CITRINE INFORMATICS SECURITY PROGRAM

EXECUTIVE SUMMARY

The Citrine Platform enables chemicals and materials companies to leverage machine learning and data management to accelerate the development of new materials. Our commitment to security allows our customers to innovate at accelerated speed and reduced costs with peace of mind.

Citrine obtained ISO 27001:2013 certification in 2018 and has continuously improved upon our Information Security Management System since. The International Standards Organization requires a complete re-certification every three years. During the two intervening years, ISO 27001 requires surveillance audits that examine half of the required controls in each of these two annual audits. In addition to strict compliance with ISO27001 Citrine Informatics has implemented controls that are in addition to ISO requirements. For example, the Citrine Platform is designed and configured to segregate user authentication from privilege authorization. Our use of unique encryption algorithms in each customer environment ensure that customer secret data is completely segregated and encrypted with keys unique to each customer. Single tenant environments ensure that customer data is never commingled.

Each customer's production environment is hosted in their own virtual private cloud (VPC) in a separate AWS instance with its own account. Encryption is used both in the cloud and to and from the cloud. To ensure cloud and network security Citrine Informatics' systems are connected using only currently supported versions of Transport Layer Security.

Security mechanisms to protect physical, network and application components of the platform, coupled with transparency about security practices and compliance best practices, give customers the confidence they need to adopt and benefit from the Citrine platform.

Table of Contents

SECURITY TAKEN SERIOUSLY

A dedicated Security Team manages Citrine Informatics' security program and ensures security Policy compliance across Citrine Informatics.

ISO 27001 is a continuously updating standard. The latest version is ISO 27001:2022. The additional changes in the newest version of ISO 27001 require new, specific controls and a refinement of the existing controls. Many Web based application providers choose to comply with SSAE 18 (SOC 2) because the controls are fewer and less prescriptive. Most importantly, the SOC 2 standard is met by service providers attestation, rather than recurring annual audit performed by a certified third party.

Security is represented at the highest levels of the company, with our Chief Informtion Security Officer (CISO) meeting with executive management regularly to discuss issues, improvements and coordinate company-wide security awareness and training.

Information Security policies and procedures are approved by management and required for all Citrine Informatics employees to read, understand and comply with. Each employee is also required to attest in writing to having read, understanding and promising to comply with policies and procedures annually.

SECURITY COMPLIANCE

Citrine Informatics has obtained our ISO/IEC 27001:2013 certification and renewed our certification yearly since 2018. Citrine begins complaince with ISO27001:2022 in 2023. Security is a top priority for Citrine Informatics, and this achievement demonstrates our commitment to information security, data protection and continuous improvement.

Our information security management system was certified by A-LIGN to be compliant with ISO/IEC 17021. The accreditation was issued by ANAB Management Systems certification body.

Citrine Informatics is committed to mitigating risk and ensuring Citrine Informatics services meet regulatory and security compliance requirements:

- Citrine Informatics complies with applicable legal, contractual, and regulatory requirements.
- The Citrine Platform is hosted at Amazon Web Services (AWS) data centers, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including SOC framework, ISO 27001 and in the Government Cloud, Fed Ramp.

GDPR, UK, and US State Privacy law Compliant

Citrine Informatics includes Data Privacy Agreements that are current GDPR / UK compliant and retains legal representation in the EU to meet the requirements to respond to Privacy issues. Citrine Informatics does not sell Personal Private Information. We are compliant with, or exempt from US state privacy laws where we conduct business.

OPERATIONAL SECURITY

Operational Security is driven by three key principles:

Customer Data is Secret

Customer data, models, and scientific domain knowledge are classified, secured and encrypted while entrusted to Citrine Informatics. Customer data are never reused for other customers, or for our own purposes.

Infrastructure management

Direct access to infrastructure, networks, and data is minimized to the greatest extent possible. The principles of "Need to Know" and "Least Privileges Access" are the foundation of privilege management.

Production systems and are secured by 20 Character minimum password length with complexity requirements and required multifactor authentication. Strict Change control procedures are required. Prior authorization is required to make any production system configuration, or privilege changes. Authorization to view Customer secret information requires demonstrated need to know, multiple approvals, is granted with the minimum privilege required and is logged and audited regularly.

Complete Segregation & Defense-in-depth

The Citrine Platform production environments, where all customer data and customer-facing applications are processed, are a logically isolated in unique Virtual Private Clouds (VPC). Each customer production environment is segregated within a dedicated AWS instance with a unique account and encryption keys. Total segregation of customer environments is ensured. Encryption in transit and at rest are managed with best available key management systems, with keys rotated regularly.

Security Controls:

CHANGE MANAGEMENT

Citrine Informatics has a formal change management process where production changes are requested prior to action being taken. Requests are required to follow a two person workflow and are approved by the System, or Data owner, or their approved delegates only. Citrine Platform configuration changes are deployed as updated versions of the entire platform. Production configuration changes follow custom code and library code review for weakness and vulnerabilities before being moved into a staging environment where it is further tested before finally being deployed to production.

ENCRYPTION IN TRANSIT

Citrine Informatics supports only current technologies to encrypt network traffic between the customer facing application interface and Citrine Platform systems. Currently this is restricted to TLS v1.3 with fall-back to TLS v1.2 when approved.

PENETRATION TESTING

Citrine Informatics regularly performs third-party penetration tests.

ACCOUNT SECURITY

Citrine Informatics secures authentication for customers and internal employees with lengthy, complex passwords and multi-factor authentication. These standards are applied to customer facing application interfaces and our supporting systems across the enterprise.

AUTHORIZATION SECURITY

The advanced security configuration applied to our Citrine Platform includes a segregation of authorization from authentication. Following successful authentication, a separate method is used to grant authorization to resources within our platform.

CLOUD AND NETWORK SECURITY

The security of our infrastructure and networks is critical. Creating a secure platform for Citrine Platform applications and customer data is foundational to our services.
Citrine Informatics' systems are connected using only currently supported versions of Transport Layer Security.

CONTINUOUS IMPROVEMENT

At Citrine Informatics, the security and resiliency of our Platform and infrastructure is a top priority. The Continuous improvement of our security program builds on our "secure by design" principles. Our Security, Engineering, Product, Data Science, Data Engineering and Customer facing teams collaborate to develop and continuously improve our secure processes and procedures.

Vulnerability Management:

Citrine Informatics Engineering team receives and responds to software and configuration vulnerabilities alerts against the Citrine Informatics platform and software.

Continuous monitoring program

Citrine Informatics approaches continuous monitoring through the development of proactive and detective controls. Through the ongoing awareness of vulnerabilities, incidents, and threats, Citrine Informatics is poised to respond and mitigate accordingly.

Incident Response Program

Citrine Informatics maintains an incident response program that is based on the SANS six step framework:

Prepare: Define and implement a corporate security policy.
Identify: Define the criteria that triggers an Incident Response.

Contain: Immediately respond stopping the threat from spreading and doing further damage. backup systems to support forensics investigations. Prepare to restore only "known good" accounts and code to production.
Eradicate: Remove infected systems, accounts and files and update defense systems.
Recover: Bring all production systems back to full production.
Learn: Review the Incident documents with the IR team and plan improvements.

PHYSICAL SECURITY

Physical security is an important part of Citrine Informatics' security strategy. We're committed to securing our facilities.

Datacenter security

Citrine Informatics leverages AWS data centers for all production systems and customer data. AWS follows industry best practices and complies with an impressive array of standards.
For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Office location security

Citrine Informatics manages visitors, building entrances, CCTVs, and overall office security. All employees, contractors and visitors are positively identified prior to gaining access to Citrine Informatics offices.

BUSINESS CONTINUITY / DISASTER RECOVERY

Citrine Informatics uses a variety of tools and mechanisms to ensure best-in-class recovery planning. Citrine Informatics maintains formal Business Continuity and Disaster Recovery plans that are regularly reviewed and updated.

Hosting our services on AWS gives Citrine Informatics the ability to remain resilient globally even if one location goes down. AWS spans multiple geographic regions and availability zones, which allow Citrine Informatics servers to remain resilient in the event of most failure modes, including natural disasters or system failures.

Citrine Informatics performs regular backups of critical data using Amazon S3 cloud storage. All backups are encrypted in transit and at rest using strong encryption. Backup files are stored redundantly across multiple availability zones and are encrypted.

THIRD-PARTY SECURITY

In today's interconnected business environment, maintaining visibility into the software supply chain is of utmost importance. Third parties used by Citrine Informatics and the products they serve are assessed before adoption. Citrine Informatics' sub processors must meet the same security and privacy requirements as Citrine Informatics and are reviewed regularly.

Once a relationship has been established, Citrine Informatics periodically reviews security and business continuity concerns at existing third parties. Citrine Informatics ensures that data is returned and/or destroyed at the end of a vendor relationship.

PEOPLE SECURITY

The people creating Citrine Informatics products are he security of our customer's data. Recurring security awareness and Phishing defence training are manditory for all employees and others. All candidates must pass a stringent background investigation by a specialized third party before being offered a position. New employees must complete Security Awareness, Phishing Defense and Policy reviews prior to being granted access to any customer data facing systems.

Updated: 3/15/2023