Usked

SECURITY INFORMATION

UPDATED MARCH 2025

TABLE OF CONTENTS

PURPOSE & PROVIDERS

PURPOSE

Usked's primary security focus is our commitment to protect our licensees' data. We have invested in resources and controls to support this need. This document will outline the specific measures put in place to ensure security of our software and the information being stored and transmitted through them. Below are the objectives we have based our security measures on:

- **PROTECTING PRIVACY OF CONFIDENTIAL DATA**
- **CONTINUITY OF SERVICE**
- **DATA INTEGRITY**
- **COMPLIANCE WITH INDUSTRY STANDARDS**

PROVIDERS

Usked software runs on dedicated servers managed by Liquid Web, a secure web hosting provider that has been top of the industry for over 20 years. More about Liquid Web can be found here: https://www.liquidweb.com/

Additionally, Usked uses Amazon Web Services (AWS) to store files and videos. Usked follows AWS's recommendations on security best practices regarding securing access to our AWS accounts.

FAQS

DEPENDABILITY

WILL USKED'S SOFTWARE ALWAYS BE AVAILABLE?

Liquid Web's SLA includes 100% network uptime. This ensures that major routing devices within the network are always reachable from the global internet.

IS MY DATA REGULARLY BACKED UP?

Yes - data is backed up to an off-site location every hour by Acronis Cyber Backups. More on Acronis Cyber Backups can be found here: https://www.liquidweb.com/products/add-ons/storage-backups/acronis-cyber-backups/

WHAT IF SOMETHING ISN'T WORKING AS EXPECTED?

If a part of the system is not working, impacted licensees would be notified. To ensure transparency and timely updates, any identified issues are published to the Usked Support Center under our Service Status page.

HOW DOES USKED ENSURE DATA INTEGRITY?

Data alteration is only possible by authenticated Usked users having a role that allows them to do so. It is not possible to destroy data in Usked; when a user takes action to delete data, the system flags the data as being deleted and hides it from default view rather than actually physically deleting it. This allows any data to be fully restored.

SECURITY

WHAT PHYSICAL SECURITY PROTECTION ARE IN PLACE TO PROTECT MY DATA?

Liquid Web facilities are highly secure. These are the safeguards put in place for the data centers:

- External walls are reinforced poured concrete
- 24/7/365 manned facilities
- Patrolled regularly by on-site security officers
- CCTV Security Cameras Covering inside, outside, and all entrances
- Entrances controlled by electronic perimeter access card system
- Remote security monitoring by 3rd party security company
- Entrances secured by mantraps with interlocking doors

FAQS

SECURITY CONTINUED

WHAT COMPLIANCE CONTROLS ARE IN PLACE?

Liquid Web data centers are SSAE-16 and Safe Harbor certified. They recently completed a SOC 2 attestation performed under the newly released AICPA SSAE 16 attestation standard that replaces the SAS 70 standard. In undertaking this examination, Liquid Web utilized the SOC 2 Trust Services Principles and Criteria for security and availability as a benchmark in developing our system description. They addressed each of the more than 100 individual controls criteria listed in the SOC 2 Principles and Criteria.

IS MY DATA ENCRYPTED?

Yes, all data is encrypted before it leaves Liquid Web servers.

WHAT SECURITY TESTING HAS USKED SOFTWARE UNDERGONE AND PASSED?

Liquid Web facilities are highly secure. These are the safeguards put in place for the data centers:

- ATO (Authorization to Operate) - accreditation from government agency
- IBM Security AppScan tool - More information about this tool can be found here: Application Security
- Tenable Network Nessus Vulnerability Scanner tool

PRIVACY

IS USKED SOFTWARE HIPAA COMPLIANT?

Yes - details can be found here:
HIPAA Compliance

DOES USKED HAVE A PRIVACY POLICY?

Yes - our privacy policy can be found here:
Privacy Policy

FAQS

PRIVACY CONTINUED

DOES USKED KEEP DATA AFTER A CONTRACT HAS ENDED?

Licensee sites and all data in them are retained for as long as a contract is valid. Data is kept active for 60 days after contract has ended or been terminated. Once that date is reached, the site and any licensee data is deleted and cannot be restored.

INTERNAL POLICY

DO USKED EMPLOYEES RECEIVE SECURITY TRAINING?

Yes - all Usked employees are required to undergo training for cyber security, HIPAA awareness, and FERPA awareness. This training is completed upon initial onboarding and then repeated every 2 years. As part of our Employee Security Policy every Usked employee must adhere to the following protocols:

ALL EMPLOYEES MUST REDUCE THE RISK OF UNAUTHORIZED ACCESS BY:

- Locking computers when leaving desks.
- Storing sensitive files on the company's secure drive only and not on any local computers or devices.
- Accessing sensitive data only from secure, private networks.
- Passwords must follow the NIST guidelines and must not be shared.
- Installing a secure work policy on any device prior to being able to access work materials from them.

HOW IS HIGH LEVEL ACCESS TO MY SITE PROTECTED?

Prior to data import our IT team changes to a unique, secure password for the ROOT account in your site. Once your site is live our team will ask you to change the password for the default Administrator account in your site as well.

ACCESS

ACCESS CONTROL METHODS

Technical controls used to grant access to data.

- **ROLE BASED, MINIMUM NECESSARY ACCESS MODEL**
- **ENCRYPTION BEFORE LEAVING SERVER**
- **NETWORK SEGREGATION**
- **SERVER ACCESS RIGHTS**
- **FIREWALL RULES**

USKED EMPLOYEE ACCESS

Who has access to licensee data and when they are accessing it.

HOW IS HIGH LEVEL ACCESS TO MY SITE PROTECTED?

Usked employees are granted access to data based on their role in the company. This is minimized to only those whose jobs require it. Our support team may log in to licensee sites to troubleshoot and resolve any licensee driven inquiries or issues.

MONITORING

MONITORING

WHAT TYPES OF MONITORING DOES USKED DO?

Liquid Web provides 24/7/365 system health monitoring, including alerts and notifications. Additionally, software provided by Usked is built to alert our IT team of any crashes or potential issues. Our IT team receives an instant notification of any security incidents involving the dedicated servers at Liquid Web, so we can monitor events and take appropriate action immediately.

HOW DOES USKED IDENTIFY SUSPICIOUS ACTIVITY?

Usked employs comprehensive time stamped logging of all user activity, including all access from web and mobile devices. All suspicious activity is automatically recorded and sent to the system administrator.

IF A DATA BREACH DOES OCCUR WHAT STEPS DOES USKED TAKE?

IT systems are fully managed by Liquid Web. In our experience, once the vulnerability is identified the systems are patched within hours of a fix becoming available. They guarantee response within 30 minutes to any inquiries. Usked will provide written notice of the breach and take prompt corrective action to rectify it. Usked will also include any steps the licensee should take to further protect themselves from potential harm resulting from the breach.

SECURITY FEATURES

USKED SCHEDULING SYSTEM

ENFORCE HIPAA SETTING - Once the toggle is set to Yes for a particular group, Usked will prevent the system from sending PII to third party systems for that group's requests. Including:

- The address of the service request location
- The room number
- The public location notes
- The names of the points of contact
- The contact information for the points of contact
- The public notes for the points of contact
- The names of the clients receiving services
- The service requested for these clients
- The public notes for these clients
- File attachments
- The public event notes (event details)

TWO FACTOR AUTHENTICATION (2FA) - Security measure imposed when signing into your account that will require a device to be validated prior to gaining access to the Usked account. This means that when enabled for your account, 2FA would require two factors in order to gain access. The first factor being something you know, 1) your password, and the second factor being something you have, 2) your email account to retrieve the validation code. Logging in will only be possible on devices that have been validated (by entering the unique validation code). When Usked detects that someone is attempting to sign into your account using a device that it has not seen before, Usked will send you an email message with a 6 digit validation code. This 6 digit code is required to be entered on the next screen with your password, in order to complete the sign in process.

SECURITY FEATURES

USKED SCHEDULING SYSTEM CONTINUED

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

When this feature is enabled Usked will use LDAP to authenticate the user account instead of the standard authentication. This will send the username and password to the LDAP server to authenticate it before allowing access.

VIRTUAL+ SERVICES URL ENCRYPTION

When a request is converted to a Virtual+ request an encrypted URL is generated. This URL acts as a key to access the Virtual+ meeting, so encrypting it ensures that the URL cannot be guessed for unauthorized access.

VIRTUAL+ SERVICES LOCK ROOM FEATURE

Once all necessary parties have joined the Virtual+ meeting you can prevent additional participants from being able to enter the room by locking the room. This allows for additional security to prevent unwanted parties from entering a room.

USKED APP

Features applicable to the Usked app:

- **ENFORCE HIPAA SETTING**
- **TWO FACTOR AUTHENTICATION (2FA)**
- **LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)**