Ascom Policy Statement on Information Security

Document ID: AODS-7-6322 | Version: 4.0 | Life cycle: Approved | Security class: Open
Approver: Per Eriksson; | Approved: 05 Feb 2021 08:43 | Process: IT | Page: 1 of 2
Modified by: Ivana Catic | Content Type: Standard Operating Procedure | Reviewers: Simone Merlino; Ivana Catic;

Ascom is aware of the fact that the attributes of Information Security Management - confidentiality, integrity and availability - are integral parts of managerial functions. Top management considers these attributes as core and fundamental responsibilities for good organizational practices in design, development, marketing, sales, installation and servicing of information, communication and workflow solutions including software, hardware and security systems.

To achieve this, we decided to implement, maintain and continuously improve an Information Security Management System according to ISO 27001: 2017.

We are committed to:

- **Ensure the confidentiality, integrity and availability of information**. We identified the most relevant risks addressed to information through risk assessment, implemented security controls and maintains security policies and procedures as well as business continuity plans.
- **Respect the rights of the personal data subjects**. We implemented the GDPR requirements. Our goal is to integrate the specific procedures and tools related to Data Protection and Information Management System.
- **Comply with all applicable legal, regulatory and contractual requirements**. We maintain a Law List, which includes the legal requirements relevant for Information Security and which is permanently updated and available for the employees.
- **Implement continuous improvement opportunities, including risk assessment**. Ascom conducts annual risk assessment and risk mitigation for information security, based on a documented methodology, as well as internal audit and management review. Non-conformities are also subject of a documented process.
- **Set, monitor and review security objectives**. The security objectives take into account the results of risk assessment and their primary role is to maintain the security risks under the acceptable level approved by the risk owners.
- **Ensure the necessary resources for security controls implementation**. We established a security team and provided the necessary resources for the ISMS and security controls implementation (knowledge, documentation, security equipment and applications, ticketing application, access control systems etc.).

- **Ensure staff awareness of information security**. Our staff benefits of awareness programs and training supports available in our internal system.

Responsibility for sustaining and enforcing this policy belongs to the entire organization, under the guidance and support of top management, which encourages the commitment of all personnel to approach Information Security as part of professional competence. We designated a Chief Security Officer, supported by a Deputy and Regional Security Officers whose role is to coordinate the information security activities and to maintain the effectiveness of the Information Security Management System.

This policy statement is available to all employees and any interested parties on our public web site, as well as on request.