Security Framework

Highlights

SysAid®

SysAid®

Contents

Objective

The purpose of this document is to detail SysAid security framework for external usages.

Introduction

At SysAid, data security, scalability and performance are our main priorities. Our state-of-the-art real-time infrastructure, advanced security and data protection, independent certifications and global regulatory compliance have earned the trust of the world's leading brands. We strive to implement the highest-level of security processes and practices across all business units.

To help ensure we attain this goal, our staff includes a Chief Information Security Officer (CISO) and a growing dedicated security team.

Our security practices are based on industry-leading standards such as ISO 27001:2013, ISO 27017:2015 and ISO 27018:2019, on which we are audited annually.

Our security framework includes policies and procedures that cover asset management, access management, physical security, people security, product security, cloud and network infrastructure security, third-party security, vulnerability management, security monitoring, and incident response.

All Information security policies and standards are annually reviewed and approved by SysAid management and are made available to all SysAid employees.

Security Team

SysAid's business operation team includes top-notch security and privacy professionals who are experts in information, application, and network security. The team's responsibilities are to:

- Maintain and improve the company's security defense systems
- Develop security review processes
- Build security infrastructure
- Implement SysAid's security policies and procedures

SysAid's dedicated security team actively scans for security threats using commercial and custom tools, conduct annual penetration tests, quality assurance (QA) measures, and software security reviews.

Members of the SysAid information security team review security plans for networks, systems and services. They provide project-specific consulting services to SysAid's product and engineering teams. They monitor for suspicious activity on SysAid's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments

Security Awareness

New employees go through an on-boarding process that includes security and privacy guidelines, expectations, and code of conduct. All SysAid employees undergo an annual security awareness training.

Phishing simulations are conducted periodically to measure the effectiveness of the security awareness program.

Hiring

The SysAid screening process is based on background checks and personal interviews with recruitment/HR managers and hiring managers. Where applicable, additional background checks are included based on local law. All employees sign a Non-Disclosure Agreement.

Communication

The SysAid security team communicates with all employees on a regular basis, covering topics such as emerging threats, phishing awareness campaigns, and other industry-related security topics.

Application Security

SysAid substantial business is based on a SaaS (Software as a Service). The center core of this service is SysAid's web application.

Secure Development

The SysAid secure software development lifecycle (S-SDLC) standard helps ensure the delivery of a highly secure platform. SysAid implements testing for security vulnerabilities on a regular basis both in-house and by independent security assessment service providers. All products and features undergo thorough security reviews and code scanning.

SysAid follows the OWASP methodology (see https://owasp.org/) for secure development. SysAid conducts routine dedicated training sessions for all its developers based on OWASP.

Change Management

SysAid follows a strict change management process. Changes are measured, reviewed, and approved to ensure operational changes are aligned with SysAid's business objectives and compliance requirements. All changes are tracked, reviewed and approved to ensure alignment with our business objectives and compliance requirements.

Penetration Tests (PTs)

SysAid conducts a variety of PTs as well as vulnerability scans using manual and automated tools on a regular basis both in-house and by independent security assessment service providers. These security assessment are part of SysAid's annual security framework SysAid's security calendar.

Data

SysAid isolates each customer's account data from other customers and users and encrypts the data at rest. Our web servers support strong encryption protocols to secure connections between customer devices and SysAid's web services and APIs.

Accounts Authentication Security

SysAid provides the most thorough authentication security measures in the ITSM industry. Among the available authentication capabilities, many settings are fully configurable to suit individual organizational standards and needs.

Full complexity passwords

All users must create full complexity passwords, which include a minimum of 8 characters, Uppercase and lowercase letters, numbers and symbols.

Temporary passwords

SysAid requires new users to create a new password immediately after signing in with a temporary password.

Password Hashing

Customer passwords are not stored in clear text in SysAid's servers. SysAid uses SHA-2 hash standard for storing all passwords

Failed logins

SysAid application blocks users after failed, unsuccessful login attempts. Customers can determine the duration of the lockout.

2-Factor Authentication

Customers can integrate with their 2FA when users log in. Available options are Google Authenticator or text message confirmation.

Single sign-on (SSO)

Customers using an IDP solution within their organization can connect and integrate it to the SysAid application. SysAid supports the SAML 2.0 standard for SSO.

Encryption

Data at Rest

Data is encrypted in our databases using AES256bit encryption by default.

Data in Transit

Data is vulnerable to unauthorized access as it travels across the internet or within networks. For this reason, securing data in transit is a high priority for SysAid. Our web servers support strong

encryption protocols to secure connections between customer devices and SysAid ‘s web services and APIs. Any traffic transferred to SysAid encrypted over https using TLS1.2 only.

Monitoring and visibility

SysAid utilizes a wide range of tools to monitor its environment across data centers on both the server and application levels. Parameters are collected and aggregated at a central location using redundancy to detect anomalies, trends, threshold crossing, etc.

SysAid security team continuously monitors and assesses compliance, regulations and risks.

Our vulnerability tests procedure establish how we identify, respond, and triage vulnerabilities against the SysAid platform.

To ensure the security of our platform, SysAid continues to improve and enhance its security capabilities: Continuous 24/7/365 monitoring and the implementation of a variety of security tools and other components to detect and mitigate any new vulnerabilities, incidents, and threats.

Cloud Security

SysAid entire production infrastructure and application is solely base on AWS which is the global leading cloud services provider.

Threats Detection

SysAid run an AWS threats detection service that continuously monitors for malicious activity and unauthorized behavior to protect SysAid’s AWS accounts, workloads, and data stored in AWS.

Asset Management

All SysAid assets are assigned with a defined owner. Access to production infrastructure is limited to the minimal number of individuals based on the principle of least privilege (PoLP) and need-to-know/work basis.

DDoS Protection

As part of the multilayered-protection approach, a dedicated DDoS mitigation ecosystem has been put in place. SysAid utilizes Anti DDoS protection, WAF and API protection tools.

Redundancy

SysAid utilizes a wide range of tools to monitor its environment across data centers on both the server and application level. Parameters are collected and aggregated at a central location using redundancy to detect anomalies, trends, threshold crossing, etc.

Physical Security

SysAid datacenters are fully based on Amazon Web Services (AWS). In alignment with ISO/IEC 27001:2013 standard, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Cloud Security Whitepaper for additional details - available at: http://aws.amazon.com/security