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 it has been renewed annually. Following best practice, our security systems separate authentication from authorization and customers' data and applications are completely segregated and encrypted.

Each customer's production and non-production environments are 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

EXECUTIVE SUMMARY **1**

SECURITY TAKEN SERIOUSLY **2**

SECURITY COMPLIANCE **3**

EU – U.S. privacy shield framework 3

OPERATIONAL SECURITY **3**

Customer Data is Secret 3

Infrastructure management 3

Complete Segregation & Defense-in-depth 4

Security Controls: 4

CONTINUOUS IMPROVEMENT **5**

Vulnerability Management: 5

Continuous monitoring program 5

Incident Response Program 5

PHYSICAL SECURITY **6**

Datacenter security 6

Office location security 6

BUSINESS CONTINUITY / DISASTER RECOVERY **6**

THIRD-PARTY SECURITY **7**

PEOPLE SECURITY **7**

SECURITY TAKEN SERIOUSLY

A dedicated Security Team manages Citrine Informatics' security program and promotes security best practices across all the teams.

The Citrine Informatics security framework is based on the ISO 27001 Information Security Standard and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, as well as Security Monitoring and Incident Response.

Security is represented at the highest levels of the company, with our Director of Security meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives.

Information security policies and standards are approved by management and available to all Citrine Informatics employees.

SECURITY COMPLIANCE

Citrine Informatics has obtained our ISO/IEC 27001:2013 certification and renewed our certification yearly since 2018, showing our maturity within the Information Security space. 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, industry, and regulatory requirements as well as industry best practices.
- 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, FedRamp.

EU – U.S. privacy shield framework

Citrine Informatics is self-certified under Privacy Shield as a part of our commitment to comply with EU data protection requirements when transferring personal data from the European Union to the United States.

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.

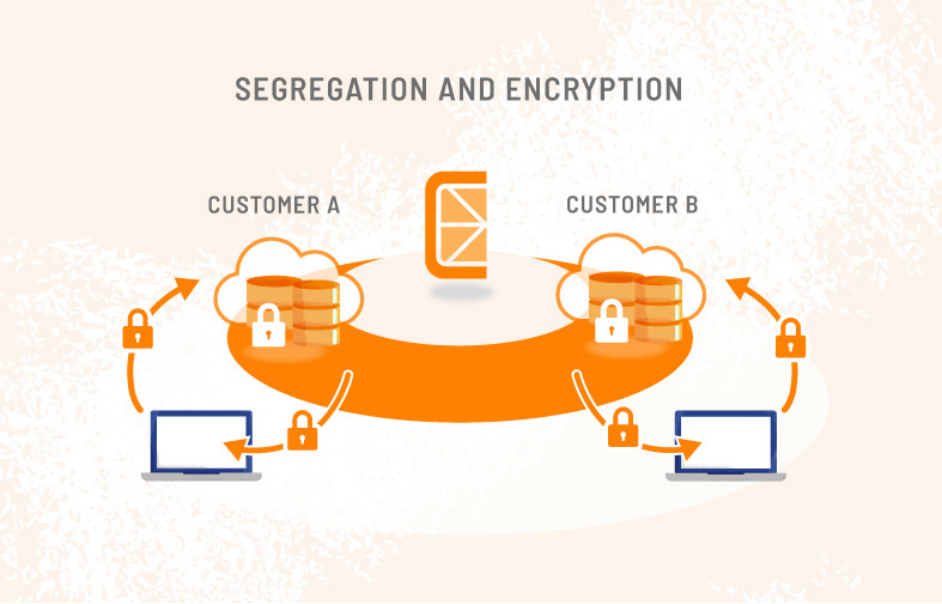
Infrastructure management

Direct access to infrastructure, networks, and data is minimized to the greatest extent possible. The principles of "Need to Know" and "Controlled Privilege Escalation" are the foundation of access to

production resources and are supported by strong multifactor authentication, and access via a bastion host. Authorization to view Customer secret information requires multiple approvals, is logged and documented, and is 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 and non-production environments are in dedicated AWS instances with unique accounts. 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 tracked and are approved. Each production change is reviewed 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.

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 are assessed before onboarding to validate that prospective third parties meet Citrine Informatics' security requirements and existing vendors 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 deleted at the end of a vendor relationship.

PEOPLE SECURITY

The people creating Citrine Informatics products are important; we've implemented processes to ensure we're bringing in the right people and keeping them up to date on the latest security trends. All candidates must pass stringent background checks by a specialized third party before being offered a position.