trint

Security Buyer's Guide

Speech to Text to Magic

Introduction

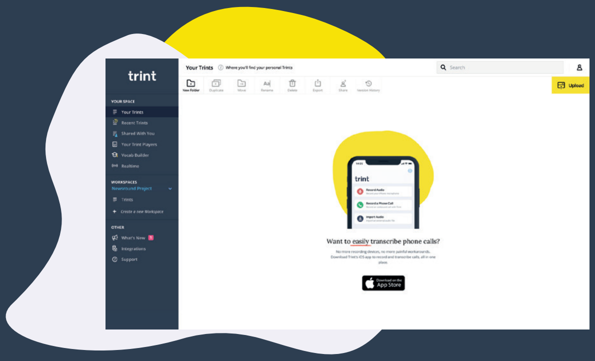
Who We Are

Trint's goal is to liberate professionals from the menial so they can focus on the meaningful in this age of audio and video. We want to make people's work joyful again by unlocking the power of speech. Our platform uses A.I. to automatically transcribe audio and video, making it easy to find the moments that matter and connects teams for seamless, fast and secure content creation.

Our Security Mission

Trint's security mission is to protect our customers and safeguard their data through best-in-class security. Our deep concern for security was born out of our background in journalism and our team has always been supported and enriched with professionals from the media sector. Because journalists often handle sensitive material, sources and information that requires the strictest confidentiality, privacy is central in everything they do. And as such, it's central in everything we do. That same vigilance in protecting private information is in Trint's blueprint and informs our culture, decision-making and corporate posture.

In a world of data breaches and cyber attacks we understand the risk that comes with sharing your information and we know how important it is to keep it safe, which is why we don't rely on a single layer of defense. From scanning to testing, our security program is based on defense in depth with multilayered security controls. We comply with privacy regulations and draw on best practice from information security standard, ISO27001:2013, the north star in security practices and culture. We take every possible step to keep your information and data safe. This guide to Security at Trint outlines our approach to adhering to these principles and our commitment to continually reviewing, adapting and improving our security posture.



Want to easily transcribe phone calls?

No more recording devices, no more painful workarounds. Download Trint's iOS app to record and transcribe calls, all in one place.

Contents

Our people and culture

Security starts and ends with people. World-class technology, the best providers and bullet-proof processes are only as strong as the behaviors, practices and readiness of the people supporting them. It's with this in mind that we take extra care when it comes to your security and our people.

To create a structure of accountability, we set up an infosec team to continually review and improve our information security, and help our people understand their role in maintaining our strong security posture. Headed up by our Chief Technology Officer (CTO), the team is also supported by our experienced leaders across the company, from engineering, finance and executive management.

Vigilance through awareness and culture

This structure of accountability directly informs our culture of ongoing awareness and shared responsibility. Trint employees, who must all pass background checks prior to employment, are briefed during onboarding on their security and privacy responsibilities. But we don't stop there. Trint employees are continuously trained and tested with monthly refreshers, phishing simulations and security tips.

Security is a team effort at Trint. Employees report potential security risks and incidents through internal channels to enable our infosec team to address them quickly and early. Communication is visible across the organization for transparency and continued learning.

Trint invests in additional training for specific team members as required for broader awareness and security. For example, Trint developers are trained in secure software development principles in line with standards such as OWASP.

Our policies and practices

No one sees your data but you!

Data security is a given, but for Trint it goes beyond processes and procedures. It's in our DNA. From leadership to marketing, commercial and engineering, protecting your data is at the center of everything we do. We handle sensitive and confidential files everyday, so maintaining the highest levels of security is an absolute must, which is why our golden rule is that no one sees your data but you. We don't use customer data to train the speech-to-text algorithm and Trint employees are prohibited from accessing data. In exceptional cases, and only with express written consent from a client, is a small, pre-authorized, Trint cohort able to access respective customer data.

Safeguarding physical security

Despite living in the age of cloud computing, physical security is no less important. We've adopted practices and policies to secure our office environment and safeguard access to devices and wifi, by giving employees designated electronic access cards, screening and logging visitors and securing our offices with 24/7 CCTV. In the office we stick to a strict clear desk and locked device policy.

We also take measures to protect Trint devices. Every laptop is secured by software tools to monitor cyber threats and reinforced by full-disk encryption. When working remotely or travelling, Trint devices are protected by VPN which encrypts data over public wifi, blocks tracking and makes regular changes to the device IP address.

Controlling access

Each business system requires access permission from an employee's line manager and system administrator, submitted centrally for approval and recording. Once access is provided, employees must use password management tools to generate unique, high-complexity passwords. Single sign-on using corporate credentials and 2-factor authentication are used whenever possible. When an employee leaves Trint, system administrators remove access as part of the off-boarding process. Users are periodically reviewed so that only active and appropriate Trint employees retain access.

Ensuring business continuity

In order to provide a consistent and reliable service for our customers, we have adopted processes for business continuity, disaster recovery and backup. Since most of Trint's platform is delivered online as software-as-a-service (SaaS), the risk of service disruption is minimal. Trint's platform is hosted across multiple data center regions for performance, availability and redundancy. We've also set out steps to reduce the risk of losing access to our physical environment and if needed, quickly secure new office space, so employees can continue to work safely.

Trint customer data is hosted on Amazon Web Services (AWS) cloud platform, which offers best-in-class disaster recovery policies. Their industry-leading business continuity plans cover a range of potential risks from data recovery to water damage and outages, ensuring our customers will be able to continue to use Trint in the face of disaster. You can check AWS business continuity and disaster recovery plans, for more information.

Our infrastructure-as-code and backup policy means we can automatically reproduce environments should a disaster occur and the Trint platform need rebuilding. We can hit a recovery time objective (RTO) within 24 hours and recovery point objective (RPO) of just four hours. We don't expect it, but we are prepared for it.

Working with suppliers

From time-to-time Trint works with third-parties to provide services to customers and we take the same risk-based approach as with every other part of our business. Each supplier goes through a rigorous assessment of their security and certifications, while cross-checking the sensitivity of our data against regulatory constraints, ensuring there is no considerable risk to our business or customers. Where opportunity arises, we work with suppliers to improve their security practices.

Separation of duties

From access control management and autiding our information security management system (ISMS), to releasing new code and network infrastructure, Trint separates duties, tasks and privileges across the organization to mitigate risk, fraud and errors.

Controlling change

We've also put in place standard processes to manage change control for our software and the Trint SaaS platform, the network and to the compute infrastructure so that only appropriate and approved changes are permitted. We apply this process thoroughly so new package installations, changes to systems made during development and all new software go through code review and testing before deployment.

Continuous improvement

Our policies and the practices they promote are under constant review, testing and measurement. This security posture is refined on an ongoing basis through internal audit, our annual risk assessment, management reviews or other sources such as customers, vendors or data from operational systems.

Regulatory compliance and certifications

Compliance is a key business priority and we're constantly reviewing how we measure up against evolving and new standards and regulations.

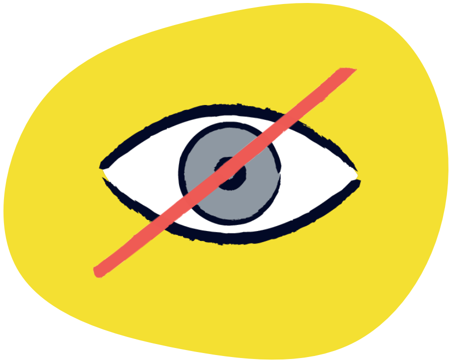
Data protection compliance

As regulations and legislation become more sophisticated and expand around the world, Trint is committed to maintaining the highest data privacy standards. We've implemented our own non-regression policy to adhere to the spirit and requirements of data legislation, even if we're not required to comply. That goes for legislation like the California Consumer Privacy Act (CCPA) and includes the United Kingdom's departure from the European Union (EU).

GDPR

Trint is fully compliant with the EU General Data Protection Regulation (GDPR). When it comes to our customers' data, we believe in transparency and accountability. Scrutinizing our data collection and retention policies has meant we've been able to eliminate unnecessary data collection and maintain data storage best practice. We've published clearly written policies so that customers and prospects understand how we process their data and can easily submit data subject access requests.

But GDPR compliance is never "done". We're continuously reviewing our posture and the way we work, to ensure we're fulfilling the Regulation's principles of lawfulness, fairness and transparency.



Certifications

As a commitment to compliance and to transparently share our security posture with our customers, we've also invested in attaining relevant security certifications.

ISO27001:2013

Trint's early adoption of ISO27001:2013 speaks of our commitment to information security. Certifying at such a young age shows how much we value the principles of strong security.

Implementing our ISMS has allowed us to control any weaknesses and eliminate the risk or damage being passed on to our customers. Applying information security best practice means we're continually monitoring and reviewing our policies to ensure they meet the needs of both our customers and organization. Risk assessments and internal audits help to identify, evaluate and address vulnerabilities in our information security processes on an ongoing basis.

Additional accreditations

We've also taken steps to self-attest to the Payment Card Industry Data Security Standard, (PCI DSS), that standardizes security around credit card payments. Additionally, we achieved Cyber Essentials certification, the information assurance scheme developed by the UK government's National Cyber Security Centre, attesting that Trint's security defences protect against the overwhelming majority of common cyber threats.

While compliance and certifications are important benchmarks, they're never complete in our view and we do not rest on certificates alone.

We know our users need to trust us. That's why we have military-grade data security. ☑

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Information Security Management ISO 27001 Certified

Crown Commercial Service Supplier

THIS REGISTRATION IS MAINTAINED BY US FEDERAL CONTRACTOR REGISTRATION Verified Vendor

CYBER ESSENTIALS

Our product

Helping you control access

Trint helps our customers and users stay secure by proactively building features and capabilities into our platform. Enterprise customers can integrate Trint with corporate identity management systems and protocols such as Active Directory, Security Assertion Markup Language (SAML), and Single Sign On (SSO) to secure access at an account level. Team leaders and managers can set user roles and permissions to control access to content and capabilities. We also work with customers to support their custom retention policies and litigation hold needs to help their own information security and compliance policies.

Continuously testing

To safeguard access to our platform, we use a third party to carry out penetration tests of our software. This helps to spotlight vulnerabilities and gives us a head-start at remediation. Prospective Enterprise clients may request an executive summary of our most recent penetration tests.

As an extra dimension to testing we run an ongoing bug bounty program that incentivizes security researchers from around the world to find and disclose any vulnerabilities through our responsible disclosure process. If vulnerabilities are found, we work to fix issues quickly, based on severity. These security professionals add a layer of crowd-sourced vulnerability monitoring that further reinforce our testing and security. Trint's vulnerability disclosure program can be found at: https://hackerone.com/trint.

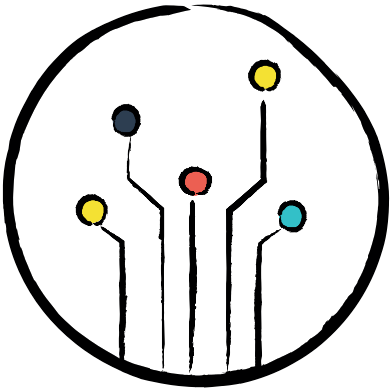
Our infrastructure and data centers

Hosting the platform

We host our platform on Amazon Web Services (AWS) and as the leader in cloud computing, they set the benchmark for cloud security. Trint is responsible for all data stored on AWS and we set our own policies for encryption, transfer and retention. In addition to AWS's automatic encryption, we add a further layer of encryption to secure data in transit and at rest using TLS encryption, (e.g. TLS 1.2 and AES 256), to protect data from unauthorized access or interception. In addition to cloud security, AWS guarantees stringent measures on site to control physical access to data centers.

Securing the network

To protect customer data, Trint segregates systems into separate networks, limiting the damage in the unlikely event of a breach. Trint's network architecture is protected by ring-fenced firewalls around the network perimeter, supported by intrusion detection to monitor unauthorized attempts to access our systems. Our network architecture is expressly designed to limit access and protect data. It's supported by fundamentals like separating company networks between employees and guests, blocking access to Trint's platform network for non-employees, while also designing a tiered network architecture that separates access and protects data. These components in tandem are secure by design. The tooling allows us to monitor for anomalous system behavior and potential data exfiltration.



To Conclude

When it comes to protecting our customers' information, we know we're fussy, but if our customers trust us with their data, it's down to us to keep it safe. From day one, security has been baked into everything we do here at Trint, from training our teams in security best practice, to implementing an ISMS and securing our networks.

We're always on the lookout for ways to improve and we work hard to maintain our strong posture. It's down to our background in journalism that we're so dedicated in ensuring that the information we hold is safeguarded at the highest level. We're set on keeping our customers and our team safe. If you have any questions or want to chat through our security, you can reach out to our sales team for more information.

2021

trint

Security is our priority.
We always keep your data safe.

To discuss an Enterprise contract, please get in touch at sales@trint.com

Crown Commercial Service Supplier

Information Security Management ISO 27001 Certified

bsi ISO/IEC 27001 Information Security Management CERTIFIED

This registration is maintained by US Federal Contractor Registration Verified Vendor

CYBER ESSENTIALS

UKAS MANAGEMENT SYSTEMS