Rewst Security & Compliance FAQ Responses

Rewst develops and delivers SaaS products that provide our customers with a Robotic Process Automation platform for automating workflows. Recognizing the need by many of our customers to satisfy vendor due diligence questionnaires, the following responses have been prepared by our security and compliance team.

If you have additional questions, please work with your Rewst point of contact to submit them for a response or contact our security team. To request a copy of the most recent SOC 2 Type 2 audit report, please visit our Trust Center to begin the process.

security@rewst.io

GENERAL SECURITY PROGRAM INFORMATION

Does your information security program align with industry standards or frameworks?

Rewst is SOC 2 Type 2 certified and aligns our information security program with NIST Cybersecurity Framework (NIST CSF). In addition, we have been successfully audited by a third-party for GDPR compliance.

Do you have a formal Information Security Program in place?

Yes, Rewst is committed to implementing cybsersecurity best practices in both our internal IT systems, as well as our Rewst application and associated services.

Do you have a formal authorization process that restricts and controls privileged access rights?

Yes, more information on our process is documented in our SOC 2 Type 2 report.

Last Updated: 8/04/2025

Do you have a formal process whereby asset owners review users' access rights at regular intervals?

Yes, more information on our process is documented in our SOC 2 Type 2 report.

Is your Privacy Notice/ Privacy Policy externally available?

Yes, policy is publicly available on our website: https://rewst.io/privacy-policy/

DATA HANDLING

How do you encrypt customer data?
Data encryption both at-rest and in-transit, more detailed findings are included in SOC 2 audit report, available in our Trust Center.

Do you have a formal process for the removal of data at the end of the engagement?

Yes, we collect, retain, and use collected data in accordance with our publicly available Privacy Policy. Details on data rights and erasure timelines can be found in this document as well.

Does your organization have a Disaster Recovery Plan?

Yes, Disaster Recovery Plan (DRP) is in place. Plan is considered internal/confidential and is not available for distribution to external parties. However, it is included in our SOC 2 Type 2 audit with an independent third-party to ensure that required continuity, disaster recovery, and security controls are met.

Does your organization have an Incident Response Plan?

Rewst has an incident response process, which includes escalation procedures, rapid mitigation, and clear communication.

Last Updated: 8/04/2025

Policies

Are all personnel required to sign Confidentiality Agreements to protect customer information, as a condition of employment?

Yes, required prior to start on first day of employment.

Are all personnel required to sign an Acceptable Use Policy?

Yes.

Do you have an access control policy in place?

Yes, Rewst has access control policies in place that are based on the principles of role-based access and principle of least privilege.

Security Program Solutions and Vulnerability Management

Is MFA required for employees to log in to production systems?

Yes, MFA is strictly enforced on all production systems.

Does Rewst regularly evaluate patches and updates for your systems, infrastructure, and code vulnerabilities?

Yes, we have an in-depth vulnerability identification and remediation process in place.

How do you ensure code is being developed securely?

Throughout the development process, Rewst has integrated security tools and processes including, but not limited to automated DevSecOps code tests/checks, static and dynamic code testing reviews - SAST & DAST, secrets scanning, dependency security review, and code update (PR) change management processes. Rewst also utilizes third-party pentesting services to test web application security.

Vulnerability Disclosure Program (VDP)

We have partnered with Bugcrowd to manage our vulnerability disclosure program. The Bugcrowd platform allows us to collaborate with security researchers and responsibly address any potential security issues. To learn more, please visit our vulnerability disclosure program page:

https://www.rewst.io/vulnerability-disclosure/

Do you perform logging and monitoring?

We continuously monitor and log activities across various cloud services, including, but not limited to our Microsoft and Amazon AWS.

Do you have a security awareness training program?

Yes, Rewst has a continuous security awareness training program with metrics reported to management and also conducts internal simulated phishing campaigns on employee accounts.