Village messenger Security

Table of Contents

3. SECURITY

Effective: May 25th, 2018

We take the security of your data very seriously at village messenger. As transparency is one of the principles on which our company is built, we aim to be as clear and open as we can about the way we handle security.

If you have additional questions regarding security, we are happy to answer them. Please write to legal@village-messenger.com and we will respond as quickly as we can.

3.1. CONFIDENTIALITY

We place strict controls over our employees' access to the data Users and Customers make available via the village messenger services, as more specifically defined in your agreement with village messenger covering the use of the village messenger services ("User and Customer Data"), and are committed to ensuring that User and Customer Data is not seen by anyone who should not have access to it. The operation of the village messenger services requires that some employees have access to the systems which store and process User and Customer Data. For example, in order to diagnose a problem you are having with the village messenger services, we may need to access your User/Customer Data. These employees are prohibited from using these permissions to view User/Customer Data unless it is necessary to do so. We have technical controls and audit policies in place to ensure that any access to User/Customer Data is logged.
All of our employees and contract personnel are bound to our policies regarding User/Customer Data and we treat these issues as matters of the highest importance within our company.

3.2. PERSONNEL PRACTICES

Village messenger conducts background checks on all employees before employment, and employees receive privacy and security training during onboarding as well as on an ongoing basis. All employees are required to read and sign our comprehensive information security policy covering the security, availability, and confidentiality of the village messenger services.

3.3. DATA ENCRYPTION IN TRANSIT AND AT REST

The village messenger services support encrypted SSL protocol.
We monitor the changing cryptographic landscape closely and work promptly to upgrade the service to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. For encryption in transit, we do this while also balancing the need for compatibility for older clients.

3.4. AVAILABILITY

We understand that you rely on the village messenger services to work. We're committed to making village messenger a highly-available service that you can count on. Our infrastructure runs on systems that are fault tolerant, for failures of individual servers or even entire data

centers. Our operations team tests disaster-recovery measures regularly and staffs an around-the-clock on-call team to quickly resolve unexpected incidents.

3.5. DISASTER RECOVERY

User and Customer Data is stored redundantly at multiple locations in our hosting provider's data centers to ensure availability. We have well-tested backup and restoration procedures, which allow recovery from a major disaster. User/Customer Data and our source code are automatically backed up nightly. The Operations team is alerted in case of a failure with this system. Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected.

3.6. NETWORK PROTECTION

In addition to sophisticated system monitoring and logging, we have implemented two-factor authentication for all server access across our production environment. Firewalls are configured according to industry best practices and unnecessary ports are blocked by configuration with AWS Security Groups.

3.7. HOST MANAGEMENT

We perform automated vulnerability scans on our production hosts and remediate any findings that present a risk to our environment. We enforce screens lockouts and the usage of full disk encryption for company laptops.

3.8. LOGGING

Village messenger maintains an extensive, centralized logging environment in its production environment which contains information pertaining to security, monitoring, availability, access, and other metrics about the village messenger services. These logs are analyzed for security events via automated monitoring software, overseen by the security team.

3.9. INCIDENT MANAGEMENT & RESPONSE

In the event of a security breach, village messenger will promptly notify you of any unauthorized access to your User/Customer Data. Village messenger has incident management policies and procedures in place to handle such an event.

3.10. EXTERNAL SECURITY AUDITS

We contract with respected external security firms who perform regular audits of the village messenger services to verify that our security practices are sound and to monitor the village messenger services for new vulnerabilities discovered by the security research community. In addition to periodic and targeted audits of the Village messenger services and features, we also employ the use of continuous hybrid automated scanning of our web platform.

3.11. CONTACTING VILLAGE MESSENGER

If you believe you have found a security vulnerability on village messenger, please let us know right away. We will investigate all reports and do our best to quickly fix valid issues.
To find out more about village messenger security, please visit our security information page.
For other security questions or issues, please email legal@village-messenger.com.