rewind



Security Whitepaper

Rewind's security practices

Rewind is built from the ground up with a "security first" ethos. As experts in data backups, security isn't just a feature. It's at the core of what we do. We are happy to share our security practices to provide assurance in our processes and procedures.

Rewind has implemented a robust Information Security Program.

Security and compliance

- SOC 2® Type 2: Rewind has implemented a security compliance program including security controls, policies, and practices that are validated through regular external audits by AICPA's SOC for Service Organizations Trust Services Criteria. Rewind's SOC 2 report can be reviewed subject to the signing of Rewind's non-disclosure agreement at security.rewind.com
- SOC 3®: Request access to view Rewind's SOC 3 report here

Policies and procedures

- An information security program is in place which includes formal policies and procedures based on best practices such as the NIST Cybersecurity Framework
- Information security policies are reviewed at least annually and approved by senior management
- Employees review and sign Rewind's information security policies upon hire or after any material change
- Our information security program is audited by an external third-party auditor for continued success with Rewind's SOC 2 assessments

Risk management

- A formal risk management program is in place to identify and remediate security threats, vulnerabilities, and risks to business continuity
- Independent risk assessments are performed annually. Risks are registered in Rewind's Risk Register with mitigation plans and owners assigned
- Risk register reviews are performed on a periodic basis with senior management

Vendor security

- All third-party vendors undergo a vendor risk assessment prior to being onboarded. In this assessment, Rewind assesses the vendor's security and privacy practices and business reputation
- Onboarded vendors are reassessed annually or in the event of any major changes to their business
- Rewind uses sub-processors to assist in providing our products and services. A sub-processor is a third-party data processor who, on behalf of Rewind, processes personal data
- See Rewind's sub-processor list here

Incident response

- Rewind has an incident management policy and procedures in place
- Rewind's Trust Team is responsible for incident response coordination with 24/7 on-call employees available for incident response
- A communication plan is in place to inform customers of any incident that may impact their data

Rewind protects your data and complies with relevant privacy legislation and regulations.

Data privacy and security

- At Rewind, we take a privacy by design approach in implementing privacy in all aspects of our organization
- We have a dedicated Trust Team who are responsible for the privacy program. They implement internal policies and key privacy initiatives to ensure compliance with data protection legislation, such as GDPR, advising on privacy matters, liaising with data subjects and the national Data Protection Authority
- Rewind offers data residency options across multiple geographical locations, such as US, UK, Europe, Australia, and Canada for compliance with requirements like GDPR
- If you have a requirement to have backup data stored in a different geographic location, you can contact our team and we can work with you to store your data where needed
- A retention procedure is in place to securely delete customer backup data at defined periods after termination
- Read Rewind's Policy on Data Retention and Disposal of Customer Data here
- Our privacy notice describes our privacy commitments to our customers and website visitors and explains how we collect, use, and process your personal data when you use our services
- Our Data Processing Addendum (DPA) provides our commitments related to data processing, international data transfers, and our commitment to GDPR compliance

At Rewind we are dedicated to ensuring our employees are confident and empowered to work securely.

Personnel security

- We apply the “least privilege” model meaning we assign access to employees based on role and the absolute least access someone needs to be able to perform their duties. Access is reviewed on a periodic basis
- Background checks are performed on employees including criminal record and employment history

Personnel security cont.

- Security awareness training for all employees takes place upon hire and quarterly
- Social engineering tests take place on a continuous basis
- Employees sign employee confidentiality and proprietary property agreements and must abide by Rewind's code of conduct
- Rewind employees are empowered to be responsible for security controls in their business units as part of Rewind's SOC 2 program
- When an employee leaves Rewind, their access is revoked following revocation processes

Building secure applications is at the heart of what we do.

Product security

- We require two-factor authentication (2FA) for all users for all systems that support 2FA (code repositories, build systems, and cloud providers)
- Our internal systems are only accessible over a VPN
- To ensure confidentiality of data within the Rewind service, customers are prevented from accessing other customers' data through appropriate segmentation controls. All customers receive their own tenant of the Rewind service and their data is logically separated and not accessible to other tenants to prevent unauthorized access
- All infrastructure used by the product is defined as part of an infrastructure as code model and held under version control which requires several levels of review for any changes made
- Where applications need to communicate with external services using credentials, the credentials are stored encrypted in a vault out-of-band from the service itself and any build or deploy systems we use
- For sensitive data like platform access tokens, we encrypt these with a second key within the database. This means that even applications and humans that can query the database must be able to decrypt the access keys in order to communicate with a platform. The key itself is stored encrypted and only accessible by applications that require it
- We maintain a patch management process to ensure the timely installation of patches and updates. In addition, production systems are scanned to test for patch compliance on a periodic basis

Secure software development

- We utilize industry standard tools to ensure we are writing secure code
- Based on roles and responsibilities, only authorized employees are granted access to promote changes in production environments. All changes follow the change management process prior to deployment
- We have a thorough onboarding process for new developers
- Developers are continuously trained on secure software development best practices, such as OWASP Top 10 and secure coding standards

We host Rewind on Amazon Web Services (AWS), the most secure infrastructure provider on the planet.

Physical security

- The Rewind application is hosted within AWS "secure by design" data centers
- Read more about the security of AWS data centers
- Rewind's office buildings have physical security and access controls in place such as CCTV and on-site security officers. Access to the building and office is limited to employees with approved access and controlled via access cards

Data is secured in transit and at rest.

Encryption

- All data at rest in our databases, cache services, or other data stores is encrypted using standard AWS encryption mechanisms – typically AES 256
- For data in transit across the network, all communication takes place using HTTPS (encrypted) connections. We use a certificate with a 2048 bit key size on all of our Rewind endpoints and certificates are rotated yearly

Rewind performs continuous security testing on our applications.

Security testing and monitoring

- An external third-party performs penetration testing on Rewind's applications and external network on a periodic basis
- Vulnerability scans are performed on Rewind's applications on a scheduled basis and automatically when new threat definitions are updated
- Monitoring and alerting is configured on Rewind's network to alert for any anomalies or suspicious activity
- Rewind has an Intrusion Detection System (IDS) in place to monitor and alert for suspicious activity
- Rewind's on-call teams are available to respond to security alerts 24/7
- Through our vulnerability disclosure policy (VDP), we work with external security researchers and examine all submissions and remediate where required (a bug bounty program)
- Logging is enabled and logs are stored in a centralized logging system accessible only to authorized employees
- Rewind is continuously monitoring for supply chain vulnerabilities and notifications will be posted at security.rewind.com

Security of customer content

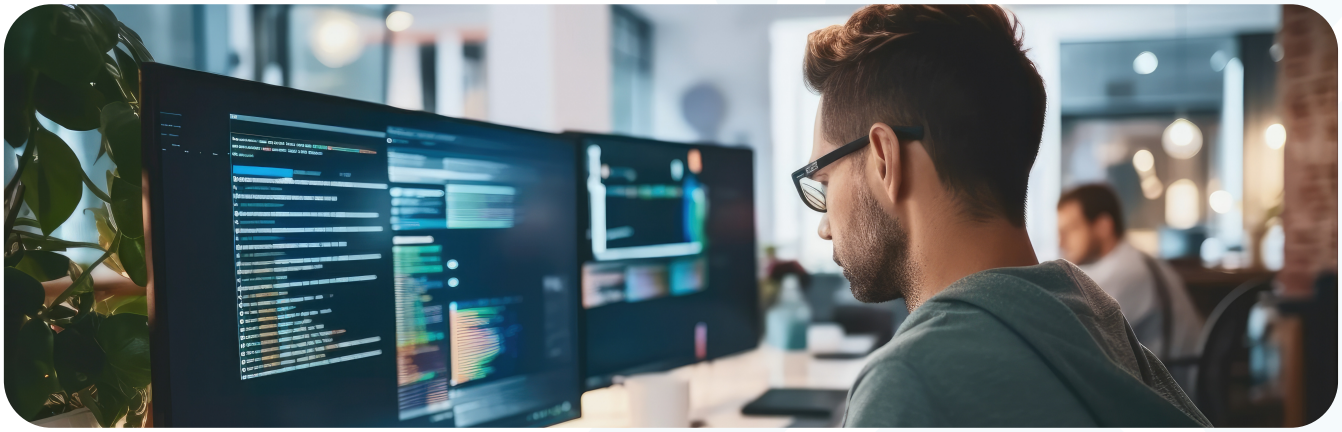
- Rewind access to customer backup data is restricted to key roles and under the principles of least privilege and roles based access controls in order to assist customers with backup or restore issues. Access to customer data is managed via multiple layers of security best practices and controls
- Backup data is securely stored in AWS S3 storage. S3 versioning is enabled for resilience
- Backup data cannot be modified. Data is retained, and then deleted, in line with Rewind's Policy on Data Retention and Disposal of Customer Data

Built by data protection specialists

- Rewind is built from the ground up with a "security first" ethos across all roles. All Rewind employees complete security training quarterly, with regular role specific training, such as OWASP top 10 for developers and privacy training for Marketing teams
- Rewind also has a dedicated Trust Team who are committed to enhancing our security and privacy programs to ensure Rewind's programs are in line with industry best practices
- Rewind's Trust Team specialize in key domains across application security, data privacy, cloud and network security, GRC and IT security. Holding gold standard industry certifications and awards such as: CISSP, CCSP, SSCP, CIPM, CIPP/E, CIPP/C, CRISC, ISO 27001 Lead Auditor, AWS Certified DevOps Engineer - Professional, AWS Certified Security - Specialty, CISM, CEH

Network security

- Network diagrams are available for review in Rewind's SOC 2 & SOC 3 reports
- All network infrastructure is provisioned by infrastructure-as-code tooling and requires review for configuration changes
- AWS security groups with minimal access rules are used to secure all load balancers and AWS services
- S3 buckets are private with no public inbound access permitted
- Rewind utilizes AWS multi-tier architecture including logically separated VPC's (Virtual Private Cloud), VPC endpoints, and NAT gateways

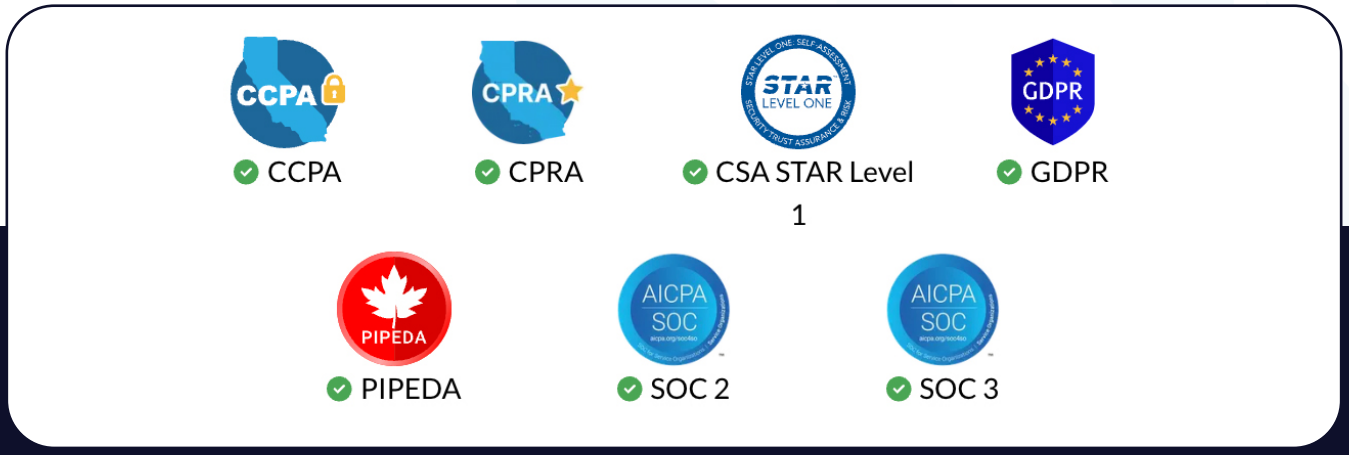


Availability and disaster recovery

- At Rewind, we prioritize data resilience by performing bi-annual disaster recovery tests, ensuring that our backup systems are always ready to respond to any unexpected events and that our customers' data remains secure and accessible
- Disaster recovery testing involves executing technical runbooks to ensure correctness along with table-top testing of various disaster scenarios to ensure procedures are correct

Account security

- Rewind keeps your data safe against online threats. Your Rewind account can be protected with 2-factor authentication via a third-party authenticator application, such as 1Password or via the use of a hardware token, such as Yubikey
- Rewind supports single sign-on (SSO) for improved access control and security for your Rewind account. Rewind uses Security Assertion Markup Language (SAML), which is an SSO login method offering more secure authentication (with a better user experience) than usernames and passwords
- Rewind will support SAML-based identity providers (IdPs) such as Okta, OneLogin, Auth0, and more
- Rewind contains a full audit log, viewable and searchable by users allowing monitoring of activity related to their organization's users, plans, and content. It tracks common actions such as user authentication, administration activities, and vault actions such as backups, restores, and exports
- Rewind administrators can manage who has access to their instance of the Rewind app by adding, inviting, and removing users to their Rewind organization. This is done in the Member Permissions area of the Settings menu



Ready to begin protecting your SaaS data?

Start your free trial of Rewind or get in touch at sales@rewind.com to inquire about custom backup bundles for your organization.

rewind