Is my data safe in the Circuit cloud?
Absolutely!

At Unify, we take security very seriously. We understand how important the confidentiality, integrity and availability of your data is to you, and we've diligently built security measures into our processes, data centers, and applications.

Here is some important information on how we keep all of your content secure and private in Circuit – We hope this gives you peace of mind.

Circuit is a highly secure, public, multi-tenant cloud offering. Circuit relies on a secure web browser for connection to the cloud, and the browser uses the WebRTC protocol for real-time communications sessions. All your conversations with other Circuit users are encrypted and secure.

All data access is controlled via Access Control Lists, and strict enforcement ensures domain data isolation so that only you can see your company's data, and your colleagues can see only data that you explicitly share with them.

You and your organization own the data you store in Circuit. Access to your user data is restricted to your user account. Sensitive user account data like passwords is encrypted or where it can be avoided, not stored at all.

Our security architecture

We've deployed multiple layers of security to protect access to Circuit. This includes firewalls, complemented by built-in security to the Circuit application which protects information, and restricts access to intruders.

Circuit domains (also referred to as tenants) are separated within the Infrastructure as a Service (IaaS) using private Virtual LANs. Dedicated hardware such as bare metal servers and firewalls are not shared with other domains.

While data is in transmission, the communication protocols used by Circuit assure that data is always encrypted. All communication between clients and servers is encrypted using HTTPS and SRTP transport. Circuit also supports Perfect Forward Secrecy to make sure session keys are not compromised.

All files uploaded are actively scanned during upload for known viruses and blocked before they're stored or allowed to be shared, using commercially available anti-virus technology. The Anti-virus libraries are updated regularly. However, we recommend that our customers operate anti-virus software on their clients.

Our security management practices

At Unify we have implemented a best practices security management framework according to ISO27001 and hold several certificates within the organization.

This includes regular vulnerability management assessments and product security assessments for each major release of Circuit or major extensions to the application. As part of our change management processes, all changes are implemented in our test and integration system before being implemented in the production systems.

Prior to Circuit's release last fall, we conducted an external audit on our data centers' infrastructure and service. Our data center service provider has strong security management processes in place, including ISO 27001 certificates and regular internal and external audits.

Our Data Centers

We currently have 3 Circuit systems: 1 production system in Washington DC for North American customers, and 2 systems in Amsterdam; one for system test and integration, and the other is a production system for customers in Europe. Our plan is to add another production system in Frankfurt Germany by mid-next year.

Our data centers are protected against unauthorized access and are only accessible to authorized individuals. Access is monitored via smart cards and biometric controls at all physical access points. Video cameras are employed to deter and detect unauthorized access. Audits and re-validation of authorized individuals are performed quarterly.

Our data centers maintain security management systems that are independently reviewed by independent auditors. Access to data center systems is monitored and logged and regularly reviewed.

Facilities are in place to ensure 24/7 system availability with uninterruptible power supplies, emergency power generators, and environmental monitoring and controls.

The privacy of your data

You and your organization own the data you store in Circuit, and are responsible for the content of all visual, written or audible communications, files, documents, videos, recordings, and any other material ("User Content") used in connection with your Circuit user accounts, and for your interactions with other users.

Our data retention policy is in compliance with privacy regulations and relevant standards for all circumstances where Circuit is available.

At the conclusion of your Circuit free trial, when you convert your trial to a paid subscription, all your data and communications are preserved securely. However, if your organization discontinues use of Circuit, all of your data will be deleted within 14 days.

Your Circuit domain

All Circuit domains are logically separated. As a Circuit Administrator, you have administrative control of your Circuit domain, and are able to see an overview of your users and the amount of data uploaded to your Circuit domain.

Circuit uses cookies to store a Circuit user's preferences and settings, to authenticate the user, to collect usage data and in general to operate Circuit. Unify has made the necessary contractual arrangements that are required under the EU Data Protection Directive and the applicable local law for a legally compliant transfer or processing of personal data. Critical data such as passwords are not exposed to log files.

By default, users are configured in the system with only the ability to see their own data and data explicitly shared with them.

yourcircuit.com

circuit
by unify

Make your
team*work* better.