Security Overview

Revision Date: February 12, 2024

Cloud Infrastructure

Data Security

Data is encrypted using industry-leading encryption standards

Data Retention

Customer data is retained and disposed of in accordance with Procurify's Data Retention and Disposal Policy

Database Backups & Recovery

Database backups are performed daily and systems are in place to protect the confidentiality, integrity, and availability of stored data.

Software Development Lifecycle

Procurify's Software Development Lifecycle (SDLC) combines Technical, Security, and DevOps expertise to streamline software delivery through automated Continuous Integration and Continuous Delivery (CI/CD) practices. This method ensures the efficient release of high-quality software solutions.

Business Continuity & Disaster Recovery

All essential data is stored remotely using commercial cloud providers with proper backup and redundancy processes in place. This approach is designed to minimize any disruption from physical incidents or disasters.

Incident Response

Procurify fields a Security Response Team (SRT) consisting of team members from key departments to manage security incidents.

Vulnerability Prevention

Vulnerability management is integrated into the Change Management Process.

Organizational Security

Access Control

Access to internal systems is granted on the principle of least privilege based on business needs, job roles, and functions

Authentication

Procurify's Security Policies enforce password and MFA requirements. Team members utilize a password manager to ensure unique and strong passwords.

Device Management

Procurify has implemented systems to manage and secure team member devices.

Security Awareness Training

Procurify's Security Awareness Training Program promotes awareness of obligations for maintaining information security and understanding of internal policies.

Governance, Risk, and Compliance

Security Policies

Procurify's Security Policies outline the responsibilities to ensure the security of its systems and service commitments.

Risk Management

Procurify maintains a Risk Management program with a detailed Risk Register that identifies risks, develops plans to address risks, and assigns ownership.

Vendor Risk Management

Procurify's Vendor Management Policy guides the execution, management, and termination of vendor and other third-party agreements. Due diligence activities are carried out prior to contract execution and on an annual basis thereafter.

Third-Party Penetration Testing

Procurify engages with a third-party vendor to conduct an application penetration test of the production environment at least annually.

Compliance Standards

Procurify is SOC 2 Type 2 and GDPR Compliant

Responsible Disclosure

If you have any questions, comments, or concerns, or if you wish to report a potential security issue, please contact security@procurify.com