

RoleDream: security audit report

Created on 14 February 2026 @ 08:24

RoleDream wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at RoleDream 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 RoleDream 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	<ul style="list-style-type: none">✓ Principle of least privilege applied for cloud users✓ Principle of least privilege applied for cloud resources✓ Restricted geo-location access to resources✓ Application is properly configured✓ Prevents unauthorized access to resources
A02:2021	Cryptographic failures	<ul style="list-style-type: none">✓ Enforces encryption of data at rest✓ Enforces the use of secure connections✓ Prevents the exposure of secret keys
A03:2021	Injection	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ Configured monitoring for code repositories
A05:2021	Security misconfiguration	<ul style="list-style-type: none">✓ Cloud environments are properly configured✓ Application is properly configured
A06:2021	Vulnerable and Outdated Components	<ul style="list-style-type: none">✓ No issues have been open longer than their configured SLA✓ Principle of least privilege applied for cloud users
A07:2021	Identification and Authentication Failures	<ul style="list-style-type: none">✓ Enforces MFA for cloud users✓ Prevents bypassing authorization controls✓ Prevents improper certificate validation✓ Restricts public access to sensitive cloud resources



A08:2021	Software and Data Integrity Failures	<ul style="list-style-type: none">✓ Code repositories use lockfiles to pin dependencies✓ Takes measures to ensure proper deserialization
A09:2021	Security Logging and Monitoring Failures	<ul style="list-style-type: none">✓ Has email notifications set up
A10:2021	Server-Side Request Forgery	<ul style="list-style-type: none">✓ App scanned for SSRF attack opportunities

SLA compliance report

The table below shows the configured SLAs and pinpoints instances shows the amount of issues that do currently do not meet these standards.

Issue priority level	SLA	# Issues too late
Critical	5 days	0
High	20 days	0
Medium	60 days	0
Low	100 days	0

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	<ul style="list-style-type: none">✔ Has checks in place for enforcing permissions
A.8.3 - Information access restriction	<ul style="list-style-type: none">✔ Prevents public access to cloud resources✔ Has proper access controls for cloud resources
A.8.5 - Secure authentication	<ul style="list-style-type: none">✔ Requires MFA for cloud users✔ Enforces encryption of data in transit
A.8.6 - Capacity management	<ul style="list-style-type: none">✔ Has budgeting alerts set up✔ Uses load balancers correctly
A.8.7 - Protection against malware	<ul style="list-style-type: none">✔ Prevents unwanted write operations to filesystems✔ Has enabled threat detection✔ Uses Lockfiles to pin code dependencies
A.8.8 - Management of technical vulnerabilities	<ul style="list-style-type: none">✔ Does not have any issues outside of their SLA
A.8.12 - Data leakage prevention	<ul style="list-style-type: none">✔ Securely stores files✔ Enforces encryption of data in transit✔ Prevents remote code execution✔ Is protected against SSRF attacks✔ Has measures against SQL injection attacks✔ Prevents XSS attacks
A.8.13 - Backups	<ul style="list-style-type: none">✔ Has backups for stateful cloud resources✔ Has cross account backups enabled
A.8.15 - Logging	<ul style="list-style-type: none">✔ Enabled security logging for cloud instances



A.8.18 - Use of privileged utility programs	<ul style="list-style-type: none"> ✔ Enforces secure access for cloud users ✔ Prevents the exposure of sensitive data ✔ Requires MFA for cloud users ✔ Has proper access controls for cloud resources
A.8.20 - Network security	<ul style="list-style-type: none"> ✔ Prevents unauthorized network access
A.8.31 - Separation of development, test and production environments	<ul style="list-style-type: none"> ✔ Has separate production and test environments
A.8.24 - Use of cryptography	<ul style="list-style-type: none"> ✔ Enforces safe SSL protocol usage ✔ Uses secure cookies ✔ Uses up-to-date cryptographic libraries
A.8.9 - Configuration management	<ul style="list-style-type: none"> ✔ Runs cloud instances on up-to-date versions ✔ Uses Lockfiles to pin code dependencies
A.8.16 - Monitoring activities	<ul style="list-style-type: none"> ✔ Has connected a cloud environment ✔ Receives security alerts in real time ✔ Has enabled threat detection
A.8.25 - Secure development lifecycle	<ul style="list-style-type: none"> ✔ Uses a CI integration ✔ Has connected a code repository ✔ Has connected a cloud environment
A.8.28 - Secure coding	<ul style="list-style-type: none"> ✔ Does not have any issues outside of their SLA
A.8.32 - Change management	Monitoring, not fully compliant
A.5.15 - Access control	<ul style="list-style-type: none"> ✔ Applies the least privilege principle for cloud users ✔ Applies the least privilege principle for cloud resource ✔ Applies the least privilege principle to cloud resources ✔ Prevents the exposure of sensitive data
A.5.16 - Identity management	<ul style="list-style-type: none"> ✔ Properly manages the identity of cloud users

A.5.28 - Collection of evidence	<ul style="list-style-type: none">✔ Has budgeting alerts set up✔ Enabled security logging for cloud instances✔ Has enabled threat detection
A.5.33 - Protection of records	<ul style="list-style-type: none">✔ Prevents public access to cloud resources✔ Encrypts data at rest



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	<ul style="list-style-type: none">✔ Applies the least privilege principle for cloud resource✔ Requires MFA for cloud users✔ Applies the least privilege principle to cloud resources✔ Enabled security logging for cloud instances✔ Threat detection is enabled
CC3.2: Estimate Significance of Risks Identified	<ul style="list-style-type: none">✔ Properly manages the identity of cloud users✔ Threat detection is enabled✔ 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✔ Configured monitoring for domains
CC5.2: The entity selects and develops general control activities over technology to support the achievement of objectives	<ul style="list-style-type: none">✔ Applies the least privilege principle for cloud resource✔ Has deletion protection for cloud resources✔ Properly manages the identity of cloud users✔ Does not have any severe infrastructure as code issues
CC6.1: Restricts logical access	<ul style="list-style-type: none">✔ Requires MFA for cloud users✔ Applies the least privilege principle to cloud resources✔ Threat detection is enabled✔ Enforces encryption of data in transit✔ 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	<ul style="list-style-type: none"> ✔ 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	<ul style="list-style-type: none"> ✔ Has secured load balancer access points
CC6.1: Manages credentials for infrastructure and software	<ul style="list-style-type: none"> ✔ Has secured load balancer access points
CC6.1: Use encryption to protect data	<ul style="list-style-type: none"> ✔ Encrypts data at rest ✔ Enforces encryption of data in transit ✔ Uses up to date cryptography libraries
CC6.6: Restrict Access	<ul style="list-style-type: none"> ✔ Prevents public access to cloud resources
CC6.6: Require additional authentication or credentials	<ul style="list-style-type: none"> ✔ MFA is enforced for cloud users
CC6.6: Implement boundary protection system	<ul style="list-style-type: none"> ✔ DNS Domain transfer is locked ✔ Applies the least privilege principle for cloud resource
CC6.7: Use encryption technologies or secure communication channels to protect data	<ul style="list-style-type: none"> ✔ Enforces latest TLS version ✔ Uses up to date cryptography libraries
CC6.8: Restrict application and software installation	<ul style="list-style-type: none"> ✔ Protects unauthorized runtime access ✔ Prevents container orchestration takeover
CC6.8: Detect unauthorized changes to software and configuration parameters	<ul style="list-style-type: none"> ✔ Enabled security logging for cloud instances
CC6.8 Use anti-virus and anti-malware software	<ul style="list-style-type: none"> ✔ Threat detection is enabled ✔ Aikido Malware Scanner is enabled

CC7.1: Monitor infrastructure and software	<ul style="list-style-type: none"> ✔ Enabled security logging for cloud instances ✔ Configured SLAs to resolve issues ✔ Connected code repositories ✔ Connected cloud environment ✔ Connected public facing domain
CC7.1: Implement change detection mechanism	<ul style="list-style-type: none"> ✔ Alerting is enabled
CC7.1: Detect unknown or unauthorized components	<ul style="list-style-type: none"> ✔ Does not have risky licenses
CC7.1: Conduct vulnerability scans	<ul style="list-style-type: none"> ✔ Uses Lockfiles to pin code dependencies ✔ Does not have any issues outside of their SLA ✔ Connected code repositories ✔ Connected public facing domain
CC7.1: Implement filters to analyze anomalies	<ul style="list-style-type: none"> ✔ Connected code repositories ✔ Threat detection is enabled
CC7.1: Restores the affected environments	<ul style="list-style-type: none"> ✔ Runtimes are up to date ✔ Has no critical open source dependency issues
CC8.1: Protect confidential information	<ul style="list-style-type: none"> ✔ Prevents the exposure of sensitive data
CC8.1: Track system changes	Monitoring, not fully compliant
CC10.3: Tests integrity and completeness of backup data	<ul style="list-style-type: none"> ✔ Has backups for stateful cloud resources

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">✓ 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	<ul style="list-style-type: none">✓ Enabled security logging for cloud instances✓ Has enabled threat detection✓ Configured SLAs to resolve issues
1.4.4 Administrative Safeguards: Information access management	<ul style="list-style-type: none">✓ Requires MFA for access to cloud resources✓ Applies the least privilege principle for cloud resource✓ Applies the least privilege principle for cloud users✓ Applies the least privilege principle to cloud resources
1.4.5 Administrative Safeguards: Security awareness and training	<ul style="list-style-type: none">✓ Enabled security logging for cloud instances✓ Has enabled threat detection
1.4.7 Administrative Safeguards: Contingency plan	<ul style="list-style-type: none">✓ Has backups for stateful cloud resources✓ Has cross account backups enabled
1.6.1 Technical Safeguards: Access control	<ul style="list-style-type: none">✓ Requires MFA for access to cloud resources✓ Applies the least privilege principle for cloud resource✓ Applies the least privilege principle for cloud users✓ Applies the least privilege principle to cloud resources
1.6.2 Technical Safeguards: Audit controls	<ul style="list-style-type: none">✓ Enabled security logging for cloud instances✓ Has enabled threat detection



1.6.3 Technical Safeguards: Integrity	<ul style="list-style-type: none">✔ 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	<ul style="list-style-type: none">✔ Applies the least privilege principle for cloud resource✔ Requires MFA for access to cloud resources✔ Applies the least privilege principle to cloud resources✔ Applies the least privilege principle for cloud users
1.6.5 Technical Safeguards: Transmission Security	<ul style="list-style-type: none">✔ 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	<ul style="list-style-type: none">✔ 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	<ul style="list-style-type: none">✔ Enforces Multi-Factor Authentication (MFA)✔ Proper Access Management for Resources✔ Proper Access Management for Users✔ Proper Access Management to Resources
4.5 Processor	<ul style="list-style-type: none">✔ 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	<ul style="list-style-type: none">✔ Logging Enabled✔ Threat Detection Enabled✔ Backups Enabled
4.9 Security of Processing	<ul style="list-style-type: none">✔ Encryption at Rest Enabled✔ Use of Cryptography: Enforces SSL✔ Use of Cryptography: Enforces TLS✔ Use of Cryptography: Secure Cookies✔ Use of Cryptography Libraries

