relevant Interested Parties information, proprietary knowledge, assets and others systems in scope.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data.

of information and other relevant assets

The information can include digital information, printed or written on paper, transmitted by any means, or spoken in conversation, as well as information stored electronically. Assets include all information-based processing devices owned by the organization or those of relevant Interested Parties and BYOD in scope that are processing organization related information.

of our organization

The organization and relevant Interested Parties that are within the scope of the ISMS have signed up to our security policy and accepted our ISMS.

Document Owner and Approval

The CEO is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements set out in ISO 27001:2022.
A current version of this document is available to all members of staff in the ISMS controls environment and accessible via the various Business, HR and Technical Policy Groups.
This information security policy was approved by the Performance Audit & Improvement Board and is issued on a version-controlled basis under the approval of the PAIB.

Change History Record and approval process is done on line in the platform.