Khoros

Security Datasheet

Introduction

Khoros takes information security very seriously. Our security controls and mechanisms are based on the ISO 27001 global security management standard and we conduct external security audits and independent security testing on a regular basis. This datasheet provides an overview of the security measures implemented throughout the organization to provide full transparency and a peace of mind for Khoros customers that their information is in good hands.

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 non-disclosure agreements may request a copy of our most recent audit report by contacting security@khoros.com.

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 at https://goo.gl/o1xfzf

Privacy Certifications

Khoros (Lithium) 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 (Lithium) TRUSTe Privacy Seal status at https://goo.gl/HnCZzt

Khoros (Spredfast) is certified under the EU-US Privacy Shield. And Swiss-US Privacy Shield programs. Access Khoros (Spredfast) TRUSTe Privacy Seal status at https://www.privacyshield.gov/participant?id=a2zt0000000017IAAQ

Encryption

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

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

Khoros

Security Datasheet

Physical Security

Hosting Facilities

Khoros products are hosted on Amazon Web Services (AWS) and in Equinix datacenters in North America and in Europe. The security measures implemented at these facilities include monitoring system, digital video recorders, man traps, biometric identification, mandatory visitor check-ins, fencing and 24x7 security guards.

The datacenters are also equipped with fire, water, and heat detection and protection systems as well redundant UPS and diesel generators for uninterrupted high availability operation of mission critical systems. All systems undergo regular maintenance and are tested by the vendors every ninety days for proper operation and safety.

Access Control

Access to the Equinix colocation space is restricted to authorized Khoros staff and trusted local vendors for remote-hands system management only and reviewed on a regular basis. Multiple forms of authentication are required to access the facility such as a valid picture ID, a secret PIN code, and biometric identification (hand or palm geometry scan).

Physical access to AWS facilities is restricted to authorized AWS personnel who have a legitimate business need.

Logical access to the live customer environment can only be established via a secure encrypted session utilizing multi-factor authentication and is restricted to authorized Khoros staff only. All administrative access is logged and audited on a regular basis.

Operations

Proactive Monitoring

Khoros monitors all its production environments and critical infrastructure on a 24x7 basis. An alert system is tied to each of the site's health statistics as well as all major parts of the hosting infrastructure. All major services such as DNS, firewalls, servers, and Internet connectivity are actively monitored. 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.

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** - We collect relevant security information via subscriptions to various security outlets such as US-CERT and notification from our vendors. Information is also collected from monthly vulnerability scans, penetration tests and customer reports.

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

Khoros

Security Datasheet

- **Assess** – The acquired vulnerability information is assessed for relevance and criticality based on a pre-established criterion. Critical and High-risk severity items are classified as P1 and mitigation is rolled out on an urgent basis. Other categories are prioritized based on the likelihood and impact of a given vulnerability.
- **Manage** – We acquire the patch or fix and deploy it using appropriate tools to the target systems. The fixes are tested in the QA environment before they are rolled out to the production environment. Standard patches are installed during normal maintenance windows on a published schedule.
- **Report** – Systems are assessed using manual and automated tools to report on the status of security patches. Any missing patches and updates are processed using the Khoros vulnerability management lifecycle process.

Data Handling and Backups

- At the database layer, data replication is set up from master database servers to slave database servers in real-time. We also take regular snapshots throughout the day.
- 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 regular basis.
- All customer data is retained for the length of the customer contract.
- Once the contract is over, we securely turn the data over to the customer in a machine-readable format. The data is made available for up to 30days before it is purged from our systems.
- Retired media used for storage is scrubbed or destroyed using NIST SP 800-88 guidelines.

Network and Infrastructure Security

Khoros (Lithium) is ISO 27001 certified, which signifies that our security controls and mechanisms are validated against a globally accepted standard based on security best practices such as:

- Redundant multi-tier firewalls (or functionally equivalent technologies) allow relevant ports only such as port 80 (HTTP) and port 443 (HTTPS);
- Front-end application and web servers are isolated from utility services such as DNS and SMTP;
- Database servers are in a separate segment from the front-end servers;
- No direct access from the Internet is allowed to the database servers;
- Intrusion Detection Systems are deployed to monitor unauthorized access or detect malicious traffic;
- Regular security vulnerability scanning on a monthly basis.

System-level security conforms to the same high standard of security best practices such as:

- Only necessary services and software are installed;
- Servers are regularly updated with the latest security patches;
- All management traffic to the servers is encrypted;
- Administrative access is restricted to authorized staff and must occur over a secure encrypted session.
- All administrative access is logged and monitored;
- Security auditing is turned on and logs are sent to a secure log collection system.

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

Khoros

Security Datasheet

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 secure coding practices training
- 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.

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/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

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

Khoros

Security Datasheet

Incident Response

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

The incident response process is thoroughly documented and exercised at least once a year. Khoros has provisions for customer notifications in case of a breach involving customer data.

Business Continuity and Disaster Recovery

The hosting infrastructure utilized by Khoros is designed with multiple redundancies for maximum uptime.

- Secure datacenters have UPS and generator backup systems for power and diverse entry points for key utilities and communication facilities.
- Multiple high-speed Internet Service Providers for fast Internet connectivity using BGP for redundancy and automatic failover.
- Critical systems are set up in a redundant manner to eliminate single points of failure. This includes redundant servers, load balancers, firewalls, switches, and routers.
- Servers are deployed with redundant power supplies, redundant network cards, and redundant disk storage.
- At the database layer, data replication is set up from master database servers to slave database servers in real-time. We also take regular snapshots throughout the day.
- 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.

Contact Khoros

- For Security related requests please email security@khoros.com. 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
© 2019 Khoros Technologies, Inc. All Rights Reserved.