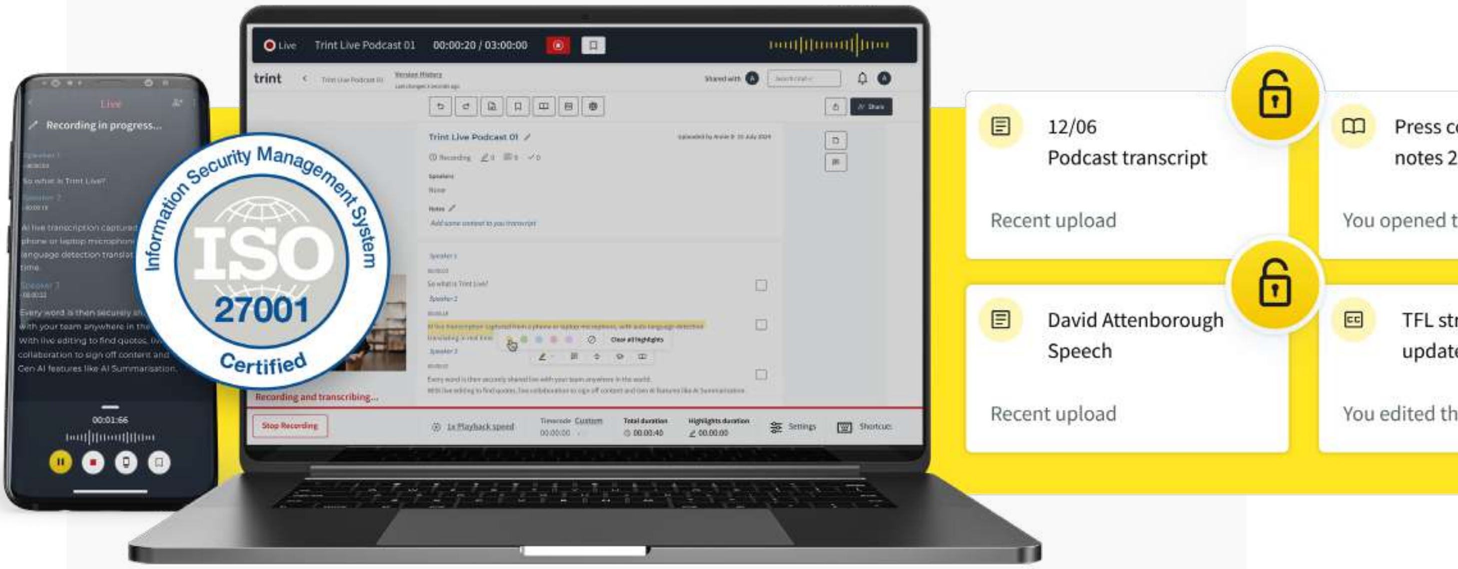
INFORMATION SECURITY FAQS

A comprehensive guide to our security frameworks and protocols

trint

trint

CONTENTS



DATA PRIVACY

Does Trint encrypt all data? If keys are used, who holds the keys?

Data is encrypted in transit using TLS 1.3+ or later, and at rest using AES 256. Keys are stored and managed by AWS, but are controlled by Trint.

Does Trint have backup, storage and restoration procedures? How long are backups retained? And are the backups encrypted?

Our cloud database takes incremental snapshots enabling us to continuously back-up customer data and allow point in time recovery for one week. Daily, weekly and monthly snapshots are taken and held for up to one year. Snapshots are duplicated offsite from the DaaS provider for business continuity purposes.

Database recovery tests occur once per quarter.

Customer content is stored in AWS S3 with version control enabled. The data is replicated over at least three of the Availability Zones in the region. AWS states a durability of 99.999999999%, and availability of 99.99% over a given year. No additional backup is made of this data.

All data at rest is encrypted with AES 256.

Can any third party access customer content and, if so, how?

Trint uses third parties to provide its service:

Trint services run inside Amazon AWS, with Trint customer content stored in encrypted AWS S3 buckets.

Trint uses a cloud-based database within the MongoDB Atlas service to store customer transcriptions in encoded documents with full encryption at rest and in transit.

FileStack is used for file transfer services; when files are uploaded via the Trint app they will go directly from the User to Trint. However, uploaded media may pass via Filestack if transferring directly from a cloud storage provider (e.g. Dropbox or Google Drive).

For a complete list of Trint sub-processors, please see here.

Will customer data be permanently erased from the solution, including any backup storage, when this data is deleted or the service ended?

A monthly secure deletion request can be arranged via your Customer Success Manager at Trint. As the client, your content will be removed from AWS S3, and data will be removed from the database.

Database backups may retain content metadata (filename, excerpt, media type, duration, file size) for up to a year.

Trint can check the database and S3 for the files that were removed and validate that they are missing. We can also search the secure deletion log with the status of each file that has been queued for deletion.

Is verification provided that data has been securely deleted?

Yes, via your Trint Customer Success Manager.

Are third party vulnerability assessments conducted on the applications processing customer data? What is the frequency of these assessments?

A thorough vulnerability assessment is performed once a year by a well-established software security auditing company. In addition, we continuously run a Vulnerability Program Disclosure via a security testing platform. A summary of this report can be provided under NDA.

Is “Enforced TLS” the default standard for outgoing Trint emails”?

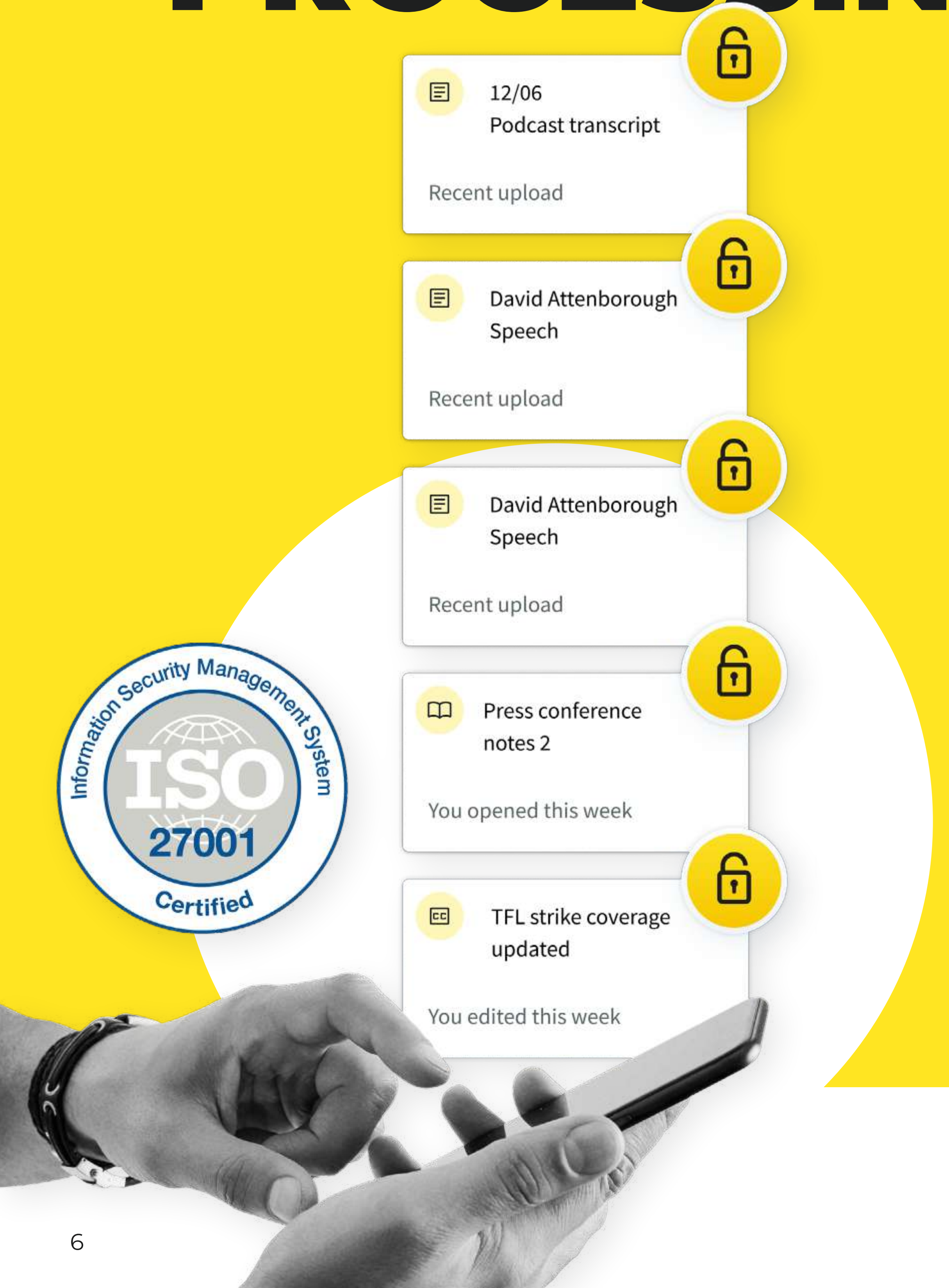
Trint does not transmit our customers’ data via email.

TLS is enforced as default, while our email domain is configured with DMARC.

Is an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) deployed and monitoring all traffic?

We use AWS Guard Duty for anomaly detection and alerting, and AWS WAF for request filtering and rate limiting.

DATA PROCESSING



12/06
Podcast transcript

Recent upload

David Attenborough Speech

Recent upload

David Attenborough Speech

Recent upload

Press conference notes 2

You opened this week

TFL strike coverage updated

You edited this week

Is any sensitive personal data being processed?

Trint does not process sensitive information as a Data Controller.

Customers may upload media that contains sensitive personal information that Trint processes as a Data Processor on behalf of the customer. Trint has no visibility or control over this data. Trint does not access customer content without the prior written consent of the customer unless required by local law. Customers will be notified prior to execution of such a request.

With regards to sub-contractors that hold customer data, how does Trint ensure that they meet the required information security standards?

All of Trint's suppliers are subject to a Vendor Security Assessment process as per our ISO approved Information Security Management System (ISMS). Vendors are required to meet or exceed Trint's own security standards for the type of data processed.

For more details, ask a member of the Trint team.

How does Trint comply with cross-border data transfer requirements

Trint is GDPR compliant and asserts Standard Contractual Clauses in our enterprise contracts.

For data transfer and storage, Trint uses HTTPS (using TLS 1.3+) for secure data upload, export and transfer.

Why does Trint need to collect personal data or sensitive personal data?

This is for the provision of user accounts.

Has Trint provided a Privacy Notice?

Trint has a platform privacy policy that can be viewed here and a website and marketing policy that can be viewed here. If you have any questions, please contact a member of the Trint team.

What access do Trint developers have and what training do they receive to ensure security standards?

Trint is designed and built with security in mind. Trint uses the principle of least privilege. Our Developers are required to undertake OWASP and other security training on an annual basis.

What is Trint's retention policy for data processing?

The lifetime of the user account.

Where is the data stored?

We store our data in Amazon Web Services (AWS).

Does Trint have the ability to promptly delete or provide information on a specific individual on instruction from the customer?

Administrators appointed by the customer can view activity and remove users from the organization within the admin dashboard.

Secure deletion of customer content and user accounts can be performed by Trint upon request once per month.

How is the data transferred?

In all cases, data is transferred over a TLS v1.3+ encrypted connection.

ACCESS CONTROL

What is the process for mutual authentication on sending API commands?

An API key will be generated by the customer, which is used to authenticate the calling user.

The server is authenticated by use of a TLS v1.3+ connection and the certificate obtained during the connection.

Does the service allow for a login federated IDM infrastructure? Does your service support SAML or ADFS for Single Sign-On (SSO)?

SAML based SSO integrations are possible.

Does Trint log and audit staff's privileged access and activities?

Yes. All access and changes in the platform are logged using AWS CloudTrail.

How is customer data kept logically and/or physically separated from other users' data?

Data stored is kept in per user file system containers. Processing of data occurs in single use container instances that are destroyed upon completion.

Is there multi-factor authentication (MFA) implemented for user access?

Trint does not currently provide MFA. It is recommended that enterprise customers enable an SSO integration allowing them to enforce their own security standards for authentication and authorization.

What happens if an access violation is identified?

For access violations identified, customers can provide the documented process for remediation that is followed. Our Information Security Incident Response Procedure would be followed.

Is remote access allowed for employees, contractors and / or agents?

Trint Engineers can access the cloud environment, with access policy based on the least privilege principle.

What levels of user access are available? What reports are available?

The fine-grained controls within our Workspaces include:

- **Add Workspace members**
- **Archive Workspace**
- **Can access Workspaces**
- **Comment on Trints**
- **Create folders**
- **Edit folders**
- **Edit Trints**
- **Edit Workspace members**
- **Edit Workspaces**
- **Remove Workspace members**
- **Share transcripts with the public**
- **Share transcripts with users outside the Workspace**
- **Upload to Workspace**

Predefined roles and custom roles comprised of these are available.

Usage reports are available upon request or via the admin dashboard (exportable as CSV).

How are the accounts with the highest level of privilege authenticated and managed?

Access to the AWS root account is restricted. All access to the platform is controlled using time-limited credentials authorized by Google Workspace SSO and group membership, which in turn relies on Multi-factor authentication.

Will any form of remote access technology be required and, if so, what? Does this include two factor authentication?

The customer's users access the platform using a web browser, desktop app, mobile app or via the API where an automated process is integrated. Trint can also be accessed on mobile or a desktop app now too.

AUDIT & SECURITY REVIEWS

What scanning and testing processes, if any, does Trint perform, and at what frequency? How does Trint resolve issues identified through such testing?

Penetration testing is performed annually by a 3rd party. Currently that provider is Cyber Armed. The last test was performed in Jul 2024.. The report is available under NDA (though a limited executive summary is available on request without an NDA required).

Trint runs a Vulnerability Disclosure Program for the responsible disclosure of issues identified outside of penetration testing.

Do you (or a third party) conduct internal audits regularly?

Our internal audit process provides a comprehensive, annual assessment of our information security controls.

Has Trint undergone an independent review of information security (example: ISO 27001, SOC 2 Type 2, PCI, etc)?

Trint holds ISO 27001 certification which is audited by an external team annually. Please reach out to a Trint team member if you need a copy of this certificate.

Do Trint (or a third party) conduct external audits regularly?

External audits of Trint's ISO 27001 ISMS are performed annually.

Have all relevant statutory, regulatory, contractual requirements (including: intellectual property rights, protection of records, protection of personally identifiable information and cryptographic controls), and your approach to meet these requirements, been explicitly identified, documented and kept up to date for the customer?

As part of our ISO ISMS, Trint reviews all legal, regulatory and contractual requirements relevant to our business operations.

Is your ISMA (i.e. control objectives, controls, policies, processes and procedures for information security) reviewed and inspected for compliance, independently at planned intervals, or when significant changes to the security implementation occurs?

The internal audit occurs every six months. An external audit occurs annually.

Has an internal audit group performed a formal information security assessment of your environment?

Yes. ISO 27001 certification requires a regular internal audit.

This is performed annually to ensure continuous improvement of Trint's information security management system.

trint

If you have any questions regarding this guide, please contact your Trint representative or email us at info@trint.com.