IT Security Policy

Effective date: 17.05.2024.

Security is very important to Unicis and everyone here is doing their best to keep your presentations and data secure. This document describes our internal security policies, and minimum security baseline and how those translate into creating a secure platform, add-ons and plugins that you can trust.

We at Unicis are using the Minimum Viable Secure Product (MVSP) as a baseline for enterprise-ready products and services.

MVSP

Data Protection

You can request the Data Processing Agreement example, and by contacting us.

GDPR, DPA, privacy, data-protection

GDPR

We are committed to follow and implement all the guidelines and recommendations from GDPR with regards to all the data and information we handle, process, and store at Unicis.

GDPR

Data Security

All of Unicis infrastructure runs in OVHCloud, hosted in European regions. You can find more information about security practices on their cloud security page.

Data Encryption at Rest

We use hybrid cloud services, and configured to use AES-256 encryption for all data at rest.

Data Classification

We like to keep our data organized, and for that we created different categories on which all Unicis's data needs to be categorized. The categories define who can access it and which level of monitoring they receive:

- **Public**: Information available in our main website and marketing information
- **Internal**: Unreleased information and details about Unicis roadmap
- **Confidential**: Customers' data and Unicis employees' information

Data Transport Security

All communications with Unicis servers is done over TLS.

Application Security

Code Security

At Unicis we inspect closely any code before it is release. Our developers inspect the logic and information flows of each new feature to ensure no security vulnerabilities are introduced. But because humans aren’t perfect we also write tests to ensure the application does not behave in an unexpected way.

We also run semiautomatic scanning tools for new features to find any security problems.

Authentication

We enforced two-factor authentication (2FA), and Single Sign-On (SSO) for all internal and external tools that we use at Unicis.

Password Policy

The complexity of the password must be at least 12 characters, and it must contain at least one uppercase and lowercase letter, digit, and special character.

If password authentication is used in addition to single sign-on, we enforce:

- Do not limit the permitted characters that can be used
- Do not limit the length of the password to anything below 64 characters
- Do not use secret questions as a sole password reset requirement
- Require email verification of a password change request
- Require the current password in addition to the new password during password change
- Store passwords in a hashed and salted format using a memory-hard or CPU-hard one-way hash function
- Enforce appropriate account lockout and brute-force protection on account access
- Do not provide default passwords for users or administrators

password, policy

Third-Party components

We use third-party libraries to make our application better every day. Hence we review and monitor our third-party components and libraries for known vulnerabilities using automatic systems like Dependency Scanning, Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST). Each report is analyzed and acted on based on the criticality of the vulnerability, with a response time from 1-3 days for critical vulnerabilities to 8-14 days for medium risk vulnerabilities (as defined by their CVSS score).

Application Implementation Security

List of data

We maintain a list of sensitive data types that the application is expected to process.

Data flow diagram

At Unicis we maintain an up-to-date diagram indicating how sensitive data and where it ends up being stored.

Infrastructure Security

Network Segmentation

Inside our hybrid cloud infrastructure we segment our network into different areas, decoupling our production environments from our testing and development environments.

Incident Monitoring

We use monitoring services to alert us on any anomalous behavior and any suspicious activity within our backend systems and in our infrastructure.

Third-Party Integrations

As listed in our website, we have integrations for Atlassian products.

We follow Atlassian Marketplace Bug Bounty Program and complete Security-Self-Assessment Program.

Organizational Security

Security Incident Management

Our systems monitor for anomalous and suspicious activity across the different systems we use to run the platform.

Each and every incident at Unicis goes through the rigorous internal incident management process. This allows us to ensure to identify the root cause of the incident and it is resolved. The process also describes how to escalate and communicate these incidents to the different parties involved.

Asset Management

We maintain and regularly update an internal Threat Model of our infrastructure, assets, and application. We define the type of data and risk that each component is exposed to and how we protect these. This help us in segregating our infrastructure and maintaining a minimum access policy approach and need to know principle.

Operational Security

Sub-processors

At Unicis we maintain a list of third-party companies with access to customer data, and make it available to

clients and business partners upon request, and assess third-party companies annually against the latest MVSP release.

Backups

Unicis's infrastructure is built on top of hybrid cloud providers and we use their services to generate daily backups for our database that are then retained for up to 30 days. To ensure data recovery process is working as intended, we execute data recovery exercises regularly.

Risk Management

We perform periodic risk analysis and assessments to ensure that our information security policies and practices meet the requirements and applicable regulatory obligations.

Security Vulnerability Disclosure Policy

We always appreciate when Unicis users and security researchers contact us regarding security vulnerabilities. There is no 100% secure product. Feel free to reach us at security (at) unicis (dot) tech. More details see security.txt or OpenBugBounty Program.

it-security, policy, cybersecurity, tom, toms, mvsp, vdp, risk-management, password, data, security