Security Overview

Introduction

Khoros takes Information Security and Compliance very seriously. This document is designed to help our customers ensure that their data is handled in a manner that meets their data protection and compliance requirements and to provide full transparency and a peace of mind for Khoros customers that their information is in good hands.

Our security controls and mechanisms are based on the ISO 27001 Information Security Standard and NIST Standards, which includes programs covering - Policies and Procedures, Asset Management, Access Management, Operations Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, as well as Security Monitoring and Incident Response.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com

Security Overview

Compliance

Khoros is continually evaluating security standards and certifications to determine which are most appropriate and add the most value for our customer base. Currently we are ISO27001 certified and conduct annual SOC 2 audits.

Annual SSAE 16 SOC 2 Audits

Khoros conducts annual SSAE 16 SOC 2 audits using independent external auditors and has conducted this rigorous assessment for many years. Customers and prospects who have signed nondisclosure agreements may request a copy of our most recent audit report by contacting security@khoros.com or through your Technical Account Manager.

ISO 27001 Certification

Khoros (Lithium) is ISO 27001:2013 certified, which is a global standard based on information security controls and management best practices. Certifying to the ISO 27001 standard involves a rigorous three-stage assessment conducted by independent auditors. Subsequent annual onsite audits are required to maintain the certification. Access Khoros (Lithium) ISO 27001 certification status here.

GDPR and CCPA

Khoros fully welcomes GDPR and CCPA and is here to help our customers address the GDPR and CCPA compliance through our robust privacy and security protections. We appreciate that the GDPR and CCPA requires our customers, as data controllers, to engage data processors that deploy appropriate safeguards. We can confirm that Khoros is GDPR and CCPA compliant after evaluating our controls, policies, and processes. Khoros fully appreciates and recognizes the importance of GDPR and CCPA to our customers in the delivery of our services to them. For the list of our sub processors, please visit https://khoros.com/khoros-subprocessors

Privacy Certifications

Khoros participates in the TRUSTe Enterprise Privacy & Data Governance Practices Certification program. This program is designed to help businesses implement strong privacy management practices consistent with a wide range of global regulations and industry standards. Access Khoros TRUSTe Privacy Seal status here.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com

Security Overview

Security Operations

Proactive Monitoring

Khoros monitors all its critical infrastructure, workstations and mobile devices on a 24x7 basis. Alerts are also setup to monitor security-related events and detect security violations from the Intrusion Detection System. Security auditing is enabled on host systems and logs are sent to a secure log collection system for retention and safe keeping. In addition to proactive alerts, security logs are monitored regularly. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel.

Encryption

Khoros assures that all sensitive customer data in encrypted both in transit and at rest using industry standards, TLS 1.2 protocols, AES-256 encryptions, SHA2 hashes. User passwords are using strong cryptographic one-way SHA 512-bit hash with unique salts. Khoros periodically evaluates encryption standards and updates the algorithms in use as necessary.

Vulnerability Management

In addition to security hardening and installing security patches during the controlled build process, Khoros has adopted a standards-based approach to vulnerability lifecycle management following these four key steps: Acquire, Assess, Manage, and Report.

- Acquire - The vulnerability data is acquired from multiple sources such as Internal Process, Customer Reports and Third Party researchers in conjunction with Open Source (NIST NVD, US-CERT and others) and Commercial feeds.
- Assess - The information acquired from the above step is then assessed to evaluate the risk that the vulnerability posses and is assigned a severity level (Critical, High, Medium or Low) baed based on the likelihood, impact, relevance of the vulnerability. Critical and High severity vulnerability are classified as P1 and mitigation is rolled out on an urgent basis.
- Manage - Patching process differs based on the criticality of the vulnerability that is being addressed. For Critical and High severity patches, an out of schedule patch is issued and applied and for others patches are deployed during normal maintenance windows on a published schedule. All of the patches follow the standard patching process, the fix are testing in QA environment and then are applied to production system to minimize any disruption.
- Report - Systems and applications are monitored using manual and automated tools to report on the status of security patches. Any patches or security updates that are missing are processed using the Khoros Vulnerability Management Lifecycle.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com

Security Overview

Network and Infrastructure Security

Khoros divides its system into separate networks to better protect more sensitive data and to separate public services from internal services. Customer data submitted into Khoros is only permitted to exists in Khoros's production network. Administrative access access to systems within the production network is limited to those engineers with a specific business need.

Khoros platform servers are allocated to the respective security groups, characterized by specific security settings (TCP/IP level), and supplemented by individual instance-level stateful firewalls. Separate VLANs are used to split production, testing and development environments, as well as to segregate end-user and administrative traffic. All network access to the production environment is protected by a multiple network traffic filtering system in a "deny-all" mode.

Consistent with our DevSecOps approach, we maintain a "configuration-as-a-code" approach for network security and firewall rules, and have alerts for any discrepancies between the approved configuration and production settings.

Data Retention

Customer data is retained for the duration of the customer's contract with Khoros, unless otherwise instructed by the customer. Once the contract ends, Khoros Support contacts the customer to offer the return of the data. Once the data has been returned or declined, the data is deleted. Deletion occurs within thirty (30) days with the following exceptions: (a) as otherwise required by applicable law; (b) data on backup systems or media is maintained for 90 days in order to maintain sound business continuity practices and then deleted; and (c) log files are maintained for up to twelve months for security reasons and then deleted.

During and after the life of the contract Khoros can use aggregated and anonymized data for metrics and reporting purpose. This data does not include any personal information and does not include any information about the customer or the end user.

Data Backup & Restoration

Backups are encrypted using AES 256-bit encryption and are overwritten every ninety (90) days. Access to the backups is restricted to authorized individuals. Offsite backups are kept in a secure facility. Backups are made daily and weekly. We conduct backup restoration testing every six (6) months.

Data Destruction

Once the contract is over, if the customer wishes to have a copy of its data, we securely provide the information to the customer for: (i) Khoros Community content, at one time and at no charge, in a machine-readable format, and at Khoros's option, either in a single data extraction or multiple data extractions; and (ii) all other Khoros Applications, customer may download the content itself in a comma separated value (.csv) format. Khoros may provide additional reasonable assistance for data

extractions at Khoros's standard Professional Services rates. The availability of Content for extraction or downloading from certain Applications may be limited to the most recent 24 months.

The data is made available for 30 days from the contract expiration or termination, after which time it is deleted in accordance with the above "Data Retention" Section, unless otherwise agreed to by the parties. The active databases are also dropped from the production servers as well after the data extraction is transferred to the customer. Once the media used for storage is retired it is scrubbed or destroyed using NIST SP 800-88 guidelines.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com

Security Overview

Secure Application Development

Khoros has very robust processes in place to assure that security is tightly integrated within our products.

Secure Software Development Lifecycle (SDLC)

Khoros utilizes a secure software development lifecycle that includes the following steps to prevent and/or detect security vulnerabilities from getting into our products:

- OWASP Top 10
- CWE/SANS TOP 25 Most Dangerous Software Errors
- Security design reviews
- Manual security reviews of source code
- Automated static source code security scans
- Automated dynamic security scans

Penetration Testing

Khoros conducts annual third-party application penetration tests. Customers and prospects who have signed non-disclosure agreements may request a copy of our most recent penetration test reports by contacting security@khoros.com or through your Technical Account Manager. Khoros also allows existing customers to perform independent security tests against non-production application instances under certain conditions. For more details, see the Khoros Security Testing and Reporting Policy is available on our website at https://www.khoros.com/khoros-security.

Application Security Features

Khoros applications have built in features to address common web application security flaws and attacks, some of which include:

- Input validation: Inputs and outputs are checked for proper and expected input to protect against cross-site scripting and script injection attacks.
- Role based permissions: Our applications support a robust permissions system which allow granular control over user access.
- CSRF protection: Sensitive features and form submissions are protected with secure and time sensitive cross-site request forgery (CSRF) tokens.
- Logging: User activity is logged and monitored for potential malicious behavior

Open Source Software

The use of Open Source Software in Khoros products undergoes a risk assessment review process to identify the security, legal risks involved before they are released as part of any product or use of it inside the organisation. The review included checking the library for security vulnerabilities, license that the library is being distributed under and intended use case.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com © 2019

Security Overview

Physical Security

Khoros products are hosted on Amazon Web Services (AWS) in North America and Europe*. Physical and environmental controls are specifically outlined in AWS's Security Whitepaper. Additionally, AWS supports ISO 27001, FedRAMP and FISMA certification, which requires best practice in physical and environmental controls.

* Only for Khoros Community.

Incident Response

Khoros has established policies and procedures (also known as runbooks) for responding to potential security incidents. All incidents are managed by Khoros dedicated Security Incident Response Team. Khoros defines the types of events that must be managed via the incident response process. Incidents are classified by severity. Incident response procedures are tested and updated at least annually. Khoros has provisions for customer notifications in case of a breach involving customer data.

Khoros' incident response process conforms to industry best practices. It involves the following phases: Identification, Containment, Investigation, Eradication, Recovery and Lessons Learned.

- Identification – Determining if an incident is or has occurred
- Containment – Preventing the spread of the incident by taking the impacted systems offline
- Investigation – Determining the extent and root cause through forensics investigations
- Eradication – Elimination of the root cause
- Recovery – Restoration of services or capacity that were disabled during containment
- Lessons learned – Review of the incident to recommend long term changes that should be made to prevent or mitigate future occurrences

Business Continuity and Disaster Recovery

Khoros utilizes AWS as its hosting platform which gives us the ability to remain resilient globally even if one location goes down. AWS spans multiple geographic locations and availability zones.

The hosting infrastructure utilized by Khoros is designed with multiple redundancies for maximum uptime. Critical systems are set up in a redundant manner to eliminate single points of failure. This includes redundant servers, load balancers and databases.

Regular backups are made daily and weekly and stored offsite in a secure location for safety. The backups are encrypted using AES 256-bit encryption. Backup restore testing is conducted on an annual basis. Khoros' Disaster Recovery Plan is updated at least annually and tested on an annual basis.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com

Security Overview

Risk Management Program

Khoros maintains a risk register internally that lists of all the risks that are present to the organization as a whole either internally or externally and are categorized into Critical, High, Medium and Lows. The risk management program is a multi step process which include -

1. Risk Identification
2. Risk Assessment
3. Risk Mitigation
4. Risk Acceptance

The risk is calculated using factors like Likelihood, Impact and Risk Rating. The risk register forms a vital part of the Khoros Information Security roadmap so there is continuous reduction in risk to the organization and are prioritized based on the residual risk that is present after corresponding compensating controls are put in place.

Third Party Vendor Management

Khoros engages with third party vendors to provide you services effectively, where those sub-service organizations may impact the security of Khoros's Security Posture, we take appropriate steps to ensure our security posture is maintained by establishing contractual agreements that requires services organizations to adhere to security requirements laid out by Khoros and to ensure their ongoing compliance with our security requirements. To review the list of our sub-services organization, please visit https://khoros.com/khoros-subprocessors.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com

Security Overview

Contact Khoros

For security related requests please email security. Please consider using a secure communication method such as PGP or SMIME for sharing sensitive information.

Khoros
Pier 1, Bay 1A, San Francisco, CA 94111 | Tel: 415.757.3100 | Fax: 415.757.3200 | khoros.com