# ONEIO SAAS SECURITY

# INTRODUCTION

Security and building customer trust are top priorities at ONEiO. We prioritize the security of our services to ensure your data's confidentiality, integrity, and availability. This security overview provides a comprehensive understanding of our security practices and measures. We are committed to maintaining a secure environment that aligns with industry standards and best practices.

This document describes technical and organizational security measures and controls implemented by ONEiO (later: “we” or “us”), or our subcontractors, to protect customer data and ensure the ongoing confidentiality, integrity and availability of the ONEiO SaaS.

## What is ONEiO SaaS?

ONEiO is a cloud-based integration service that contains components to manage and run enterprise-grade, highly available and secure integrations. The service is based on our proprietary Integration Automation Platform and is delivered as a continuous service with 24/7/365 end-to-end monitoring that requires no maintenance breaks.

# SHARED SECURITY RESPONSILIBITY MODEL

ONEiO SaaS runs in the Amazon Web Services (AWS) cloud. AWS outlines a shared responsibility model, where responsibilities between customers (in this case, ONEiO) and AWS are defined. In accordance with this model, our security standards are aligned with AWS's security framework. While AWS ensures the security of the underlying infrastructure, network, and physical data centers, we manage and secure the services and applications deployed within the AWS environment, within the services offered to customers. In addition, our customers retain the crucial role of securing their own data, configuring access controls, and implementing security measures. This is valid within their applications, ONEiO subscription, as well as the systems that stand connected to ONEiO for integrations and on the devices they use for accessing ONEiO User Interfaces. Together, we maintain a strong and collaborative approach to ensure the security and compliance of the ONEiO Cloud services hosted on AWS.

ONEiO in itself has been designed with strong security controls in mind, so that a possible extra burden of securely using the service is minimized for the customer. These security controls include  always-on authentication, authorization, encryption in transit, encryption at rest and data retention. In addition to this, we provide automated updates of the service with zero downtime. The chapter *Security Controls* describes these and other controls in more detail.

Ultimately, customers themselves retain the responsibility for securely configuring integrations, deciding what integration data is passed through ONEiO and managing user access to their subscription.

# INFORMATION SECURITY MANAGEMENT SYSTEM

## Overview of Information Security Management System

Our dedicated Information Security Management System (ISMS) is continually maintained and improved based on the requirements of the ISO/IEC 27001:2013 standard. The ISMS preserves the confidentiality, integrity and availability of information by applying a risk management process, serving confidence to interested parties that risks are adequately managed.

## Third-party Audits and Certifications

### ISO 27001 Certification

Our ISMS has been ISO/IEC 27001:2013 certified. The certificates are downloadable from our Security and compliance page.

### GDPR

We prioritize the privacy and confidentiality of our customers' data at ONEiO. We strictly adhere to applicable data protection regulations, such as the General Data Protection Regulation (GDPR), and implement robust measures to safeguard sensitive information. Our data privacy practices include encryption of data in transit and at rest, strict access controls, and regular security audits to identify and address potential vulnerabilities. We also have strict confidentiality agreements with our employees and third-party service providers in place in order to ensure the protection of customer data.

## Information security roles and responsibilities

Information security responsibilities have been defined and allocated in accordance with approved policies for information security. The policies are communicated to all parties required for compliance, employees as well as any external parties.

# Review of information security

The ISMS is reviewed regularly, at a minimum yearly. Both internal and external audits are conducted.

## Compliance with security policies and procedures

The compliance of information processing and procedures with the appropriate applicable security policies is regularly reviewed. The review takes place at minimum every 2 years, or when significant changes occur.

## Technical compliance review

The compliance of information systems with the information security policies is regularly reviewed. The review takes place at minimum every year, or when significant changes occur.

# Risk Assessment and Management

The ISMS contains a methodology for assessment and treatment of information risks at ONEiO. Risk assessment and treatment are regularly reviewed and possible risks are assessed for any new assets that may affect confidentiality, integrity and availability of information in the organization.

# Security Policies and Procedures

## Acceptable Use of Assets Policy

The purpose of this policy is to define the requirements for proper and secure use of ONEiO assets. This policy applies to all ONEiO Cloud Oy, employees, contractors, consultants and other third parties that have access to ONEiO's information or information assets. "Information asset" or "asset associated with information or information processing" (further "asset") is anything that has value to ONEiO and which therefore requires protection. This includes, for instance, but is not limited to, information, hardware, software, laptops and mobile devices.

## Backup Policy

The purpose of this policy is to ensure that backup copies are created at defined intervals and regularly tested. This policy applies to information and information assets in the scope of Information Security Management System.

## Business Continuity Policy

The purpose of this policy is to set key requirements for us to be able to sustain our ability to perform critical processes in case of emergency, including prompt recovery of critical business and information security processes after interruption. This policy

applies to all employees of ONEiO Cloud Oy and its subsidiaries. The users of this policy are our employees defining our business continuity or disaster recovery plans.

The objective of business continuity is to maintain a level of readiness that allows planned recovery within predefined timeframes meeting the company's and its customers' minimum requirements, without causing any risk to personnel or information security.

## Change Management Policy

The purpose of this policy is to set the key requirements for ONEiO change management processes in order to ensure correct and secure operations within the scope of the ISMS. This policy applies to ONEiO Cloud Oy, its subsidiaries and affiliates. The requirements set in this policy are applicable for people defining and implementing change management processes and governance related to changes in the ONEiO software and infrastructure. The users of this policy are all our employees who work with the development, maintenance or operations of the ONEiO service.

## Cryptography Policy

The purpose of this policy is to describe the principles and recommended baseline for ONEiO information encryption and to ensure the proper and effective use of cryptographic controls at ONEiO. This policy contains the approved and recommended solutions and levels of protection for data and transactions, the process for risk assessments concerning cryptographic controls, the responsibilities and approval process for cryptographic solutions. This policy outlines the objectives, scope, approach and the principles concerning the cryptographic controls for protecting information at ONEiO. Cryptographic controls at ONEiO protect the confidentiality, integrity, non-repudiation and authentication of data and transactions.

## Disciplinary Actions on Information Security Violations Procedure

At ONEiO, we do business in a direct, clear and ethical manner. We are accountable for our words and actions, and we have the responsibility to uphold the principles of our Information Security Policy. We also have a responsibility to communicate any violations or potential violations that may occur to the Information Security team. If a breach has occurred by accident, measures to increase awareness and education must be considered first, rather than instigating the disciplinary process. The disciplinary process is designed to help take action in cases of repeated, reckless or intentional violations.

## Disposal and Destruction Policy

The purpose of this policy is to help us safeguard classified information from unauthorized disclosure, as well as to comply with software licensing agreements, data security and privacy laws, and regulations impacting the data security and privacy. This policy applies to information and information assets in the scope of the ISMS. We safeguard classified information from unauthorized disclosure by setting

requirements for the disposal and destruction of our information and information assets.

## Identity and Access Management Policy

This policy defines the mandatory requirements for ONEiO Identity and Access Management (IAM). The Policy outlines the objectives, scope and approach for the processes, controls and practices regarding IAM in ONEiO. The users of this policy are our employees and externals involved in defining or implementing IAM controls or solutions, and IT in general.

## Incident Management Process

The purpose of this document is to define the processes we have in place for reporting and managing information security related incidents and weaknesses. The document also describes the processes for keeping a knowledge base of information security incidents for us to be able to learn from them as an organization, and for collecting evidence of malicious activities to be handed over for officials for criminal investigation. This process outlines the objectives and activities for managing information security incidents and weaknesses at ONEiO.

## Information Classification Policy

The purpose of this policy is to ensure that information is protected at an appropriate level. This policy is applied to the entire ISMS scope, i.e. to all types of information, regardless of the form - paper or electronic documents, applications and databases, people's knowledge, etc.

## Information Security Awareness Policy

The purpose of this policy is to define the level of security awareness education, training and regular updates in organizational policies and procedures aimed to ensure the security awareness at ONEiO. This policy outlines the objectives, scope and approach to our information security awareness. In this policy we define the ways of conducting information security awareness education, training and other activities as well as the process for documenting the level of awareness and measuring the coverage of training and awareness activities.

## Information Security Policy

The aim of this top-level policy is to define the purpose, direction, principles and basic rules for information security management. This policy is applied to the entire ISMS, as defined in the ISMS Scope Document.

## Internal Audit Procedure

The purpose of this procedure is to describe all audit-related activities – writing the audit program, selecting an auditor, conducting individual audits and reporting. This procedure is applied to all activities performed within the ISMS.

## Log Management Policy

This policy's objective is to ensure the recording of events and generating evidence, to ensure that:

1. Audit logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed
2. Log information is protected against tampering and unauthorized access
3. System administrator and system operator activities are logged and the logs protected and regularly reviewed
4. The clocks of all relevant information processing systems within an organization or domain are synchronized to single reference time source
5. Capability to perform security monitoring and investigations can be established and maintained

This policy applies to log data in the scope of the ISMS. This covers all system environments and vendors performing log management on our behalf.

## Network Security Policy

The purpose of this policy is to set the key requirements for ensuring the protection of information in our networks and its supporting information processing facilities. It also describes the principles of secure architecture, design and aspects of controls associated with most common network scenarios. The requirements set in this policy are applicable to all our employees, externals and where relevant, suppliers, defining or implementing network security controls.

## Physical Security Policy

The purpose of this policy is to set the key requirements for ensuring the protection of information in our networks and its supporting information processing facilities. It also describes the principles of secure architecture, design and aspects of controls associated with most common network scenarios. The requirements set in this policy are applicable to all our employees, externals and where relevant, suppliers, defining or implementing network security controls.

## Procedure for Document and Record Control

The purpose of this procedure is to ensure control over creation, approval, distribution, usage and updates of documents and records (also called: documented information) used in the ISMS. This procedure is applied to all documents and records related to the ISMS, regardless of whether the documents and records were created inside ONEiO or whether they are of external origin. This procedure encompasses all documents and records, stored in any possible form - paper, audio, video, etc.

## Procedure for Identification of Requirements

The purpose of this procedure is to define the process of identification of interested parties, as well as legal, regulatory, contractual and other requirements related to

information security, and responsibilities for their fulfillment. This document is applied to the entire ISMS.

## Remote Work Policy

The purpose of this policy is to define the requirements and approach for secure remote working
practices and mobile device use at ONEiO.

## Screening

We have an internal procedure for vetting employees that have access to sensitive or confidential data. New employees are screened already during the hiring process with various checks. Subcontractors are also screened according to the requirements of our Supplier Security Policy.

## Secure Software Development Policy

The purpose of this policy is to ensure that security is taken into account during the entire lifetime of the software. The policy covers the secure software development approach, secure software engineering principles , software development lifecycle, system acquisition and out-sourced development. This policy applies to all software developed by us across the entire period of its use.

## Supplier Security Policy

The requirements in this policy  are applicable to our suppliers and subcontractors (later “supplier(s)”), our subsidiaries and affiliates (collectively as ONEiO), who are authorized to access, store, process, or transmit our information. This policy sets requirements prior to establishing a supplier relationship and also during the relationship and when ending the relationship.

## Vulnerability Management Process

Our Vulnerability Management Process provides a method to manage internal and external vulnerabilities that might present threats to our applications, systems or platforms. This process addresses the identification, evaluation and treatment of vulnerabilities, as well as the verification of applied fixes. This process applies to all our environments, including those used for development and testing, and most importantly all environments in production use.

# BUSINESS CONTINUITY AND DISASTER RECOVERY

There is a business continuity policy and relevant continuity plans in place for us to be able to sustain the ability to perform critical processes in case of emergency, including prompt recovery of critical business and information security processes after interruption.

Backups of all databases are done at least daily, and the backup restoration process is tested at least once per year during our disaster recovery exercises to ensure data can be restored quickly and effectively. The databases use AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data and backups. Keys for disk encryption are managed by AWS. Daily backups are kept for 7 days, weekly backups for 4 weeks and monthly backups for 3 months. Backups are kept in multiple in multiple, geographically separated data centers within the AWS region where the data is used.

We have a Recovery Point Objective (RPO) of 24 hours and Recovery Time Objective (RTO) of 7 hours. These objectives are for disaster situations, which are very unlikely. We are well prepared with a high level of redundancy at multiple levels of the architecture (e.g. replicated databases, 3 separate data centers) and have a track record of zero total service outages that would affect all parts of our service. For cases where servers, storage and networks break, redundancy addresses these issues within seconds.

We have a Service Level Commitment of 99.9% for each calendar month and customers are entitled to compensation if the availability rate falls below the thresholds. See *Service Level Commitment* in ONEiO - SaaS Master Terms.

# SECURITY CONTROLS

## Physical security

ONEiO service is hosted in Amazon Web Services (AWS) region eu-west-1 Ireland or us-west-1 USA. Customers can select which region their subscription is hosted in. AWS data centers are secure by design. AWS has certifications/assessments including ISO 27001, ISO 27017, ISO 27701, ISO 27018, CSA STAR Level 2, SOC 2 and PCI DSS for an independent proof of their compliance controls. More information about AWS data center security controls and compliance:

https://aws.amazon.com/compliance/data-center/controls/

https://aws.amazon.com/compliance/programs/

### Site selection

Data center locations are carefully selected to mitigate environmental risks, like flooding, extreme weather and seismic activity.

### Redundancy and availability

Data centers are designed to tolerate failure while maintaining service levels. Critical system components have been identified and are backed up across multiple locations. The AWS regions where we host our services have at least 3 availability zones, which are discrete data centers. Data center electrical power systems are designed to be fully redundant. Data centers use mechanisms to control climate and maintain an appropriate operating temperature. They are also equipped with fire detection and suppression and leakage detection equipment.

### Security perimeters

Physical access points to server rooms are recorded by CCTV. Physical access is controlled by security staff utilizing surveillance, detection systems and other electronic means. Multi-factor authentication mechanisms are utilized. Entrances to server rooms are secured with devices that sound alarms if the door is forced or held open.

### Access to facilities

Only approved employees have physical data center access. Access is given only for valid business justification and with the principle of least privilege and is time-bound.

# Configuration management

We use a Configuration as Code (CoC) approach, which allows us to easily see the baseline and ensure that all configuration changes have been peer reviewed before configurations are taken into production.

ONEiO service currently uses only server images that are offered and hardened by AWS (i.e. Amazon EKS optimized Amazon Linux AMIs). We follow security best practices from AWS related to server image security. All code changes (including server image changes are code changes, due to our practice of configuration-as-code) are peer reviewed.

# Operations security

## Operational instructions

Procedures to address the configuration, operation and management of systems, networks and services that store or process customer data are documented and maintained. The procedures and additional guidelines are communicated to all persons involved in the processing of customer data.

## Logging and monitoring

Audit logs recording user activities are produced, kept and reviewed. Access to logs is given only for authorized personnel. Services and their resource usage is monitored 24/7 and the operations team alerted of any issues. ONEiO Service related logs are archived in AWS S3, with a retention time of 5 years.

## Protection from disruptions

Our services are protected against disruptions by a high availability design that ensures redundancy and automatic recovery.

# Data security

## Data encryption at rest

ONEiO encrypts integration message contents with the industry standard AES-256 encryption before writing the data into the database. Keys are managed by us, outside of the database. AWS KMS is used for storing master keys. In addition to that, the database uses AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. Keys for disk encryption are managed by AWS. Also database backups are encrypted the same way.

### Data encryption in transit
Data is encrypted in transit using the newest possible TLS version. Currently, TLS versions 1.2 and 1.3 are supported.

### Protection of data
Appropriate processes are implemented to protect data records from loss, destruction, unauthorized access and unauthorized release.

### Data retention
Customer data in integration messages will be automatically deleted from ONEiO database after 30 days. Integration message conversations that contain conversation attributes and message headers (system identifiers, timestamps, entity types and entity identifiers), are kept until 1 year has passed since an integration conversation has had any new messages.

Customers may also request their data to be erased before these retention periods expire.

Upon termination of the customer subscription term, we delete customer data within 30 days from the end of the Integration Subscription Term.

### Password storage
Passwords are stored salted and hashed, using scrypt.

## Personnel access controls

### Authorization
Access to customer data and systems is restricted to only those support and operations personnel whose access is necessary to providing and maintaining the service.

### Least privilege user accounts
When personnel are given access, the permissions are given using the least privilege principle.

### Need-to-know access
We will not access customer's data for any purpose other than as necessary to perform our obligations to the customer.

### Suspension or termination of access rights
Upon suspension or termination of personnel or external party users, access rights to customer data and systems are removed.

### Access control system
We use an access control system to control access to our information systems, including the ONEiO service. Access rights are periodically reviewed based on the basic principle of least privilege and need-to-know. We maintain and update records of personnel authorized to access systems that contain customer data.

### Authentication
We use industry standard practices to identify and authenticate users who attempt to access information systems.

### Passwords
In cases where authentication is based on passwords, passwords are required to conform to strong password policies (length, character set, etc).

### Multi-factor
Multi-factor authentication is used everywhere it's possible to use it.

## Communications security

### Firewall
ONEiO SaaS is protected inside environment-specific AWS Virtual Private Clouds (VPC). ONEiO SaaS has static IP addresses for both inbound and outbound traffic, making it easy for customers to configure their own firewalls when limiting access to their internal systems.

### Intrusion detection
We use AWS GuardDuty as a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect our servers, AWS accounts and workloads. It combines managed rule-sets, threat intelligence from AWS security and 3rd party intelligence partners, anomaly detection and Machine Learning to intelligently detect malicious or unauthorized behavior.

## Authentication
For end-user access, ONEiO service currently supports 2-step verification with username-password pair and an additional code sent to the user's email address.

Integration endpoints can be authenticated using various authentication methods, for example OAuth2, HTTP Basic, mutual certificate authentication, to name a few.

# PENETRATION TESTING, VULNERABILITY SCANNING AND AUDIT REPORTS

## Penetration testing

ONEiO software is audited yearly by an independent third party. The latest web application security audit was conducted in August 2022. An independent auditor has audited and verified the information security of the ONEiO App and API. According to the audit and the fix verification, the service has no critical, high or moderate security vulnerabilities. The audit methodology was based on industry standards and best practices, such as OSSTMM (Open Source Security Testing Methodology Manual) and OWASP (Open Web Application Security Project).

The audit was performed in August 2022 with a workload of 11.5 days. Implemented fixes were verified in November 2022 and the workload was 1.5 days.

## Security and vulnerability scanning and patch management

We have a Vulnerability Management Process that provides a method to manage internal and external vulnerabilities that might present threats to ONEiO applications, systems and platforms. This process addresses the identification, evaluation and treatment of vulnerabilities, as well as the verification of applied fixes. This process applies to all our environments, including those used for development and testing, and most importantly all environments in production use.

There are multiple sources for vulnerability intelligence in use at ONEiO, like tools for static code analysis, open source library vulnerability scanners, container scanners, AWS security tools, threat intelligence from security feeds and new sources, reporting from employees, customers and security researchers.