Information Security Policy

Security Team

The Reveal Security team is comprised of Reveal’s following staff:

- Alexandre Sadones (CTO)
- Antoine Moreau (Lead Engineer)

The team is responsible for carrying out all security policies and procedures. The team has a direct line to the CEO and can communicate with the CEO whenever they need to.

Security Officer Role

The CTO is the Security Officer. With that title, the CTO is responsible for creating and enforcing security policies and procedures; leading the monitoring, vulnerability management, and incident detection and response initiatives; and tracking and reducing risk organization-wide.

People Operations Security

Background Screens

All Reveal employees undergo background checks prior to gaining substantial access to customer data systems. Reveal may rescind an employee’s offer letter if their background check is found to be falsified, erroneous, or misleading.

When local law does not allow background checks, reference calls from at least 1 previous employer, ideally as many as possible, will be performed instead of background checks.

Security Awareness Training

Reveal employees and contractors are provided training on the company’s security policies and procedures during their first 30 days of employment and annually thereafter. All Reveal personnel are then required to acknowledge, electronically, that they have the attended training and understand the security policy.

Security Coding Training

Reveal employees and contractors in developer roles are provided with SDLC / Secure Coding training during their first 30 days of employment and annually thereafter. Software developers are trained in secure coding techniques, including how to avoid common coding vulnerabilities.

All such personnel are then required to acknowledge, electronically, that they have attended and understand SDLC training and OWASP Top Ten common coding vulnerabilities.

Acceptable Use Policy

Reveal's Acceptable Use Policy covers employee responsibilities and behavior for using Reveal systems, including devices, email, internal tools, and social media. Reveal employees must acknowledge in writing that they've read and will abide by the Acceptable Use Policy.

All of Reveal's security policies, including the Acceptable Use Policy, are presented to new employees during onboarding, and all employees are required to sign off that they have read all such policies.

Remote Work

Reveal employees who work remotely must follow these rules:

- All company-provided equipment and any equipment used to perform work must remain in the presence of the Reveal employee or be securely stored.
- VPN must be used for all connections with production infrastructure.
- All of Reveal's data encryption, protection standards and settings must be followed for company-provided equipment and any equipment used to perform work.
- The confidentiality, security and privacy of Reveal's customers must be preserved by ensuring that no unauthorized individuals may view, overhear, or otherwise have access to Reveal's customer data.
    - To enforce, all Reveal employees are required to use screen protectors or be conscious of "shoulder surfing" when working in public places like a coffee shop or airport. Reveal employees are further required not to teleconference with customers in public areas.
- All remote work must be performed in a manner consistent with Reveal's security policies.

Disciplinary Action

Employees who violate any Information Security policies may face disciplinary consequences in proportion to their violation. Reveal management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations, employees may face severe disciplinary actions up to and including termination.

Responsibility

The CTO is responsible for ensuring all Information Security policies are followed.

Last updated: 2021-08-23