The *Security for Saas CTOs* Checklist

Vanta

Data security is a critical risk for your business, with legal consequences and the loss of users' trust looming as a constant threat if a break occurs. As a CTO for a SaaS organization, you hold this vital responsibility in your hands, and you're under pressure to do everything you can to protect your users, your app, and your business.

There are so many measures to take to properly protect your security that it's difficult to know where to begin. Vanta has spent years helping businesses protect their data and their users, and our experts are here to help you simplify your security protocols too. Start with this information security checklist for SaaS CTOs.

STEP 1:

Secure your employees

- □ Educate your employees about good security practices and get them accustomed to following them.
- □ Set up encryption for all employee computers, phones, and other devices.
- □ Hire a security engineer (or a security engineering team) to oversee information security.
- □ Create policies requiring employees to follow basic security measures:
  - □ Locking their devices
  - □ Avoiding sharing their user accounts with anyone, including other employees
  - □ Using two-factor authentication whenever possible
- □ Create employee onboarding and offboarding workflows or checklists that include security measures like activating and deactivating access controls, wiping device data, and so on.
- □ Set up a password manager so employees are all using strong passwords and changing passwords regularly.
- □ Install monitoring software on employee devices so you can detect malicious or risky activity.
- □ Use centralized account management to keep track of each employee's permissions, such as by using Vanta's access control management.
- □ Build an office culture that respects and prioritizes security.

STEP 2:

Tighten the security of your company

- □ Adopt a policy of transparency about any user data you collect.
- □ Create a security policy and make it publicly accessible, and have an internal security policy as well.
- □ Use a password-protected WiFi network for your employees and do not allow access to anyone else.
- □ Consider each of your critical services and make sure they are all secured firmly.
- □ Inventory your company's assets and maintain it regularly for reference if an incident would arise.
- □ Protect your domain names with the appropriate security certifications.
- □ Secure your domain against domain name spoofing by buying similar or misspelled domain names.
- □ Develop a security incident response plan.
- □ Consider establishing a bug bounty program to pay individuals for finding and reporting security risks in your site or application.
- □ Maintain a portfolio of security tools that protect your company and regularly evaluate to make sure you're using the right tools for your needs.
- □ Use scalable security practices and tools that can grow with your business.

STEP 3:

Write secure code

- □ Design your SDLC with security as a priority.
- □ Use a trusted source for your cryptography.
- □ Create a secure code review checklist and require developers to follow it for all deployments.
- □ Implement a security tracking tool that includes security bugs.
- □ Establish an automated security process within your SDLC to ensure that no critical security checks are missed.
- □ Implement a security training course for all developers and engineers to complete when they are hired.
- □ Use a pre-production analysis tool to evaluate the security of every deployment.

STEP 4:

Secure your application

□ Create an automated security monitor as soon as your app is in production.

□ Hire a penetration testing service to identify security risks in your app.

□ Run containerized applications as an unprivileged user.

□ Use a RASP or other real-time protection service.

□ Maintain clear documentation of all code dependencies.

STEP 5:

Make your infrastructure secure

□ Implement encryption for all APIs.

□ Always keep your OS and Docker images up-to-date.

□ Use a cycle of continuous backups and testing each backup.

□ Set up monitors for any and all exposed services as well as internal services.

□ Develop logs that are clear and usable and make them centralized for developers to access.

□ Monitor traffic and use scalable infrastructure to protect against a DDoS attack.

□ Keep assets isolated at the network level to minimize access in the event of a breach.

□ Restrict internal services to necessary IP addresses.

□ Have a documented process for redeploying your infrastructure in case of an incident.

□ Regularly monitor your data points for irregularities that could signal an incident.

STEP 6:

Determine if you need to do a data protection impact assessment

- □ Make user privacy a priority and make this clear to users.
- □ Set minimum password requirements for security.
- □ Offer two-factor authentication for users and encourage all users to take advantage of it.
- □ Monitor user activity for red flags and potentially malicious activity.

Make your Saas security simpler with Vanta

Securing your application and your business is a start, but for your continued growth, many future clients and partners will require you to hold certain security certifications as well to verify your security. Vanta makes this process smoother and simpler with our automated security compliance platform. Learn about Vanta compliance automation today and let us help you protect your SaaS business.

Vanta

Vanta is the easy way to get SOC 2, HIPAA, ISO 27001, GDPR, and PCI compliant. Over 2,000 fast-growing companies trust Vanta to automate their security monitoring and prepare security audits in weeks instead of months. Simply connect your tools to Vanta, fix the gaps on your dashboard, and then work with a Vanta-trained auditor to complete your audit. We'll guide you throughout the process and help tailor your security monitoring and compliance to meet the needs of you and your customers. Vanta was founded in 2018 and is headquartered in San Francisco.

VANTA.COM