Kyroo: security audit report

Created on 11 May 2026 @ 16:52 Kyroo

Kyroo wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at Kyroo 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 Kyroo 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	✓ Principle of least privilege applied for cloud users ✓ Restricted geo-location access to resources ✓ Application is properly configured ✓ Prevents unauthorized access to resources
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) ✓ Prevents command injection
A04:2021	Insecure design	✓ Configured monitoring for code repositories
A05:2021	Security misconfiguration	✓ Cloud environments are properly configured ✓ Application is properly configured
A06:2021	Vulnerable and Outdated Components	Monitoring, not fully compliant
A07:2021	Identification and Authentication Failures	✓ Prevents bypassing authorization controls ✓ Prevents improper certificate validation ✓ Restricts public access to sensitive cloud resources
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	Monitoring, not fully compliant
A.8.3 - Information access restriction	✓ Prevents public access to cloud resources ✓ Has proper access controls for cloud resources
A.8.5 - Secure authentication	✓ Enforces encryption of data in transit
A.8.6 - Capacity management	Monitoring, not fully compliant
A.8.7 - Protection against malware	✓ Prevents unwanted write operations to filesystems ✓ Uses Lockfiles to pin code dependencies
A.8.8 - Management of technical vulnerabilities	Monitoring, not fully compliant
A.8.12 - Data leakage prevention	✓ Securely stores files ✓ Enforces encryption of data in transit ✓ Encrypts data at rest ✓ Prevents remote code execution ✓ Is protected against SSRF attacks ✓ Has measures against SQL injection attacks ✓ 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	✓ Has separate production and test environments

A.8.24 - Use of cryptography	✓ Enforces safe SSL protocol usage ✓ 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	✓ Has connected a cloud environment ✓ Receives security alerts in real time
A.8.25 - Secure development lifecycle	✓ Has connected a code repository ✓ Has connected a cloud environment
A.8.28 - Secure coding	Monitoring, not fully compliant
A.8.32 - Change management	Monitoring, not fully compliant
A.5.15 - Access control	✓ Applies the least privilege principle for cloud users ✓ Applies the least privilege principle to cloud resources ✓ Prevents the exposure of sensitive data
A.5.16 - Identity management	✓ Properly manages the identity of cloud users
A.5.28 - Collection of evidence	Monitoring, not fully compliant
A.5.33 - Protection of records	✓ Prevents public access to cloud resources

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	✓ Applies the least privilege principle to cloud resources
CC3.2: Estimate Significance of Risks Identified	✓ Properly manages the identity of cloud users ✓ Does not have any severe surface monitoring issues ✓ Does not have any severe open source dependency issues ✓ Configured monitoring for code repositories ✓ Configured monitoring for container images
CC5.2: The entity selects and develops general control activities over technology to support the achievement of objectives	✓ Properly manages the identity of cloud users ✓ Does not have any severe infrastructure as code issues
CC6.1: Restricts logical access	✓ Applies the least privilege principle to cloud resources ✓ Enforces encryption of data in transit ✓ Encrypts data at rest ✓ Prevents the exposure of sensitive data ✓ Has measures against SQL injection attacks ✓ Is protected against SSRF attacks ✓ Is protected against command injections attacks ✓ Prevents XSS attacks
CC6.1: Consider network segmentation	✓ Prevents unauthorized public access to file storage ✓ Prevents unauthorized public access to database ✓ Prevents unauthorized access via ssh ✓ Has separate production and test environments
CC6.1: Restrict access to information assets	✓ Has secured load balancer access points
CC6.1: Manages credentials for infrastructure and software	Monitoring, not fully compliant

CC6.1: Use encryption to protect data	✓ Encrypts data at rest ✓ Enforces encryption of data in transit ✓ Uses up to date cryptography libraries
CC6.6: Restrict Access	✓ Prevents public access to cloud resources
CC6.6: Require additional authentication or credentials	Monitoring, not fully compliant
CC6.6: Implement boundary protection system	✓ Applies the least privilege principle for cloud resource
CC6.7: Use encryption technologies or secure communication channels to protect data	✓ Enforces latest TLS version ✓ Uses up to date cryptography libraries
CC6.8: Restrict application and software installation	✓ Protects unauthorized runtime access ✓ Prevents container orchestration takeover
CC6.8: Detect unauthorized changes to software and configuration parameters	✓ Enabled security logging for cloud instances
CC6.8 Use anti-virus and anti-malware software	✓ Aikido Malware Scanner is enabled
CC7.1: Monitor infrastructure and software	✓ Enabled security logging for cloud instances ✓ Connected code repositories ✓ Connected cloud environment
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	✓ 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	✓ Runtimes are up to date ✓ 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	✓ Has backups for stateful cloud resources

UK Cyber Essentials compliance

A brief overview of the UK Cyber Essentials requirements and any measures taken for these.

Title	Taken measures
1.1 Ensure that only safe and necessary network services can be accessed from the internet	✓ Prevents public access to file storage ✓ Prevents public access to databases ✓ Prevents public access to network resources ✓ Thread detection logging enabled
2.1 Ensure that computers and network devices are properly configured to reduce the level of inherent vulnerabilities	✓ Proper access management for resources ✓ Encryption at rest enabled ✓ Enforces Proper SSL usage ✓ Enforces Proper TLS usage ✓ Prevents abuse of cookies ✓ Uses up to date cryptography libraries
3.1 Ensure user accounts are assigned to authorised individuals only and provide access to the minimum necessary services	✓ Properly verifies the identity of cloud users ✓ Protects runtime access to cloud resources
4.1 Ensure that known malware and untrusted software are not executed	✓ No malware issues ✓ Uses lockfiles
5.1 Ensure that devices and software are not vulnerable to known security issues for which fixes are available	✓ Runtimes are up to date ✓ Uses up to date cryptography libraries

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	✓ Encrypts data at rest ✓ Enforces safe SSL protocol usage ✓ Enforces latest TLS version ✓ Prevents abuse of cookies ✓ Uses up to date cryptography libraries
1.4.1 Administrative Safeguards: Security management process	✓ Enabled security logging for cloud instances
1.4.4 Administrative Safeguards: Information access management	✓ Applies the least privilege principle for cloud users ✓ Applies the least privilege principle for cloud resource ✓ Applies the least privilege principle to cloud resources
1.4.5 Administrative Safeguards: Security awareness and training	✓ Enabled security logging for cloud instances
1.4.7 Administrative Safeguards: Contingency plan	✓ Has backups for stateful cloud resources
1.6.1 Technical Safeguards: Access control	✓ Applies the least privilege principle for cloud users ✓ Applies the least privilege principle for cloud resource ✓ Applies the least privilege principle to cloud resources
1.6.2 Technical Safeguards: Audit controls	✓ Enabled security logging for cloud instances
1.6.3 Technical Safeguards: Integrity	✓ Encrypts data at rest ✓ Applies the least privilege principle to cloud resources ✓ Uses up to date cryptography libraries
1.6.4 Technical Safeguards: Person or entity authentication	✓ Applies the least privilege principle for cloud resource ✓ Applies the least privilege principle to cloud resources ✓ Applies the least privilege principle for cloud users

1.6.5 Technical Safeguards: Transmission Security	✓ Encrypts data at rest ✓ Uses up to date cryptography libraries ✓ Enforces safe SSL protocol usage ✓ Enforces latest TLS version ✓ Prevents abuse of cookies

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	✓ Encryption at Rest Enabled ✓ Use of Cryptography: Enforces SSL ✓ Use of Cryptography: Enforces TLS ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries ✓ Runtimes are up to date
4.2 Data Protection by Design	✓ Proper Access Management for Users ✓ Proper Access Management for Resources ✓ Proper Access Management to Resources
4.5 Processor	✓ Encryption at Rest Enabled ✓ Use of Cryptography: Enforces SSL ✓ Use of Cryptography: Enforces TLS ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries ✓ Runtimes are up to date
4.7 Records of Processing Activities	✓ Logging Enabled ✓ Backups Enabled
4.9 Security of Processing	✓ Encryption at Rest Enabled ✓ Use of Cryptography: Enforces SSL ✓ Use of Cryptography: Enforces TLS ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries

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	2026-05-11
OSS licenses: 0 monitored for compliance	Weekly	2026-05-11
Static app security testing: 0 repositories monitored	Daily	2026-05-11
Infrastructure as code: monitored for misconfigurations	Daily	2026-05-11
Exposed secrets: history of 0 repositories scanned	Daily	2026-05-11