Sumerian Services Policies ▶▶

sumerian®
Forward Thinking ▶▶

Sumerian Services Policies

Data security and privacy

Sumerian employs the highest standards of internal security and privacy for our clients' data. Sumerian has been ISO27001 compliant since 2008 and accredited since February 2011. Sumerian is externally audited every six months to verify compliance to our Information Security processes and procedures. These include annual external penetration tests, and quarterly internal audits.

Sumerian's service environment is hosted on our own private hardware, co-located in a secure Tier II datacenter, managed by Verizon. Physically this is a state-of-the-art, security-manned datacenter, with all the best practice security controls you would expect from a company that provides co-location services for thousands of large enterprises.

Sumerian has followed good industry practice when it comes to designing, implementing, and running our service environment. Our approach is outlined in more detail below.

Network

Our service environment is deployed on our own private hardware. Only our web servers can be accessed from the Internet and then only via a secure username and password. The application and database servers are separated from the web servers via clustered Firewalls. These servers can only be accessed from within our Local Area Network.

Access to our Production application servers and database servers is strictly controlled. Access may only be granted through an approval process and all access is logged and audited.

Application security

Your data is only ever stored in our Production environment and, for a limited time, in the backup files we take of those systems. Should you upload any of your data using our Data Collector utility, the data files will be compressed prior to transit and encrypted during transit (again using a 128 bit SSL certificate). Your uploaded data files are then stored in our private storage. We have processes in place to restrict our access to your data including strict audit trails.

Managing threats and vulnerabilities

Following good practice, we:

- employ multiple different types of firewalls across our infrastructure to protect against unauthorized network connections;

- run continuously-updating, anti-malware software on each of our servers;

- only open necessary network ports;

- regularly patch our servers against vulnerabilities;

- test the patches on our test and development environments before they go live on production;

- monitor our servers around the clock and our monitoring systems alert our team of critical failures;

- backup data every day to an off-site location;

- automate our server build process to make recovery faster.

Data sensitivity

In forming a judgment as to whether you regard our security as sufficient for your business, you should consider how sensitive the data is that you intend to send us or upload.

The data we process for you is related to your infrastructure and infrastructure performance. It is unlikely that this data will contain commercial or personal data and as such will, in most businesses, be regarded as non-sensitive. However, as a policy we treat your data as confidential and we have put in place security measures to protect it.

Accessing Sumerian Capacity Planner

If you access Sumerian Capacity Planner the following data and security features will apply:

Your browser will display a secure padlock indicating that you are on a secure site. This means that all data transmitted between your browser and our servers is encrypted. We apply modern cryptography techniques to encrypt data in transit by using 128 bit TLS1.2 Comodo High Assurance Secure Server Certificate Authority including RSA as the key exchange mechanism. For any browser based application, once data is in your local browser it is not encrypted (data is only encrypted during transportation). We also cannot protect information (i.e. reports) that you may store locally on your systems. This is your responsibility.

Sumerian will ask you to use a password that is likely to be longer and more complex than your corporate standard. Your password is only ever stored in one place on our system and it is hashed and salted. We do not know it nor will we ever ask you to tell us it.

The only data about you that we can access and store is your registration data (such as your name, company, user name and email address). This is necessary so that we can support you if you contact us for help when using our software. We also store, and can access, any correspondence between you and us. This includes support tickets raised.

Disaster recovery and business continuity

Data pertaining to production services are backed up to an off-site, secure location every 24 hours.

Sumerian has a disaster recovery facility (secondary datacenter) that is geographically remote from its primary datacenter. In the event of the primary datacenter being rendered unavailable, Sumerian will invoke Business Continuity plans to restore service. These plans are reviewed, audited and tested once per year.

Service levels

Sumerian monitors your service continuously and we operate the following service levels:

- Availability:
    - 99.9% for UK business hours (Monday to Friday, 9am to 5pm).
    - 95% outside these hours, and outside scheduled maintenance windows.
- Planned maintenance: all planned maintenance will be scheduled to take place outside normal working hours from Monday to Friday either before 9am or after 5pm (UK time).
- Essential maintenance: Sumerian reserves the right to perform essential maintenance during UK business hours in response to service incidents.

Support

Our standard support arrangements are telephone and email support during UK business hours (9am to 5pm, Monday to Friday).

Constraints and customer responsibilities

When using Sumerian Capacity Planner you have the right to upload data solely for the purpose of analyzing the current and future capacity and performance of your IT infrastructure. If you upload data for any other purpose, Sumerian reserves the right to suspend and ultimately terminate your access at our sole discretion. The upload of any personal, financial or business sensitive data is not permitted unless expressly agreed in advance by Sumerian.

When you upload your data into Capacity Planner, it is stored and processed in our secure datacenter. The security arrangements in place are outlined above.

We apply a fair use policy to the number of users who access the system and the amount of data you require us to store. If we feel that you are exceeding fair use we will inform you. Should you continue to breach our fair use policy, we reserve the right to archive your data, suspend and ultimately terminate your access to the service at our sole discretion.

Data extraction and upload

From time to time, we may provide advice to assist you in the extraction of log data. This advice may take the form of a script or software utility to be executed in your environment. Such a script or software utility is provided as is with no support or warranties, it is executed at your own risk.

Solution requirements

Sumerian Capacity Planner has no specific technical dependencies or requirements on the client side in terms of bandwidth or latency.

It requires the following minimum Operating Systems and Browsers:

- OS
  - Windows 7
  - OS X 10.7

- Browsers
  - Google Chrome 30
  - Mozilla Firefox 21
  - Apple Safari 6
  - Microsoft Internet Explorer 11

(20160913)