ADITRO GLOBAL SECURITY POLICY

TABLE OF CONTENTS

1 Introduction

Security and data privacy are essential elements for Aditro's business to ensure customer's trust, as the processes involve financial, personal and health data with major impact to customer's business and operations.

The purpose of this document is to describe the top-level policy for security in Aditro Group and highlight key practises for security management in group level. The document links to other policies and documentation, some of which are restricted to internal use only.

2 Scope

The document covers all Aditro Group companies, business processes and organizational units.

3 Essential changes

Version	Change
3.0	First version with change history table included
3.1	Minor update: Updated security principles and details added to 8.1, 8.2, 11 and 16. Update to new layout.
3.2	Added commitment to continual improvement of the Information Security Management System to chapter 6.
3.3	Updated organizational roles and document names.
3.4	Clarified data privacy role in security management, as related to ISO 27701:2019. Updated text with current document structure.

4 Approval

Approved by	Aditro CEO, Martin Sjögren
Approval date	20.4.2020
Effective date	20.4.2020

5 Glossary and acronyms

Term	Explanation
GMT	General Management Team
ISQ	Information Security and Quality team
SOC	Security Operations Center

Copyright © Aditro. All rights reserved.

GMT	General Management Team

6 Security objectives

Aditro has a fundamental obligation to commit itself to be a reliable and reputable partner in the market and continuously earn customer's trust. This obligation also means that personal data protection, as related to information security controls, is included in all information security governance, principles, operational management and controls as interpreted in ISO 27701:2019 5.1.

Aditro's security governance objectives are:

- ***Provide secure services and products to customers***
- ***Operate in secure and compliant manner in each location by each employee***
- ***Commit to continual improvement of the information security management system***
- ***Continuously improve and develop the processes to overcome future security challenges***

7 Aditro security principles

Aditro's security management is driven by the following principles:

- Protection of customer data confidentiality, integrity and availability
- Risk prediction, prevention and mitigation to ensure business continuity
- Thorough knowledge, service attitude and security mindset of the staff
- Delivery of secure and reliable SaaS services with layered security controls
- Quick and accurate incident response with transparent communication to external parties

8 Security responsibilities

Aditro has defined the following global security responsibilities.

8.1 Security governance

Aditro's security is governed by the General Management Team (GMT) by information security strategy aligned to the business strategy, investment planning and security objectives and documented in Aditro Information Security Strategy. In addition, Aditro Compliance Committee aligns various standards and frameworks to ensure consistency and compliance.

8.2 Security management

Aditro's security is managed by Director of Security and Quality, together with the Information Security and Quality team (ISQ), distributed globally.

Director of Information Security and Quality reports to Chief Information Officer (CIO), who is a member of the General Management Team.

Copyright © Aditro. All rights reserved.

8.3 Process security

Each business area is responsible to maintain and follow the agreed security policies and practises to ensure Aditro's security posture always fulfils the business objectives. Each employee is responsible to follow the issued security instructions.

9 Security management

Security management contains the elements needed to ensure security posture is effective, such as:

- Documentation via frameworks, standards, policies, guidelines and procedures
- Steering via objectives, goals and completion criteria
- Training for security awareness, mandatory annual security training and focused topics
- Measurement and monitoring via audits, checks and use of tools
- Evidence generation via logs, audit reports and checks

Security management default framework is ISO 27001:2013 with extension to privacy protection via ISO 27701:2019, responsibility set for Director of Security and Quality.

10 Risk Management

Security risk management is centralized and managed by Director of Security and Quality, who periodically collects the input from stakeholders, process members and employees via various channels. The risk management framework is ISO 31000:2018.

Security risks are assessed using defined criteria, including, but not limited to:

- Business Impact
- Impact on customer
- Data privacy and security

Risk mitigation actions are traced, and residual risk is accepted by the risk owner.

Details of the process are described in: Aditro Risk Management policy.

11 Business Contingency Planning

Business contingency is managed via centralized process with separated layers for Business Impact Assessment and Recovery Plans with practices. The default framework is ISO 22301:2012.

Aditro reports annually for the business contingency preparation to customers via Annual Reporting.

Details for the process are described in: Aditro Business Continuity Policy.

12 Information Security and Data Protection

Information security is at the core of Aditro processes and business. As a vital element, the information security aspects are embedded in all areas of security management, including but not limited to:

- Data classification schemas to support efficient and secure data management and personal data protection practises
- Customer data identification, labelling and protection to ensure meeting the security objectives
- Personal information identification, labelling and protection for GDPR compliance
- Acceptable use policies for employees, NDA’s, social media guidelines and daily information security guidelines to ensure personnel compliance
- Intellectual property compliance with process for free and open source software use authorization for compliance
- Defined data deletion process with industry best practises
- Logical security and documented access management

Information security documentation is embedded as part of the process policies and operating procedures.

Data protection policy is defined in detail in: Aditro Data Protection Policy.

13 Operational security

Operational security is an ongoing process to ensure Aditro can react to threats and mitigate vulnerabilities in its operations. Operational security contains essential areas, such as:

- Asset management to ensure critical assets such as customer data are identified, categorized and labelled for protection.
- Threat identification and risk management from the threat landscape and vulnerability analysis
- Security controls, risk mitigations and countermeasures to protect the assets, personnel and operations.
- Security monitoring, threat identification and incident management with an external Security Operations Center (SOC)
- Training, knowledge distribution and awareness management to ensure the personnel can maintain the defined security posture.

Operational security management is the responsibility of Information Security and process owners.

14 Secure Application Development

As Aditro offers its solutions for both on-premise and cloud use, secure software development process is essential to protect both on-premise and cloud customers. Secure application development is the core requirement for each development team.

Software development security requirements contain:

- Training for secure software development
- Peer-review of features developed for best security practises
- Security testing during the release process
- Vulnerability management and patching
- External penetration testing for solution security

Application development security requirements are documented in: Aditro Development Security Policy and privacy considerations in Privacy by Design.

15 Physical Security

Physical security ensures that the locations and facilities Aditro operates contain the security controls, such as access control, monitoring and logging and process segregation, identified to be necessary to ensure Aditro's defined security posture.

Physical security is the responsibility of the facilities owner or office manager, working together with Information Security and Quality (ISQ) personnel.

Physical security practises are described in: Aditro Physical Security Policy.

16 Personnel Security and Training

Personnel security contains the controls needed to ensure the staff involved in the operations is qualified and equipped for the processes, such as:

- Background security screening with academic verifications, identity verifications, reference checks for past employment and security clearance, pending on position and applicable local legislation.
- Attitude to work together for improved security, aligned with business goals
- Training via mandatory annual security training at minimum and with detailed security policies and work instructions
- Sufficient knowledge to work in secure manner, for example to develop secure applications

Information Security works together with HR, process stakeholders and supervisors to ensure the personnel security objectives can be met as needed.

17 Supplier Security Requirements

Aditro extends its security controls and requirements to suppliers and providers of external services to ensure its security objectives can be met.

The areas covered include, but are not limited to:

- Non-disclosure agreements to protect confidential information in personal and company levels
- Documented and communicated security requirements tailored to the acquired service
- Requirements for physical protection, information security, patching level and communication encryption
- Requirements for segregation of duties and access management

The default security requirements and supplier management process are defined in: Aditro Supplier Management Policy and Aditro Supplier Requirements.

Copyright © Aditro. All rights reserved.

18 Technical IT Security

Technical security contains the assets, controls and tools needed to enforce and maintain the security levels for Aditro office network and employee end-points.

The following principles guide the design of technical security measures:

- Asset management to identify and protect critical information and hardware assets
- Centralized application management to ensure compatibility and security
- Access control designed with least privileges needed
- Threat prediction and security monitoring
- Traffic monitoring and logging to protect the critical assets and operations
- Encryption of both computers and traffic where feasible

Information Security works closely with internal IT, stakeholders and external service providers to ensure technical security measures meet the expectations.

Main principles for IT security administration is described in: Cloud and IT Security Policy.
Additional details are documented in IT Security policy and technical documentation.

19 Technical SaaS Security

SaaS security contains the elements of all previous Security areas and operates in the centre of the business to provide secure software-as-a-service (SaaS) for the customers and internal users.

The scope contains, but is not limited:

- Secure communications and technical documentation
- Secure and private data storage practices
- Infrastructure and asset management
- High availability
- Separated administration layers
- Release and deployment for SaaS software processes
- Change management processes
- Support and request management processes
- Recovery and resiliency planning and documentation

The details are described in: Cloud and IT Cloud Security Policy and Cloud Security Overview for SaaS delivery.

20 Security Incident Management

To protect customer data and ensure compliancy, Aditro has defined an incident management process, with escalation steps from event into major/security/personal data breach incidents. The incidents can be triggered by staff observation of input from an external Security Operations Center monitoring.

Aditro works in a transparent manner during the process, involving authorities, customers and other stakeholders as needed.

Copyright © Aditro. All rights reserved.

Details for the process are described in: Security Incident Management SOP and Personal Data Breach Policy.

Incident management process contains analysis of the root cause and steps for continuous improvement.

21 Security auditing, measurements and KPI's

Aditro follows internal auditing plan with integrated management system to ensure security aspects of processes and functions are periodically audited. Security personnel assist the auditors as needed to evaluate the security state in the audits.

Defined security KPI's are reported monthly to the CIO and GMT and are part of annual management review. Each process area is responsible for the daily measurement and monitoring of the security controls in their respective area.

The details are described in: Aditro Compliance Management Policy and Aditro Audit Policy

22 Referenced Information

- Information Security Strategy
- Aditro Risk Management policy
- Security Incident Management SOP
- Aditro Business Continuity Policy
- Aditro Data Protection Policy
- Privacy By Design
- Aditro Development Security Policy
- Aditro Physical Security Policy
- Aditro Supplier Management Policy
- Aditro Supplier Requirements
- Aditro Cloud and IT Security Policy
- Personal Data Breach Policy
- Cloud Security Overview for SaaS delivery
- Aditro Compliance Management Policy

Copyright © Aditro. All rights reserved.