

# Security Program

We know your data is sensitive. That's why Rippling combines enterprise-grade security features with regular audits to ensure you're always protected.



## Table of Contents

<b>01</b>	<b>Rippling security organization and program</b>	<b>3</b>
<b>02</b>	<b>Personnel security</b>	<b>3</b>
<b>03</b>	<b>Product security</b>	<b>4</b>
<b>04</b>	<b>AI security and governance</b>	<b>5</b>
<b>05</b>	<b>Cloud and infrastructure security</b>	<b>6</b>
<b>06</b>	<b>Vulnerability management</b>	<b>6</b>
<b>07</b>	<b>Security monitoring and incident response</b>	<b>7</b>
<b>08</b>	<b>Physical security</b>	<b>7</b>
<b>09</b>	<b>Business continuity / disaster recovery</b>	<b>7</b>
<b>10</b>	<b>Security risk management</b>	<b>8</b>
<b>11</b>	<b>Security compliance</b>	<b>8</b>

# 01 Rippling security organization and program

While security is a high priority for all teams, a dedicated Security Team manages the Rippling security program. Our security framework is based on ISO 27001, industry best practice security standards, and includes policies covering: data classification, access management, cryptography, change management, secure server configuration, physical security, business continuity, vendor assurance, vulnerability management, security monitoring, and incident response. Security is represented at the company's highest levels, with our Chief Security Officer meeting with executive management frequently to assess risk and coordinate company-wide initiatives. Information security policies and standards are approved by management and available to all Rippling employees.

## 02 Personnel security

The people building and maintaining Rippling products are our most precious assets. We've implemented processes to ensure we're bringing in the right people and keeping them up to date on the latest security trends. Here are some of the procedures we have in place:



### Onboarding/offboarding process

We use Rippling software to automate account provisioning, onboarding, and offboarding in compliance with ISO 27001.



### Interviews, background checks, and confidentiality

Applicants must be interviewed before acceptance and, where permitted by law, employees must undergo background checks by a specialized third party. Additionally, all employees are required to sign confidentiality agreements.



### Legal and infosec training

All new employees attend legal and security training during the onboarding process. In addition, all employees go through information security training once per year. The material is produced in-house and covers information security policies, security best practices, and privacy principles. Any non-compliance is subject to our documented disciplinary process.



### Continuous security education

The Rippling Security Team provides continuous education on emerging threats, performs phishing awareness campaigns, and communicates with the company regularly.

## 03 Product security

### Application security

The mission of the Product Security program is to enable product teams to build solutions that are best in class when it comes to security. The following activities help us to achieve this mission:

- Internal security reviews before products are launched
- Regular threat modeling exercises
- Regular penetration tests performed by reputable third parties
- An invite-only bug bounty program

### Change management

Through a formal change management process, changes to Rippling software are tracked and approved. Changes are also tested in accordance with our change management process. Rippling also has logging and monitoring in place to detect unauthorized changes to production systems.

### Data security

Rippling encrypts data in transit and at rest.

- **Encryption in transit:** All data sent to or from Rippling infrastructure is encrypted in transit using Transport Layer Security (TLS).
- **Encryption at rest:** All user data is encrypted in the database using the AES-256 encryption standard.

Rippling also has a documented Data Classification and Handling policy used to categorize Rippling's stored information based on its sensitivity level, ensuring proper handling and lowering organizational risk.

### Penetration testing

We partner with reputable security companies to perform regular penetration tests on Rippling applications and infrastructure. Our invite-only bug bounty program encourages ongoing testing and responsible disclosure of vulnerabilities by the security community.

### Platform monitoring and protection

We have deployed an array of solutions to monitor and protect our platform and applications, including:

- Technologies to monitor exceptions and detect anomalies in our applications
- Collection and storage of logs to provide an audit trail of activity
- Network security controls to automatically block identified attacks and anomalous activity
- Security headers to protect our users from attacks

### Account security

Rippling monitors authentication events. Alerts are triaged by our Security Team and investigated. Moreover, we protect users against data breaches by monitoring and automatically blocking brute-force attacks.

Customers can add another layer of security to their accounts by enforcing multifactor authentication to access the Rippling console.

## 04 AI security and governance

Rippling uses artificial intelligence (“AI”) throughout its platform to help customers work more efficiently, reduce manual effort, and streamline workflows. AI features are powered by foundation models from OpenAI and Anthropic, who are appointed as sub-processors under Rippling's [Data Processing Addendum](#).

The following controls govern Rippling's AI security and governance posture:



### Data protection

Customer data processed through AI features is not used to train or fine-tune any underlying model. This is enforced contractually with all AI sub-processors. Where feasible, Rippling enables zero data retention or other limited data retention configurations with these providers to prevent durable storage of customer data after processing.



### Permission-layer enforcement

AI features operate within the same role-based access control framework as the rest of the Rippling platform. Every AI response is strictly scoped to what the requesting user is already authorized to access. Customer data is never shared across customer environments.



### Human oversight

Rippling's AI features are designed to keep humans in control of consequential decisions. Rippling does not use AI to independently or autonomously make final decisions on hiring, compensation, or other high-stakes matters without meaningful human review.



### Transparency

Users are informed within the Rippling product when they are interacting with AI, and all AI-generated output is clearly labeled as such in the user interface.



### Accuracy and bias testing

All AI features undergo robust testing for accuracy, consistency, and bias mitigation before and after deployment.



### Pre-release review

Before release, all AI features are reviewed by Rippling's Legal, Privacy, and Security teams to assess privacy impact, model risk, and data protection controls. This includes structured risk assessment and mitigation processes applied throughout the AI system lifecycle.



### AI Management System

Rippling's AI governance framework is certified under ISO 42001, ensuring structured oversight, accountability, and continual improvement of AI-related controls. Rippling's governance approach also aligns with the NIST AI Risk Management Framework (RMF) and key principles of the EU AI Act and other applicable AI regulations.

For more information regarding how Rippling uses, protects, and governs customer data in connection with our AI features, please see [Use of AI at Rippling](#).

## 05 Cloud and infrastructure security

Our cloud security program is driven by a defense-in-depth approach.

Rippling's production environment employs defensive security controls at all layers of its infrastructure, such as:



### Network segregation

Minimal network access to Rippling production networks is granted.



### Identity and access management

Rippling follows a least-privileged approach to manage access. Role-based access control is enforced and MFA is required at all entry points into the production environment.



### Audit trail

Rippling stores an audit trail for all access activity within its production services.



### Intrusion detection systems

Intelligent threat detection is configured along with automated data driven protection.



### Security events monitoring

Infrastructure activity is continuously monitored via automated tooling.



### Cloud configuration monitoring

Continuously monitored for adherence to security best practices. We leverage automation to identify any deviation from our technical standards and raise issues within minutes of the configuration change.



### Asset management

Critical cloud assets in Rippling's infrastructure are inventoried. Assets must have a defined owner, security classification, and purpose.

## 06 Vulnerability management

The Vulnerability Management program establishes how Rippling identifies, responds, and triages vulnerabilities on our platform. The program includes the following initiatives:

- Continuous automated scans of the Rippling platform
- Regular sync with Engineering Leadership on vulnerability ownership and remediation
- Vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process
- Remediation service-level agreements (SLAs) defined according to the severity associated with the vulnerabilities discovered
- Issues identified by 3rd party penetration tests and our Invite-Only Bug Bounty Program are triaged as part of our vulnerability management program

## 07 Security monitoring and incident response

### Continuous monitoring

Through the ongoing awareness of vulnerabilities, incidents, and threats, we can quickly respond and mitigate accordingly. Rippling leverages a comprehensive collection of application, infrastructure, and software-as-a-service (SaaS) log sources to identify and triage possible security events.

### Incident response program

Rippling manages an incident response program in line with industry best practice standards. The program defines requirements under which security incidents are classified and triaged. The Rippling Security Incident Response Team evaluates the threat of all applicable vulnerabilities and security incidents and establishes remediation and mitigation responses for all events. The incident response process has precisely defined roles and responsibilities to ensure that any incident is triaged efficiently after detection, and mechanisms for evidence collection that preserve confidentiality.

Rippling has also established a dedicated Customer Trust and Safety team within the Security organization. This team operates at the intersection of Security, Privacy/Legal, and Customer Experience, handling incident response for high-impact events, platform policy enforcement, and customer recovery coordination.

## 08 Physical security

We leverage best-in-class third-party data centers for all production systems and customer data. These service providers follow industry best practices and comply with a comprehensive list of security standards. All critical vendors, including data center providers are reviewed at least annually or after a major change to ensure their controls meet our security bar. Rippling also has a clear desk policy that is included as part of both our new hire and annual security training.

## 09 Business continuity / disaster recovery

Rippling leverages robust third-party cloud computing platforms and adherence to configuration best practices to ensure best-in-class resiliency.

### Data backups

Rippling performs continuous backups of critical data (including customer data). Our production database clusters are replicated across multiple availability zones.

### Disaster recovery

We maintain a formal disaster recovery process. The disaster recovery plan is tested on a yearly basis.

## 10 Security risk management

Rippling has adopted a fully embedded approach to Security Risk Management based on the ISO 27001 standard. On an annual basis, or after a major change, Rippling undergoes a full scope risk assessment that follows our documented risk assessment and treatment process. Risks are assigned owners and the risk register is used to influence company-wide quarterly planning.

Third parties are assessed before onboarding to validate that they meet our security and legal requirements. Once a relationship has been established, Rippling reviews security and business continuity concerns periodically. This is performed by our internal third party risk management team who also leverages automated monitoring tooling.

## 11 Security compliance

Rippling complies with applicable legal, industry, and regulatory requirements as well as industry best practices. Customers and prospects can self-serve access to audit reports, certifications, and data protection documentation via Rippling's Security & Trust Center at [trust.rippling.com](https://trust.rippling.com). We hold the following certifications and attestations, which are all audited annually:

- SOC 1 Type II
- SOC 2 Type II
- ISO 27001
- ISO 27018
- ISO 42001
- CSA STAR Level 2

Rippling does not store, process, or transmit cardholder data directly. Our vendors that handle cardholder data are required to be PCI DSS compliant, ensuring that credit card data is protected in accordance with the Payment Card Industry Data Security Standard (PCI DSS).