WHITEPAPER

TRIFACTA

Trifacta Security Corporate Program

CONTENTS

INTRODUCTION

At Trifacta, we understand that data security can't be an afterthought. We've baked robust security protocols into the foundation of our products and our company culture so that as your organization scales its Trifacta usage, you can ensure your data will be protected.

Each year, Trifacta undergoes an independent SOC 2 (Type 2) review to prove the longevity of our security standards. Under an appropriate Non-Disclosure Agreement (NDA), Trifacta can share the audit report to demonstrate that Trifacta's security program is managed effectively across our business's divisions. Our security framework includes a rigorous set of management, operational, and physical security controls. We've designed our networks and access control policies such that only the minimum level of access is permitted to perform a required job.

We aim to be transparent in our data security policies, which is why we've outlined essential corporate-level security information below. However, we also understand that data security is often an on-going conversation and welcome the opportunity to answer any additional questions that you may have beyond the scope of this document.

Finally, we've created supplementary documents that describe how security is managed for our Google Cloud and AWS based SaaS solutions that you can access from the Trifacta security and trust center website. Trifacta products may also be implemented on your private cloud on Azure or AWS or even on your internal systems. In these cases, please reach out to a Trifacta team member to discuss your specific requirements.

GDPR Compliant

SOC 2 Type II Compliant

CCPA Compliant

Trifacta Security Program

Software Security Operations

Trifacta adheres to strict procedures from our information security management program in order to ensure secure product development, operations, and usage.

The program aims to reduce risk and support your business by providing:

- Software Development Life Cycle (SDLC) precise processes
- Continuous Integration and Continuous Delivery (CI/CD) toolchain hardening
- Static code analysis, vulnerability scanning and code review
- Container security scanning and immutability
- Cloud configuration and compliance audits
- Mandatory Multi-Factor Authentication
- Employe onboarding/offboarding procedures and audits
- Periodic access reviews and audits
- Change management procedures

This provides a secure process that allows developers to deploy secure code and infrastructure, while also providing guardrails for security best practices.

Monitoring and Alerting

Trifacta continually monitors assets for suspicious activity. Any suspected threats will be mitigated and/or alerted to relevant teams, if necessary.

Vulnerability Management

Trifacta has implemented a vulnerability management policy and program to identify, track, and remediate security vulnerabilities promptly.

- Every month, production application base images of the Trifacta Software are scanned for security vulnerabilities.
- Every quarter, vulnerability scanning for open-source components of the Trifacta Software is performed by an automated system
- Multiple times a year, Trifacta engages a third party to conduct penetration testing of the Trifacta hosted production environment.

For each case, Trifacta reviews and tracks security vulnerabilities to resolution.

We welcome security researchers that submit noteworthy and actionable vulnerabilities and honor responsible disclosure. Please reach out to security@trifacta.com to submit any security concerns you may have encountered.

Incident Response

Trifacta's incident response program ensures that Trifacta personnel are trained to respond effectively to any security incidents that affect Trifacta and its customers. The program's mission is to prevent or greatly reduce the impact that any security incident may have by providing a swift incident response to any unexpected security event involving Trifacta infrastructure and customer data. Blocker and critical incidents are tracked to resolution with appropriate measures to contain, mitigate, and resolve the incidents following Trifacta's change control process.

The Trifacta team reviews security incidents and identifies the need for system changes based on incident patterns and root causes. Additionally, although Trifacta has never had a security breach that has impacted any customer data, Trifacta performs a post-mortem and retrospective analysis on identified security threats to improve processes for an effective response to security incidents.

The incident response policies and procedures are continuously refined as part of all response activities, as well as through annual tabletop scenario testing. Trifacta also carries cybersecurity liability insurance as part of its overall risk reduction strategy.

Data & System Access

Trifacta employees' skills and competencies are evaluated as part of the onboarding process. Additionally, background checks are performed, where permissible by law, on employees prior to granting access to the Trifacta SaaS Systems production environment. Trifacta personnel may not access customer data without prior customer approval. Designated Trifacta support personnel are only granted limited access solely to the extent necessary to address a customer technical support issue and then only upon request.

Trifacta uses a centralized directory solution to manage authentication and authorization of users to internal systems. User access is disabled upon the employee's termination.

Risk Identification and Mitigation

At least once per year, Trifacta performs a risk assessment to identify information security risks related to identified information assets, to assess the impact and probability of the risks, and to determine how the risks should be managed. The risk assessment process includes a third-party threat and vulnerability assessment, analysis of fraud factors, and the impact of fraud risks on achieving objectives.

Compliance

Trifacta is committed to maintaining compliance with applicable regulatory and established security industry standards. We undergo an annual, independent SOC 2 (Type 2) review, and the audit report can be provided by request under NDA to all existing and prospective customers.

The audit report complements the benefits of the comprehensive set of Amazon AWS and Google Cloud Platform compliance programs Trifacta SaaS products are built upon.

Trifacta complies with the General Data Protection Regulation (GDPR) requirements regarding its collection, use, and retention of Personal Information. In its potential role as data subprocessor, Trifacta adheres to the applicable principles of EU 94/95 privacy rules.

Trifacta acknowledges the importance of protected health information ("PHI") as defined in 45 CFR 160.103. The Trifacta Software is designed so that it does not

require any access to any PHI processed by customers using Trifacta, nor is any PHI is not stored within Trifacta's environment. Trifacta is, nevertheless, willing to enter into a mutually agreed business associate agreement for the purposes of complying with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), Public Law 111-005, and the regulations promulgated thereunder.

Vendors and Subprocessors

Trifacta follows a Vendor Management Policy to address requirements for onboarding new vendors, assessing risks, and monitoring vendors. Any request for new software and vendors requires approval from the security team. All vendors and subprocessors are subjected to regular risk assessment by Trifacta personnel.

Physical & Environmental Security

Because Trifacta SaaS products rely on Amazon AWS and Google Cloud, these cloud platform providers handle physical and environmental security entirely. Both AWS and Google Cloud provide an extensive list of compliance and regulatory assurances, including SOC 1/2-3, PCI-DSS and ISO27001. For more detailed information, consult the Amazon compliance, the Amazon security, Google Cloud compliance, and Google Cloud infrastructure security documentations.

CONCLUSION

Trifacta follows rigorous processes and controls to assure security, availability, processing integrity, confidentiality, and privacy of customer data. Taking steps to ensure our platform remains secure is vital to protecting our data as well as our customers' information. This is our highest priority.

The Trifacta platform is built with ease of use, performance, reliability, and security at its core to protect your most valuable asset. Platform security white papers are available from the Trifacta security and trust center website, each describing how the product security is managed for our Google Cloud and AWS based SaaS solutions.

If you want to know more about Trifacta, reach out to team@trifacta.com.

If you need to report a security concern, email us at security@trifacta.com.