# Vitorlocateli: security audit report

Created on 10 November 2025 @ 20:08

Vitorlocateli wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at Vitorlocateli is being monitored and safeguarded from the developer's computer all the way to the infrastructure used for delivery.

This security report has been generated by Aikido Security based on real-time monitoring of Vitorlocateli code and infrastructure.

## Aikido benchmark

Bottom
**30%**
of accounts

This percentage gives an indication of your security posture as a company, compared to all other Aikido customers.

| Section | Score |
|---|---|
| Score for code repositories | N/A |
| Score for cloud environment | N/A |

## OWASP Top 10

This section details the OWASP risks for which the organization currently has active measures against.

| Code | Title | Taken measures |
|---|---|---|
| A01:2021 | Broken access control | ✓ Application is properly configured<br>✓ Prevents unauthorized access to resources |
| A02:2021 | Cryptographic failures | ✓ Enforces encryption of data at rest<br>✓ Enforces the use of secure connections<br>✓ Prevents the exposure of secret keys |
| A03:2021 | Injection | ✓ App scanned for SQL injection attack<br>✓ Prevents remote code execution<br>✓ Prevents CSRF attacks<br>✓ Prevents Cross Site Scripting (XSS)<br>✓ Prevents command injection |
| A04:2021 | Insecure design | Monitoring, not fully compliant |
| A05:2021 | Security misconfiguration | ✓ Application is properly configured |
| A06:2021 | Vulnerable and Outdated Components | Monitoring, not fully compliant |
| A07:2021 | Identification and Authentication Failures | ✓ Prevents bypassing authorization controls<br>✓ Prevents improper certificate validation |
| A08:2021 | Software and Data Integrity Failures | ✓ Takes measures to ensure proper deserialization |
| A09:2021 | Security Logging and Monitoring Failures | Monitoring, not fully compliant |
| A10:2021 | Server-Side Request Forgery | ✓ App scanned for SSRF attack opportunities |

## ISO 27001:2022 compliance

A brief overview of the ISO 27001 requirements and any measures taken for these.

| Title | Taken measures |
|---|---|
| A.8.2 - Privileged access rights | Monitoring, not fully compliant |
| A.8.3 - Information access restriction | Monitoring, not fully compliant |
| A.8.5 - Secure authentication | Monitoring, not fully compliant |
| A.8.6 - Capacity management | Monitoring, not fully compliant |
| A.8.7 - Protection against malware | ✓ Prevents unwanted write operations to filesystems |
| A.8.8 - Management of technical vulnerabilities | Monitoring, not fully compliant |
| A.8.12 - Data leakage prevention | ✓ Prevents remote code execution<br>✓ Has measures against SQL injection attacks<br>✓ Prevents XSS attacks |
| A.8.13 - Backups | Monitoring, not fully compliant |
| A.8.15 - Logging | Monitoring, not fully compliant |
| A.8.18 - Use of privileged utility programs | ✓ Prevents the exposure of sensitive data |
| A.8.20 - Network security | Monitoring, not fully compliant |
| A.8.31 - Separation of development, test and production environments | Monitoring, not fully compliant |
| A.8.24 - Use of cryptography | ✓ Uses secure cookies<br>✓ Uses up-to-date cryptographic libraries |

| | |
|---|---|
| A.8.9 - Configuration management | Monitoring, not fully compliant |
| A.8.16 - Monitoring activities | Monitoring, not fully compliant |
| A.8.25 - Secure development lifecycle | ✓ Has connected a code repository |
| A.8.28 - Secure coding | Monitoring, not fully compliant |
| A.8.32 - Change management | Monitoring, not fully compliant |
| A.5.15 - Access control | ✓ Prevents the exposure of sensitive data |
| A.5.16 - Identity management | Monitoring, not fully compliant |
| A.5.28 - Collection of evidence | Monitoring, not fully compliant |
| A.5.33 - Protection of records | Monitoring, not fully compliant |

## Esquema Nacional de Seguridad (ENS) compliance

A brief overview of the ENS requirements and any measures taken for these.

| Título | Medidas Tomadas |
|---|---|
| [op.pl.4] Planificación\Dimensionamiento - gestión de la capacidad | No se han tomado medidas activas |
| [op.acc.1] Control de acceso\Identificación | No se han tomado medidas activas |
| [op.acc.2] Control de acceso\Requisitos de acceso a la información | No se han tomado medidas activas |
| [op.acc.2] Control de acceso\Requisitos de acceso - programas utilitarios privilegiados. | ✓ Prevenir la exposición de data sensible |
| [op.acc.2] Control de acceso\Requisitos de acceso - acceso a la información - mínimo privilegio | ✓ Prevenir la exposición de data sensible |
| [op.acc.4] Control de acceso\Proceso de gestión de derechos de acceso privilegiados | No se han tomado medidas activas |
| [op.acc.6] Control de acceso\Mecanismo de autenticación (usuarios de la organización) | No se han tomado medidas activas |
| [op.exp.3] Explotación\Gestión de la configuración | No se han tomado medidas activas |
| [op.exp.4] Explotación\Mantenimiento y actualizaciones de seguridad - Gestión de vulnerabilidades técnicas | No se han tomado medidas activas |
| [op.exp.5] Explotación\Gestión de cambios en sistemas y aplicaciones | No se han tomado medidas activas |

| | |
|---|---|
| [op.exp.6] Explotación\Protección frente a código dañino | ✓ Prevención de operaciones de escritura no deseadas en sistemas de archivos |
| [op.exp.8] Explotación\Registro de la actividad y eventos de seguridad | No se han tomado medidas activas |
| [op.exp.8] Explotación\Registro de la actividad y logs de actividad | No se han tomado medidas activas |
| [op.exp.9] Explotación\Registro de la gestión de incidencias - recolección de evidencia | No se han tomado medidas activas |
| [op.mon.3] Monitorización del sistema\Vigilancia - monitoreo de actividades y eventos de seguridad | No se han tomado medidas activas |
| [mp.com.1] Protección de las comunicaciones\Perímetro seguro - medidas de seguridad para proteger la red | No se han tomado medidas activas |
| [mp.si.2] Protección de los soportes de información\Criptografía | ✓ Uso seguro de cookies<br>✓ Uso de librerías criptógraficas actualizadas |
| [mp.sw.1] Protección de las aplicaciones informáticas\Desarrollo de aplicaciones - separación de los entornos | No se han tomado medidas activas |
| [mp.sw.1] Protección de las aplicaciones informáticas\Ciclo de vida de desarrollo seguro de aplicaciones | ✓ Ha conectado un repositorio de código |
| [mp.info.6] Protección de la información\Copias de seguridad | No se han tomado medidas activas |
| [mp.s.1] Protección de los servicios\correo electrónico - medidas prevenir la fuga de datos | ✓ Prevención de ejecución remota de codigo<br>✓ Se tienen medidas para proteger contra ataques de inyección de SQL<br>✓ Prevención contra ataques de Cross-Site Scripting (XSS) |

## SOC2 compliance

A brief overview of the SOC2 requirements and any measures taken for these.

| Title | Taken measures |
|---|---|
| CC3.3: Consider the potential for fraud | Monitoring, not fully compliant |
| CC3.2: Estimate Significance of Risks Identified | ✓ Does not have any severe surface monitoring issues<br>✓ Does not have any severe open source dependency issues<br>✓ Configured monitoring for code repositories<br>✓ Configured monitoring for container images |
| CC5.2: The entity selects and develops general control activities over technology to support the achievement of objectives | ✓ Does not have any severe infrastructure as code issues |
| CC6.1: Restricts logical access | ✓ Prevents the exposure of sensitive data<br>✓ Has measures against SQL injection attacks<br>✓ Is protected against SSRF attacks<br>✓ Is protected against command injections attacks<br>✓ Prevents XSS attacks |
| CC6.1: Consider network segmentation | Monitoring, not fully compliant |
| CC6.1: Restrict access to information assets | Monitoring, not fully compliant |
| CC6.1: Manages credentials for infrastructure and software | Monitoring, not fully compliant |
| CC6.1: Use encryption to protect data | ✓ Enforces encryption of data in transit<br>✓ Uses up to date cryptography libraries |
| CC6.6: Restrict Access | Monitoring, not fully compliant |

| | |
|---|---|
| CC6.6: Require additional authentication or credentials | Monitoring, not fully compliant |
| CC6.6: Implement boundary protection system | Monitoring, not fully compliant |
| CC6.7: Use encryption technologies or secure communication channels to protect data | ✓ Uses up to date cryptography libraries |
| CC6.8: Restrict application and software installation | ✓ Protects unauthorized runtime access<br>✓ Prevents container orchestration takeover |
| CC6.8: Detect unauthorized changes to software and configuration parameters | Monitoring, not fully compliant |
| CC6.8 Use anti-virus and anti-malware software | ✓ Aikido Malware Scanner is enabled |
| CC7.1: Monitor infrastructure and software | ✓ Connected code repositories |
| CC7.1: Implement change detection mechanism | Monitoring, not fully compliant |
| CC7.1: Detect unknown or unauthorized components | ✓ Does not have risky licenses |
| CC7.1: Conduct vulnerability scans | ✓ Connected code repositories |
| CC7.1: Implement filters to analyze anomalies | ✓ Connected code repositories |
| CC7.1: Restores the affected environments | ✓ Has no critical open source dependency issues |
| CC8.1: Protect confidential information | ✓ Prevents the exposure of sensitive data |
| CC8.1: Track system changes | Monitoring, not fully compliant |

| | |
|---|---|
| CC10.3: Tests integrity and completeness of backup data | Monitoring, not fully compliant |

## CIS Controls compliance

A brief overview of the CIS controls and any measures taken for these.

| Title | Taken measures |
|---|---|
| 2.2 Ensure Authorized Software is Currently Supported | Monitoring, not fully compliant |
| 3.3 Configure Data Access Control Lists | Monitoring, not fully compliant |
| 3.4 Enforce Data Retention | ✓ Enabled security logging for cloud instances |
| 3.10 Encrypt Sensitive Data in Transit | ✓ Enforces encryption of data in transit |
| 3.11 Encrypt Sensitive Data at Rest | ✓ Encrypts data at rest |
| 3.14 Log Sensitive Data Access | ✓ Enabled security logging for cloud instances |
| 4.4 Implement and Manage a Firewall on Servers | ✓ Prevents unauthorized public access to file storage |
| 4.6 Securely Manage Enterprise Assets and Software | ✓ Enforces latest TLS version<br>✓ Enforces encryption of data in transit |
| 4.9 Configure Trusted DNS Servers on Enterprise Assets | ✓ Uses DNSSEC extensions |
| 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts | Monitoring, not fully compliant |
| 6.5 Require MFA for Administrative Access | Monitoring, not fully compliant |
| 6.4 Require MFA for Remote Network Access | Monitoring, not fully compliant |

| | |
|---|---|
| 7.1 Establish and Maintain a Vulnerability Management Process | Monitoring, not fully compliant |
| 8.2 Collect Audit Logs | ✓ Enabled security logging for cloud instances |
| 10.1 Deploy and Maintain Anti-Malware Software | ✓ No malware issues<br>✓ Prevents unwanted write operations to filesystems |
| 11.2 Perform Automated Backups | ✓ Has backups for stateful cloud resources |
| 12.3 Securely Manage Network Infrastructure | ✓ Prevents unauthorized public access to networks and instances |
| 12.6 Use of Secure Network Management and Communication Protocols | ✓ Prevents unauthorized public access to networks and instances<br>✓ Enforces encryption of data in transit<br>✓ Uses secure communications protocols |
| 13.6 Collect Network Traffic Flow Logs | ✓ Enabled security logging for cloud instances |
| 16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities | Monitoring, not fully compliant |
| 16.5 Use Up-to-Date and Trusted Third-Party Software Components | ✓ No risky licenses in 3rd party dependencies |
| 16.8 Separate Production and Non-Production Systems | Monitoring, not fully compliant |
| 16.12 Implement Code-Level Security Checks | Monitoring, not fully compliant |

## CIS AWS benchmark compliance

A brief overview of the CIS AWS benchmark and any measures taken for these.

| Title | Taken measures |
|---|---|
| 2.3 No root user account access key exists | Monitoring, not fully compliant |
| 2.4 MFA is enabled for the root user account | Monitoring, not fully compliant |
| 2.7 IAM password policy requires minimum length of 14 or greater | Monitoring, not fully compliant |
| 2.8 IAM password policy prevents password reuse | Monitoring, not fully compliant |
| 2.9 MFA is enabled for all IAM users with console access | Monitoring, not fully compliant |
| 2.11 Credentials unused for 45 days are disabled | Monitoring, not fully compliant |
| 2.12 There is only one active access key per IAM user | Monitoring, not fully compliant |
| 2.13 Access keys should be rotated every 90 days | Monitoring, not fully compliant |
| 2.14 IAM users receive permissions only through groups | Monitoring, not fully compliant |
| 2.15 IAM policies allowing full administrative privileges are not attached | Monitoring, not fully compliant |
| 2.16 Support role has been created to manage incidents with AWS Support | Monitoring, not fully compliant |

| | |
|---|---|
| 2.17 IAM instance roles are used for AS resources access from instances | Monitoring, not fully compliant |
| 2.18 IAM SSL/TLS certificates are not expired | Monitoring, not fully compliant |
| 2.19 IAM External Access Analyzer is enabled for all regions | Monitoring, not fully compliant |
| 2.21 Access to CloudShell is restricted | Monitoring, not fully compliant |
| 3.1.1 S3 Bucket Policy denies HTTP requests | Monitoring, not fully compliant |
| 3.1.2 MFA delete is enabled on S3 buckets | Monitoring, not fully compliant |
| 3.1.4 S3 is configured with 'Block Public Access' enabled | Monitoring, not fully compliant |
| 3.2.1 RDS data is encrypted at rest | Monitoring, not fully compliant |
| 3.2.2 'Auto Minor Version Upgrade' is enabled for RDS instances | Monitoring, not fully compliant |
| 3.2.3 RDS instances are not publicly accessible | Monitoring, not fully compliant |
| 3.2.4 RDS clusters use Multi-AZ for enhanced availability | Monitoring, not fully compliant |
| 3.3.1 EFS files systems are encrypted at rest | Monitoring, not fully compliant |
| 4.1 Cloudtrail enabled in all regions | Monitoring, not fully compliant |
| 4.2 Cloudtrail log validation is enabled | Monitoring, not fully compliant |
| 4.3 AWS Config enabled in all regions | Monitoring, not fully compliant |

| | |
|---|---|
| 4.4 Cloudtrail logs have server access logging enabled | Monitoring, not fully compliant |
| 4.5 Cloudtrail logs are encrypted at rest using a CMK | Monitoring, not fully compliant |
| 4.6 Symmetric CMKs rotation is enabled | Monitoring, not fully compliant |
| 4.7 VPC flow logging is enabled in all regions | Monitoring, not fully compliant |
| 4.8 Ensure object-level logging for S3 write events is enabled | Monitoring, not fully compliant |
| 4.9 Ensure object level logging for S3 read events is enabled | Monitoring, not fully compliant |
| 6.1.1 EBS volumes are encrypted by default | Monitoring, not fully compliant |
| 6.1.2 CIFS access is restricted to trusted networks | Monitoring, not fully compliant |
| 6.3 Security groups do not allow ingress from 0.0.0.0/0 on server admin ports | Monitoring, not fully compliant |
| 6.4 Security groups do not allow ingress from ::/0 on server admin ports | Monitoring, not fully compliant |
| 6.5 Default security groups restricts all traffic | Monitoring, not fully compliant |
| 6.7 EC2 metadata service only allows IMDSv2 | Monitoring, not fully compliant |

## NIS2 compliance

A brief overview of the NIS2 directive and any measures taken for these.

| Title | Taken measures |
|---|---|
| Policies on risk analysis and information system security | ✓ Configured monitoring for code repositories |
| Incident handling | Monitoring, not fully compliant |
| Business continuity | Monitoring, not fully compliant |
| Supply chain security | Monitoring, not fully compliant |
| Security in network and information systems acquisition | Monitoring, not fully compliant |
| Policies and procedures regarding the use of cryptography | ✓ Uses secure cookies<br>✓ Uses up-to-date cryptographic libraries |
| Access control policies and asset management | Monitoring, not fully compliant |
| The use of multi-factor authentication | Monitoring, not fully compliant |

## NIST 800-53 compliance

A brief overview of the NIST directive and any measures taken for these.

| Title | Taken measures |
|---|---|
| 1.2.4 Account Management \| Disable Accounts | Monitoring, not fully compliant |
| 1.2.5 Account Management \| Automated Audit Actions | Monitoring, not fully compliant |
| 1.2.8 Account Management \| Privileged User Accounts | Monitoring, not fully compliant |
| 1.2.13 Account Management \| Account Monitoring for Atypical Usage | Monitoring, not fully compliant |
| 1.3.8 Access Enforcement \| Role-based access control | Monitoring, not fully compliant |
| 1.4.22 Information Flow Enforcement \| Physical or Logical Separation of Information Flows | ✓ Enforces safe SSL protocol usage<br>✓ Prevents abuse of cookies<br>✓ Uses up to date cryptography libraries |
| 1.6.2 Least Privilege \| Authorize Access to Security Functions | ✓ Enforces safe SSL protocol usage |
| 1.17.2 Remote Access \| Monitoring and Control | Monitoring, not fully compliant |
| 1.17.6 Remote Access \| Monitoring for Unauthorized Connections | Monitoring, not fully compliant |
| 1.23.1 Data Mining Protection | ✓ Restrict excessive or unauthorized data mining queries. |
| 3.6.2 Audit Record Review, Analysis, and Reporting \| Automated Process Integration | ✓ Limit access to sensitive data based on user roles and responsibilities. |

| | |
|---|---|
| 3.9.4 Protection of Audit Information \| Cryptographic Protection | ✓ Enforces safe SSL protocol usage<br>✓ Prevents abuse of cookies |
| 3.9.5 Protection of Audit Information \| Access by Subset of Privileged Users | Monitoring, not fully compliant |
| 3.11.2 Audit Record Retention \| Long-term Retrieval Capability | Monitoring, not fully compliant |
| 3.12.2 Audit Record Generation \| System-wide and Time-correlated Audit Trail | Monitoring, not fully compliant |
| 4.7.7 Continuous Monitoring \| Automation Support for Monitoring | Monitoring, not fully compliant |
| 5.5.2 Access Restrictions for Change \| Automated Access Enforcement and Audit Records | ✓ Enforces safe SSL protocol usage |
| 5.7.9 Least Functionality \| Binary or Machine Executable Code | Monitoring, not fully compliant |
| 6.9.6 System Backup \| Transfer to Alternate Storage Site | Monitoring, not fully compliant |
| 7.2.2 Identification and Authentication (organizational Users) \| Multi-factor Authentication to Privileged Accounts | Monitoring, not fully compliant |
| 7.2.3 Identification and Authentication (organizational Users) \| Multi-factor Authentication to Non-privileged Accounts | Monitoring, not fully compliant |
| 7.5.2 Authenticator Management \| Password-based Authentication | Monitoring, not fully compliant |
| 7.5.7 Authenticator Management \| Protection of Authenticators | Monitoring, not fully compliant |
| 7.10.1 Adaptive Authentication | Monitoring, not fully compliant |

| | |
|---|---|
| 8.5.2 Incident Monitoring \| Automated Tracking, Data Collection, and Analysis | Monitoring, not fully compliant |
| 13.12.1 Insider Threat Program | ✓ Enforces safe SSL protocol usage |
| 16.10.1 Threat Hunting | Monitoring, not fully compliant |
| 17.3.2 System Development Life Cycle \| Manage Preproduction Environment | ✓ Enforces safe SSL protocol usage<br>✓ Prevents abuse of cookies<br>✓ Uses up to date cryptography libraries |
| 18.5.2 Denial-of-service Protection \| Restrict Ability to Attack Other Systems | Monitoring, not fully compliant |
| 18.5.3 Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | ✓ Enforces safe SSL protocol usage |
| 18.7.6 Boundary Protection \| Deny by Default Allow by Exception | ✓ Enforces safe SSL protocol usage<br>✓ Prevents abuse of cookies |
| 18.7.8 Boundary Protection \| Split Tunneling for Remote Devices | Monitoring, not fully compliant |
| 18.7.11 Boundary Protection \| Prevent Exfiltration | ✓ Restrict excessive or unauthorized data mining queries.<br>✓ Enforces safe SSL protocol usage |
| 18.7.16 Boundary Protection \| Networked Privileged Accesses | Monitoring, not fully compliant |
| 18.12.2 Cryptographic Key Establishment and Management \| Availability | ✓ Enforces safe SSL protocol usage |
| 18.16.3 Transmission of Security and Privacy Attributes \| Anti-spoofing Mechanisms | Monitoring, not fully compliant |

| | |
|---|---|
| 18.16.4 Transmission of Security and Privacy Attributes \| Cryptographic Binding | ✓ Enforces safe SSL protocol usage |
| 18.20.3 Secure Name/address Resolution Service (authoritative Source) \| Data Origin and Integrity | Monitoring, not fully compliant |
| 18.21.2 Secure Name/address Resolution Service (recursive or Caching Resolver) \| Data Origin and Integrity | Monitoring, not fully compliant |
| 18.22.1 Architecture and Provisioning for Name/address Resolution Service | Monitoring, not fully compliant |
| 18.23.4 Session Authenticity \| Unique System-generated Session Identifiers | Monitoring, not fully compliant |
| 18.24.1 Fail in Known State | Monitoring, not fully compliant |
| 18.28.2 Protection of Information at Rest \| Cryptographic Protection | ✓ Enforces safe SSL protocol usage<br>✓ Prevents abuse of cookies |
| 18.34.2 Non-modifiable Executable Programs \| No Writable Storage | Monitoring, not fully compliant |

## PCI compliance

A brief overview of the PCI Data Security Standards and any measures taken for these.

| Title | Taken measures |
|---|---|
| 1.2 Network security controls (NSCs) are configured and maintained. | Monitoring, not fully compliant |
| 1.3 Network access to and from the cardholder data environment is restricted. | ✓ Enforces connections to use the latest SSL version<br>✓ Prevents abuse of cookies |
| 3.4 Access to displays of full PAN and ability to copy cardholder data are restricted. | Monitoring, not fully compliant |
| 3.5 Primary account number (PAN) is secured wherever it is stored. | Monitoring, not fully compliant |
| 4.2 PAN is protected with strong cryptography during transmission. | ✓ Enforces connections to use the latest SSL version<br>✓ Prevents abuse of cookies<br>✓ Enforces encryption of data in transit |
| 5.2 Malicious software (malware) is prevented, or detected and addressed. | ✓ No malware issues |
| 6.4 Public-facing web applications are protected against attacks. | ✓ Prevents remote code execution<br>✓ Prevents CSRF attacks<br>✓ Prevents Cross Site Scripting (XSS) |
| 7.2.2 Access is assigned to users, including privileged users. | Monitoring, not fully compliant |
| 7.2.5 All application and system accounts and related access privileges are assigned and managed. | Monitoring, not fully compliant |

| | |
|---|---|
| 7.3 Access to system components and data is managed via an access control system(s). | Monitoring, not fully compliant |
| 8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE. | Monitoring, not fully compliant |
| 10.2.1 Audit logs are enabled and active for all system components and cardholder data. | Monitoring, not fully compliant |
| 10.3.3 Audit log files are promptly backed up to a secure, central, internal log server(s). | Monitoring, not fully compliant |
| 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly. | Monitoring, not fully compliant |
| 11.3.2 External vulnerability scans are performed. | Monitoring, not fully compliant |
| 11.3.1 Internal vulnerability scans are performed. | ✓ Configured monitoring for code repositories<br>✓ Configured monitoring for container images |

## HIPAA compliance

A brief overview of the HIPAA Compliance Checklist and any measures taken for these.

| Title | Taken measures |
|---|---|
| 1.3.1 Security Standards: General Requirements | ✓ Enforces safe SSL protocol usage<br>✓ Prevents abuse of cookies<br>✓ Uses up to date cryptography libraries |
| 1.4.1 Administrative Safeguards: Security management process | Monitoring, not fully compliant |
| 1.4.4 Administrative Safeguards: Information access management | Monitoring, not fully compliant |
| 1.4.5 Administrative Safeguards: Security awareness and training | Monitoring, not fully compliant |
| 1.4.7 Administrative Safeguards: Contingency plan | Monitoring, not fully compliant |
| 1.6.1 Technical Safeguards: Access control | Monitoring, not fully compliant |
| 1.6.2 Technical Safeguards: Audit controls | Monitoring, not fully compliant |
| 1.6.3 Technical Safeguards: Integrity | ✓ Uses up to date cryptography libraries |
| 1.6.4 Technical Safeguards: Person or entity authentication | Monitoring, not fully compliant |
| 1.6.5 Technical Safeguards: Transmission Security | ✓ Uses up to date cryptography libraries<br>✓ Enforces safe SSL protocol usage<br>✓ Prevents abuse of cookies |

## HITRUST LVL3 Compliance

A brief overview of the HITRUST LVL3 framework and any measures taken for these.

| Title | Taken measures |
|---|---|
| 2.3 Privilege Management | Monitoring, not fully compliant |
| 2.4 User Password Management | ✓ Prevents Exposed Secrets |
| 2.9 User Authentication for External Connections | Monitoring, not fully compliant |
| 2.10 Equipment Identification in Networks | Monitoring, not fully compliant |
| 2.11 Remote Diagnostic and Configuration Port Protection | Monitoring, not fully compliant |
| 2.12 Segregation in Networks | Monitoring, not fully compliant |
| 2.13 Network Connection Control | ✓ Use of Cryptography: Enforces SSL |
| 2.14 Networking Routing Control | Monitoring, not fully compliant |
| 2.16 Secure Log-on Procedures | ✓ Use of Cryptography: Secure Cookies<br>✓ Use of Cryptography: Enforces SSL |
| 2.17 User Identification and Authentication | Monitoring, not fully compliant |
| 2.18 Password Management System | ✓ Prevents Exposed Secrets |
| 2.22 Information Access restriction | ✓ Prevents Remote Code Execution Attacks<br>✓ Prevents CSRF Attacks<br>✓ Prevents Cross-Site Scripting Attacks |
| 2.23 Sensitive System Isolation | Monitoring, not fully compliant |

| | |
|---|---|
| 7.3 Protection of Organizational Records | ✓ Prevents Exposed Secrets<br>✓ Prevent Root Access |
| 7.4 Data Protection and Privacy of Covered Information | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography: Secure Cookies<br>✓ Prevent Root Access |
| 7.6 Regulation of Cryptographic Controls | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography: Secure Cookies<br>✓ Use of Cryptography Libraries |
| 10.12 Back-up | Monitoring, not fully compliant |
| 10.13 Network Controls | Monitoring, not fully compliant |
| 10.17 Information Handling Procedures | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography: Secure Cookies<br>✓ Use of Cryptography Libraries |
| 10.18 Security of System Documentation | ✓ Configured Monitoring for Code Repositories |
| 10.19 Information Exchange Policies and Procedures | ✓ Use of Cryptography: Enforces SSL |
| 10.26 Publicly Available Information | Monitoring, not fully compliant |
| 10.27 Audit Logging | Monitoring, not fully compliant |
| 11.2 Input Data Validation | ✓ Cross-Site Scripting (XSS) Prevention<br>✓ Server-Side Request Forgery (SSRF) Prevention |
| 11.6 Policy on the Use of Cryptographic Controls | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography Libraries |
| 11.7 Key Management | ✓ Prevents Exposed Secrets |

| | |
|---|---|
| 11.8 Control of Operational Software | ✓ No Open End-of-Life (EOL) Issues<br>✓ No Open DAST Issues<br>✓ No Open OSS Security Issues<br>✓ Configured Monitoring for Code Repositories<br>✓ Configured Monitoring for Containers |
| 11.12 Outsourced Software Development | ✓ No Open SCM Security Issues |
| 11.13 Control of Technical Vulnerabilities | Monitoring, not fully compliant |

## GDPR compliance

A brief overview of GDPR rules and any measures taken for these.

| Title | Taken measures |
|---|---|
| 2.1 Principles Relating to Processing of Personal Data | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography: Secure Cookies<br>✓ Use of Cryptography Libraries |
| 4.2 Data Protection by Design | Monitoring, not fully compliant |
| 4.5 Processor | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography: Secure Cookies<br>✓ Use of Cryptography Libraries |
| 4.7 Records of Processing Activities | Monitoring, not fully compliant |
| 4.9 Security of Processing | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography: Secure Cookies<br>✓ Use of Cryptography Libraries |

## DORA compliance

A brief overview of the DORA Compliance Checklist and any measures taken for these.

| Title | Taken measures |
|---|---|
| Article 7, ICT Risk Management: Systems, Protocols, and Tools | Monitoring, not fully compliant |
| Article 8, ICT Risk Management: Identification | ✓ Has connected code repositories |
| Article 9, ICT Risk Management: Protection and prevention | ✓ Use of Cryptography: Enforces SSL<br>✓ Use of Cryptography: Secure Cookies |
| Article 10, ICT Risk Management: Detection | Monitoring, not fully compliant |
| Article 11, ICT Risk Management: Response and Recovery | Monitoring, not fully compliant |
| Article 12, ICT Risk Management: Backup | Monitoring, not fully compliant |
| Article 15, Harmonization With Other Regulations | Monitoring, not fully compliant |
| Article 17, Incident Management Process | Monitoring, not fully compliant |
| Article 18, Classification of Incidents and Cyber Threats | ✓ Configured monitoring for code repositories<br>✓ Configured monitoring for container images |

## Scan history report

This section details all company assets that are being monitored and how often scans are performed.

| Kind | Frequency | Last occurence |
|---|---|---|
| Open-source dependencies: | Daily | 2025-11-10 |
| OSS licenses: 0 monitored for compliance | Weekly | 2025-11-10 |
| Static app security testing: 1 repository monitored | Daily | 2025-11-10 |
| Infrastructure as code: monitored for misconfigurations | Daily | 2025-11-10 |
| Exposed secrets: history of 1 repository scanned | Daily | 2025-11-10 |

## Issue insights over the past 3 months

The table below gives an overview of new findings in a 3 month rolling window. A triaged finding is one that has been either been solved, ignored after analysis or planned in a task management system for resolution.

| Issue kind | New | False positives | Handled |
|---|---|---|---|
| Open-source Dependencies | 0 | 0 | 0 |
| Container Images | 0 | 0 | 0 |
| Cloud Configurations | 0 | 0 | 0 |
| Virtual Machines | 0 | 0 | 0 |
| Secrets in source code history | 0 | 0 | 0 |
| DAST/Surface Monitoring | 0 | 0 | 0 |
| SAST/Static App Security Testing | 2 | 0 | 0 |
| Infrastructure As Code | 0 | 0 | 0 |
| Mobile | 0 | 0 | 0 |
| End-of-life Runtimes | 0 | 0 | 0 |
| Access Controls | 0 | 0 | 0 |
| Licenses | 0 | 0 | 0 |
| Malware Issues | 0 | 0 | 0 |
| AI Pentest Issues | 0 | 0 | 0 |

## Open Issues Snapshot

The table below gives an overview of all findings that were open Nov 10th 2025.

| Issue type | Critical | High | Medium | Low |
|---|---|---|---|---|
| Open-source Dependencies | 0 | 0 | 0 | 0 |
| Container Images | 0 | 0 | 0 | 0 |
| Cloud Configurations | 0 | 0 | 0 | 0 |
| Virtual Machines | 0 | 0 | 0 | 0 |
| Secrets in source code history | 0 | 0 | 0 | 0 |
| DAST/Surface Monitoring | 0 | 0 | 0 | 0 |
| SAST/Static App Security Testing | 0 | 2 | 0 | 0 |
| Infrastructure As Code | 0 | 0 | 0 | 0 |
| Mobile | 0 | 0 | 0 | 0 |
| End-of-life Runtimes | 0 | 0 | 0 | 0 |
| Access Controls | 0 | 0 | 0 | 0 |
| Licenses | 0 | 0 | 0 | 0 |
| Malware Issues | 0 | 0 | 0 | 0 |
| AI Pentest Issues | 0 | 0 | 0 | 0 |