

# Fibbler: security audit report

Created on 04 December 2024 @ 08:18

---

Fibbler wants to build trust by giving you insight in how it builds software in a secure manner. The reports details how software development at Fibbler 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 Fibbler code and infrastructure.



## 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
A02:2021	Cryptographic failures	✓ Enforces encryption of data at rest ✓ Enforces the use of secure connections ✓ Prevents the exposure of secret keys
A03:2021	Injection	✓ App scanned for SQL injection attack ✓ Prevents remote code execution ✓ Prevents CSRF attacks ✓ Prevents Cross Site Scripting (XSS)
A04:2021	Insecure design	No active measures
A05:2021	Security misconfiguration	✓ Application is properly configured
A06:2021	Vulnerable and Outdated Components	No active measures
A07:2021	Identification and Authentication Failures	No active measures
A08:2021	Software and Data Integrity Failures	✓ Code repositories use lockfiles to pin dependencies ✓ Takes measures to ensure proper deserialization
A09:2021	Security Logging and Monitoring Failures	✓ Has email notifications set up
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	No active measures
A.8.3 - Information access restriction	No active measures
A.8.5 - Secure authentication	No active measures
A.8.6 - Capacity management	No active measures
A.8.7 - Protection against malware	✔ Uses Lockfiles to pin code dependencies
A.8.8 - Management of technical vulnerabilities	No active measures
A.8.12 - Data leakage prevention	✔ Encrypts data at rest ✔ Prevents remote code execution ✔ Has measures against SQL injection attacks ✔ Prevents XSS attacks
A.8.13 - Backups	No active measures
A.8.15 - Logging	No active measures
A.8.18 - Use of privileged utility programs	✔ Prevents the exposure of sensitive data
A.8.20 - Network security	No active measures
A.8.31 - Separation of development, test and production environments	No active measures
A.8.24 - Use of cryptography	✔ Uses secure cookies ✔ Uses up-to-date cryptographic libraries



A.8.9 - Configuration management	 Uses Lockfiles to pin code dependencies
A.8.16 - Monitoring activities	 Receives security alerts in real time
A.8.25 - Secure development lifecycle	 Has connected a code repository
A.8.28 - Secure coding	No active measures
A.8.32 - Change management	No active measures
A.5.15 - Access control	No active measures
A.5.16 - Identity management	No active measures
A.5.28 - Collection of evidence	No active measures
A.5.33 - Protection of records	No active measures

## 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	No active measures
CC3.2: Estimate Significance of Risks Identified	<ul style="list-style-type: none"><li>✓ Does not have any severe surface monitoring issues</li><li>✓ Does not have any severe open source dependency issues</li><li>✓ Configured monitoring for code repositories</li><li>✓ Configured monitoring for container images</li></ul>
CC5.2: The entity selects and develops general control activities over technology to support the achievement of objectives	<ul style="list-style-type: none"><li>✓ Does not have any severe infrastructure as code issues</li></ul>
CC6.1: Restricts logical access	<ul style="list-style-type: none"><li>✓ Encrypts data at rest</li><li>✓ Prevents the exposure of sensitive data</li><li>✓ Has measures against SQL injection attacks</li><li>✓ Is protected against SSRF attacks</li><li>✓ Is protected against command injections attacks</li><li>✓ Prevents XSS attacks</li></ul>
CC6.1: Consider network segmentation	No active measures
CC6.1: Restrict access to information assets	No active measures
CC6.1: Manages credentials for infrastructure and software	No active measures
CC6.1: Use encryption to protect data	<ul style="list-style-type: none"><li>✓ Enforces encryption of data in transit</li><li>✓ Uses up to date cryptography libraries</li></ul>
CC6.6: Restrict Access	No active measures



CC6.6: Require additional authentication or credentials	No active measures
CC6.6: Implement boundary protection system	No active measures
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	✓ Prevents container orchestration takeover
CC6.8: Detect unauthorized changes to software and configuration parameters	No active measures
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	No active measures
CC7.1: Detect unknown or unauthorized components	✓ Does not have risky licenses
CC7.1: Conduct vulnerability scans	✓ Uses Lockfiles to pin code dependencies ✓ 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	No active measures

CC8.1: Track system changes	No active measures
CC10.3: Tests integrity and completeness of backup data	No active measures



## CIS 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	No active measures
3.3 Configure Data Access Control Lists	No active measures
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	No active measures
4.4 Implement and Manage a Firewall on Servers	✔ Prevents unauthorized public access to file storage ✔ Enforces encryption of data in transit
4.6 Securely Manage Enterprise Assets and Software	✔ Enforces latest TLS version ✔ 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	No active measures
6.5 Require MFA for Administrative Access	No active measures
6.4 Require MFA for Remote Network Access	No active measures









7.1 Establish and Maintain a Vulnerability Management Process	No active measures
8.2 Collect Audit Logs	No active measures
10.1 Deploy and Maintain Anti-Malware Software	<ul style="list-style-type: none"> <li>✓ Uses Lockfiles to pin code dependencies</li> <li>✓ No malware issues</li> </ul>
11.2 Perform Automated Backups	<ul style="list-style-type: none"> <li>✓ Has backups for stateful cloud resources</li> </ul>
12.3 Securely Manage Network Infrastructure	<ul style="list-style-type: none"> <li>✓ Prevents unauthorized public access to networks and instances</li> </ul>
12.6 Use of Secure Network Management and Communication Protocols	<ul style="list-style-type: none"> <li>✓ Prevents unauthorized public access to networks and instances</li> <li>✓ Enforces encryption of data in transit</li> <li>✓ Uses secure communications protocols</li> </ul>
13.6 Collect Network Traffic Flow Logs	No active measures
16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities	No active measures
16.5 Use Up-to-Date and Trusted Third-Party Software Components	<ul style="list-style-type: none"> <li>✓ No risky licenses in 3rd party dependencies</li> </ul>
16.8 Separate Production and Non-Production Systems	No active measures
16.12 Implement Code-Level Security Checks	<ul style="list-style-type: none"> <li>✓ Configured monitoring for code repositories</li> </ul>

## 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	No active measures
Business continuity	No active measures
Supply chain security	 Uses Lockfiles to pin code dependencies
Security in network and information systems acquisition	No active measures
Policies and procedures regarding the use of cryptography	 Uses secure cookies  Uses up-to-date cryptographic libraries
Access control policies and asset management	No active measures
The use of multi-factor authentication	No active measures

## 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.	No active measures
1.3 Network access to and from the cardholder data environment is restricted.	<ul style="list-style-type: none"><li>✓ Enforces connections to use the latest SSL version</li><li>✓ Prevents abuse of cookies</li></ul>
3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.	No active measures
3.5 Primary account number (PAN) is secured wherever it is stored.	No active measures
4.2 PAN is protected with strong cryptography during transmission.	<ul style="list-style-type: none"><li>✓ Enforces connections to use the latest SSL version</li><li>✓ Prevents abuse of cookies</li><li>✓ Enforces encryption of data in transit</li></ul>
5.2 Malicious software (malware) is prevented, or detected and addressed.	<ul style="list-style-type: none"><li>✓ No malware issues</li></ul>
6.4 Public-facing web applications are protected against attacks.	<ul style="list-style-type: none"><li>✓ App scanned for SQL injection attack</li><li>✓ Prevents remote code execution</li><li>✓ Prevents CSRF attacks</li><li>✓ Prevents Cross Site Scripting (XSS)</li></ul>
7.2.2 Access is assigned to users, including privileged users.	No active measures
7.2.5 All application and system accounts and related access privileges are assigned and managed.	No active measures



7.3 Access to system components and data is managed via an access control system(s).	No active measures
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	No active measures
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	No active measures
10.3.3 Audit log files are promptly backed up to a secure, central, internal log server(s).	No active measures
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly.	 Receives security alerts in real time
11.3.2 External vulnerability scans are performed.	No active measures
11.3.1 Internal vulnerability scans are performed.	 Configured monitoring for code repositories  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	<ul style="list-style-type: none"><li>✔ Enforces safe SSL protocol usage</li><li>✔ Prevents abuse of cookies</li><li>✔ Uses up to date cryptography libraries</li></ul>
1.4.1 Administrative Safeguards: Security management process	No active measures
1.4.4 Administrative Safeguards: Information access management	No active measures
1.4.5 Administrative Safeguards: Security awareness and training	No active measures
1.4.7 Administrative Safeguards: Contingency plan	No active measures
1.6.1 Technical Safeguards: Access control	No active measures
1.6.2 Technical Safeguards: Audit controls	No active measures
1.6.3 Technical Safeguards: Integrity	<ul style="list-style-type: none"><li>✔ Uses up to date cryptography libraries</li></ul>
1.6.4 Technical Safeguards: Person or entity authentication	No active measures
1.6.5 Technical Safeguards: Transmission Security	<ul style="list-style-type: none"><li>✔ Uses up to date cryptography libraries</li><li>✔ Enforces safe SSL protocol usage</li><li>✔ Prevents abuse of cookies</li></ul>



## HITRUST LVL3 Compliance

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

Title	Taken measures
2.3 Privilege Management	No active measures
2.4 User Password Management	✔ Prevents Exposed Secrets
2.9 User Authentication for External Connections	No active measures
2.10 Equipment Identification in Networks	No active measures
2.11 Remote Diagnostic and Configuration Port Protection	No active measures
2.12 Segregation in Networks	No active measures
2.13 Network Connection Control	✔ Use of Cryptography: Enforces SSL
2.14 Networking Routing Control	No active measures
2.16 Secure Log-on Procedures	✔ Use of Cryptography: Secure Cookies ✔ Use of Cryptography: Enforces SSL
2.17 User Identification and Authentication	No active measures
2.18 Password Management System	✔ Prevents Exposed Secrets
2.22 Information Access restriction	✔ Prevents SQL Injection Attacks ✔ Prevents Remote Code Execution Attacks ✔ Prevents CSRF Attacks ✔ Prevents Cross-Site Scripting Attacks



2.23 Sensitive System Isolation	No active measures
7.3 Protection of Organizational Records	<ul style="list-style-type: none"> <li>✔ Prevents Exposed Secrets</li> <li>✔ Prevents SQL Injection Attacks</li> </ul>
7.4 Data Protection and Privacy of Covered Information	<ul style="list-style-type: none"> <li>✔ Use of Cryptography: Enforces SSL</li> <li>✔ Use of Cryptography: Secure Cookies</li> <li>✔ Prevents SQL Injection Attacks</li> </ul>
7.6 Regulation of Cryptographic Controls	<ul style="list-style-type: none"> <li>✔ Use of Cryptography: Enforces SSL</li> <li>✔ Use of Cryptography: Secure Cookies</li> <li>✔ Use of Cryptography Libraries</li> </ul>
10.12 Back-up	No active measures
10.13 Network Controls	No active measures
10.17 Information Handling Procedures	<ul style="list-style-type: none"> <li>✔ Use of Cryptography: Enforces SSL</li> <li>✔ Use of Cryptography: Secure Cookies</li> <li>✔ Use of Cryptography Libraries</li> </ul>
10.18 Security of System Documentation	<ul style="list-style-type: none"> <li>✔ Configured Monitoring for Code Repositories</li> </ul>
10.19 Information Exchange Policies and Procedures	<ul style="list-style-type: none"> <li>✔ Use of Cryptography: Enforces SSL</li> </ul>
10.26 Publicly Available Information	No active measures
10.27 Audit Logging	No active measures
11.2 Input Data Validation	<ul style="list-style-type: none"> <li>✔ Prevents SQL Injection Attacks</li> <li>✔ Cross-Site Scripting (XSS) Prevention</li> <li>✔ Server-Side Request Forgery (SSRF) Prevention</li> </ul>
11.6 Policy on the Use of Cryptographic Controls	<ul style="list-style-type: none"> <li>✔ Use of Cryptography: Enforces SSL</li> <li>✔ Use of Cryptography Libraries</li> </ul>

11.7 Key Management	<ul style="list-style-type: none"> <li>✔ Prevents Exposed Secrets</li> </ul>
11.8 Control of Operational Software	<ul style="list-style-type: none"> <li>✔ No Open End-of-Life (EOL) Issues</li> <li>✔ No Open DAST Issues</li> <li>✔ No Open OSS Security Issues</li> <li>✔ Configured Monitoring for Code Repositories</li> <li>✔ Configured Monitoring for Containers</li> </ul>
11.12 Outsourced Software Development	<ul style="list-style-type: none"> <li>✔ No Open SCM Security Issues</li> </ul>
11.13 Control of Technical Vulnerabilities	No active measures



## 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	<ul style="list-style-type: none"><li>✔ Use of Cryptography: Enforces SSL</li><li>✔ Use of Cryptography: Secure Cookies</li><li>✔ Use of Cryptography Libraries</li></ul>
4.2 Data Protection by Design	No active measures
4.5 Processor	<ul style="list-style-type: none"><li>✔ Use of Cryptography: Enforces SSL</li><li>✔ Use of Cryptography: Secure Cookies</li><li>✔ Use of Cryptography Libraries</li></ul>
4.7 Records of Processing Activities	No active measures
4.9 Security of Processing	<ul style="list-style-type: none"><li>✔ Use of Cryptography: Enforces SSL</li><li>✔ Use of Cryptography: Secure Cookies</li><li>✔ Use of Cryptography Libraries</li></ul>

