oneflow

# Security White Paper

# Document Control

| | |
|---|---|
| **Title** | Security White Paper |
| **Version** | 1.2 |
| **Date Issued** | 05/07/2024 |
| **Status** | Published |
| **Document owner** | Information Security |
| **Creator Name** | Anastasiia Berveno |
| **Document Classification** | External |

Overview 3
Introduction 4
Information Security Management System 5
Hardware and infrastructure 6
Access control 7
Business Continuity and Availability 8
Privacy 9
GDPR 10
Confidentiality 10
Data retention 11
Risk management 12
Incident management 12
Vulnerability and Patch management 13
Third party subcontractors 13
Cyber Security Insurance 14

# Overview

Oneflow is an end-to-end SaaS solution for all your contract needs. We are passionate about contracts, templates, and the collaboration that takes place during the process. We love taking care of your contracts and giving you full control of all your obligations and rights. This is our pride and passion, and the core of our expertise.

Oneflow lets you author, collaborate, sign, analyze, and manage the lifecycle of your contracts in one workspace. Discuss and negotiate a contract effectively and securely with your colleagues, customers, partners, and vendors without creating long email threads. Make edits on the fly without going back and forth to your Word and PDF files.

Oneflow will notify you of the changes, statuses, and key lifecycle events like renewals and end dates. And you can automate workflows by integrating Oneflow with your favorite apps or business systems.

Save time and work smarter. Oneflow makes the contract process digital, effective, and efficient. Plus your contracts will always look awesome regardless of what device is used.

# Introduction

The purpose of this document is to give an overview of how Oneflow implements a security framework to safeguard customer data, and how surrounding policies and management processes support this framework.

First, we'll detail our Information Security Management System, how storage, server, network, and service security work, by themselves and together, to ensure the security of data, and how we use redundancy and backups to increase service availability, and safeguard data. We are ISO 27001 certified, underscoring our commitment to maintaining the highest standards of information security management.

The document will then give an overview of the General Data Protection Regulation (GDPR), how GDPR impacts the service and how it impacts contracts, and our approach to ensuring the lawfulness of processing by Oneflow for this purpose.

We then explain how our development process and our change management framework help the development team improve the service and add features, while keeping the service running and secure. Finally, our support policies are explained, and how we regulate access to customer data and systems containing customer data.

# Information Security Management System

Oneflow is certified in Information Security (ISO 27001) as of July 2024. We are happy to provide certificates and further details upon request. Implementing appropriate security measures is vital to us and a significant part of our business includes keeping up to date with information security standards and legislation. We have proactive measures in place through e.g. encryption, backup and impact assessments.

Learn more about each of the ISO certifications here.

Additionally, Oneflow is aligned to the NIST framework and has a range of internal policies, procedures, and guidelines which form our Information Security Management System and govern our approach to security and privacy. Policies are made available to all employees and all employees are required to read the policies;
A selection of our policies within Oneflow is shown below:

- Information Security Policy
- Information Security Risk Management Policy
- Information Security Incident Management Policy
- Acceptable Use Policy
- Access Control Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Policy
- Supplier Security Policy
- Secure Development Policy
- Change Management Policy
- Log Management Policy

- Decommissioning and Destruction Policy
- Workplace flexibility policy

All employees are required to complete mandatory Information Security and Privacy training annually. Employees are prohibited from storing customer data on end-user devices.

# Hardware and infrastructure

The Oneflow service is deployed and runs on top of Amazon Web Services (AWS), a cloud services provider. This means that we can leverage the experience and expertise of AWS in keeping the infrastructure secure, available, and healthy, while we focus on your contracts. We run the application in multiple separate availability zones (AZs), to maximize availability, and utilize AWS clustering services that automatically handle and mitigate network and hardware issues.

Our service is deployed within a Virtual Private Cloud (VPC), and further sectioned into subnets and security groups. This lets us segregate public and private systems, and keep fine-grained control over network traffic and services' access to systems. Further, all traffic to and from the service is transmitted encrypted, and all data stored by the service is encrypted at rest.

Server systems, when not running managed services, are set up using source-controlled templates. This allows us to quickly provision new servers when necessary.

Further, we use this system to verify and update the state of systems. Servers are isolated from each other by design and by default. As we are running in the cloud, hardware issues and network issues relating to these systems are handled by AWS. The automation of setup and cloud provisioning allows us to replace systems in case of issues.

# Access control

Authentication is required to gain access to the Oneflow application; multi-factor authentication and SSO integration is available and can be implemented for extra security. Users are only able to view contracts they have been granted access to. Segregation can be achieved within the same organisation, for example, a person who has access to one company workspace does not automatically have access to other workspaces and their contracts as there are different levels of access within the application; External counterparties can only view contracts that they are a party to.

In addition, access to systems by Oneflow employees is limited, tamperproof, and logged with timestamps, user, and type of access; logs are encrypted and stored in AWS Ireland and backed up to AWS Stockholm. In the rare event access is required to customer data for the purpose of providing support, Oneflow will first seek permission from the customer before accessing the customer's environment.

As for our offices, we have strong network security which consists of firewalls, switches, routers, and segregated wireless networks; Appropriate controls are in place to ensure the network is secure. Oneflow has a CYOD (Choose your own device policy) which addresses remote devices used to access corporate applications

such as emails, the policy details security requirements and obligations. All access is routed through secure VPNs and there are no differences in security postures depending on where our employees access our systems. User device management is rolled out and single sign-on or multi-factor authentication is used to gain access to internal systems.

# Business Continuity and Availability

The Oneflow application is built with redundancy at every layer of its infrastructure. AWS is utilised to achieve a secure, redundant system. The application, databases, storage, and auxiliary services are hosted by AWS in multiple AZs in Ireland, EU to allow for sporadic failures without any loss of availability, functionality, or customer data. Using the AWS platform allows us to easily scale the platform up, both to meet increased load, and to increase redundancy. This is true for all levels of the service, from our CDN, to our application load balancers, to the application servers themselves, the backend workers, the search services, and the storage layers.

To maintain the availability of the Oneflow application, a change management process is also in place which ensures changes are reviewed before being applied to the application thus further reducing the possibility of unscheduled downtimes.

# Privacy

The concept “Privacy by design and by default” is always adhered to throughout the product development process as it allows us to limit the risk of introducing insecure code or experiencing system outages. Developers always consider the following:

- **Sensitive information** – Does the code expose any sensitive information?
- **Establish the context** – Does the intended purpose of the code being developed meet the acceptable risk parameters?
- **Making intrusion difficult** – Is all aspects of the code and system difficult to compromise and does the new negatively impact pre-existing code?
- **Making disruption difficult** – Is the system and code resilient and not easily susceptible to denial-of-service attacks and usage spikes?
- **Making intrusion detection easier** – Is the code and system designed in a manner which allows suspicious activity to be noticed easily, e.g. are adequate logging and monitoring in place?
- **Reducing the impact of intrusion** – is the system developed in a manner which minimizes the escalation and blast radius of an intrusion; including structuring functionality in a way which does not allow unnecessary connections to other parts of the system?
- **Protection against common vulnerabilities** – Are systems developed safe against most vulnerabilities e.g., OWASP Top 10?

Penetration testing is carried out by external parties at least annually or whenever significant changes have been made; Vulnerabilities identified are addressed in line with our Information Security Risk Management Policy and remediated.

# GDPR

Oneflow has implemented technical and organizational measures according to the GDPR requirements to protect personal data from disclosure, removal, or modification.

We have proactive measures in place to ensure compliance is maintained by deploying controls to limit access to those with an absolute need for it, encrypting data, implementing privacy by default and by design in our development, taking robust backups and conducting impact assessments. Security is a serious and important area and part of our responsibilities includes keeping up to date with current legislation and the latest information security best practices.

We aim to provide assistance to customers to fulfill their obligations under GDPR when a Data Subject Access Request is made. Oneflow considers right to data portability and to be forgotten by handling data in a way that makes removal and porting possible, through automatic transmission or file export.

GDPR gives everyone the right to demand full disclosure of their personal data from companies at any time. The disclosure has to be provided in an easy to access digital format, and is a central part of our customers' obligations towards their end customers, employees, and vendors.

# Confidentiality

Our systems are designed by default to not allow customer data to be extracted from production to ensure the confidentiality of the

system and the data held within it is not compromised. Customer and system data is stored at encrypted mirrored databases in multiple different AZ's with multiple layers of backup strategies. Customer documents and files are encrypted and stored on Amazon Simple Storage Service (S3) and are replicated across multiple data centers automatically. System logs and authentication logs are stored for 90 days, followed by 30 days off-site backup.

Data is encrypted in transit and at rest; TLS 1.2 is currently being used to encrypt data in transit, from the public internet to our CDN edge locations, all the way into our internal network before being processed. Additionally, databases, servers, and file storage all encrypt data before storing it at rest utilizing state-of-the-art encryption with the AES 256 algorithm.

Customer data is not stored on end-user devices such as laptops; this is also mentioned within our Acceptable Use Policy. All Employees are made aware of their responsibilities for Information Security, Compliance, and confidentiality within their employment contract and are required to complete mandatory Information Security and Privacy training annually.

# Data retention

Contracts are stored within the Oneflow application indefinitely, however, customers can configure different retention periods for their contracts to match their own data retention policies.

# Risk management

Our Information Security Risk Management Policy details how risks should be identified, analysed, evaluated, and mitigated. Risks are scored based on their likelihood of occurring and the potential impact to the organization and its customers. All risks are assessed and remediated in accordance with our remediation timelines which are based on best practices.

# Incident management

In regard to Incident Management, we have an Information Security Incident Management Policy in place including identification, classification, logging, notification, analysis, remediation, and incident postmortems. We aim to notify customers within 24 hours of a confirmed breach. All incidents are impact assessed and categorised to determine their severity and urgency.

# Vulnerability and Patch management

To minimize vulnerabilities within Oneflow products and its infrastructure, penetration tests are carried out by reputable external parties at least annually or whenever significant changes have been made. In addition, vulnerability scans are conducted on a regular basis in order to capture vulnerabilities within the infrastructure as well as regular checks on reputable websites and vendor websites for known vulnerabilities. We also utilize

automated code scanning whenever a change is made to the Oneflow applications.

Identified vulnerabilities are categorized based on the Common Vulnerability Scoring System (CVSS) and addressed in line with Oneflow's Information Security Risk Management Policy and remediated accordingly. Patches are tested on staging and testing environments before being applied to production.

# Third-party subcontractors

Oneflow uses a small number of subcontractors to provide services to its customers, these can be found on our website here.

Secure storage and processing of data is of utmost importance to us. Oneflow's services are hosted on Amazon Web Services (AWS), which stores the data in compliance with the regulations within Europe. AWS' safety work complies with the industry standard and CISPE.

# Cyber Security Insurance

We understand things do not always go to plan and as such Oneflow has a comprehensive Cyber Security Insurance plan in place to cover those situations that are simply out of our control in order to put our customers at ease. We have cover for Data breaches, regulatory fines, interruptions, and damages.

oneflow

# For more information, go to oneflow.com

Oneflow AB
Corporate identity no: 556903-2989
oneflow.com | +46 8 517 297 70
Gävlegatan 12 A | 113 30 Stockholm | Sweden

Read more