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 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

Table of Contents

SECURITY TAKEN SERIOUSLY

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

The Citrine Informatics Information Security Management System (ISMS) is Certified under ISO 27001. ISO/IEC 27001 is an international standard to manage information security. The standard was originally published jointly by the International Organization for Standardization and the International Electrotechnical Commission in 2005, revised in 2013, and again most recently in 2022.

Security is represented at the highest levels of the company, with our CISO and Data Protection Officer 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 Managing risk and ensuring Citrine Informatics services meet regulatory, Contractual, security and Privacy compliance requirements:

- Citrine Informatics complies with All applicable Legal, Contractual, and Regulatory requirements.
- The Citrine Platform is hosted at Amazon Web Services (AWS) Regional data centers, which are physical locations around the world where they cluster data centers. AWS calls each group of logical data centers an Availability Zone (AZ). Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area. AWS complies with leading security policies and frameworks, including SOC framework, ISO 27001

Global Privacy Compliance

GDPR and other nations that have adopted this standard prescribed compliance with these laws by Publishing the Standard Model Clauses that are required in a Data Privacy Agreement (DPA) that is appended to our contractual agreements with customers that have residents in the EU. Citrine Informatics does not have offices in the EU and must have legal counsel for GDPR compliance based in the EU. Contact information for Citrine's representative firm is published in our Privacy Policy on this website (https://www.citrine.io/privacy)

OPERATIONAL SECURITY

Operational Security is driven by three key principles:

Customer Data is Secret

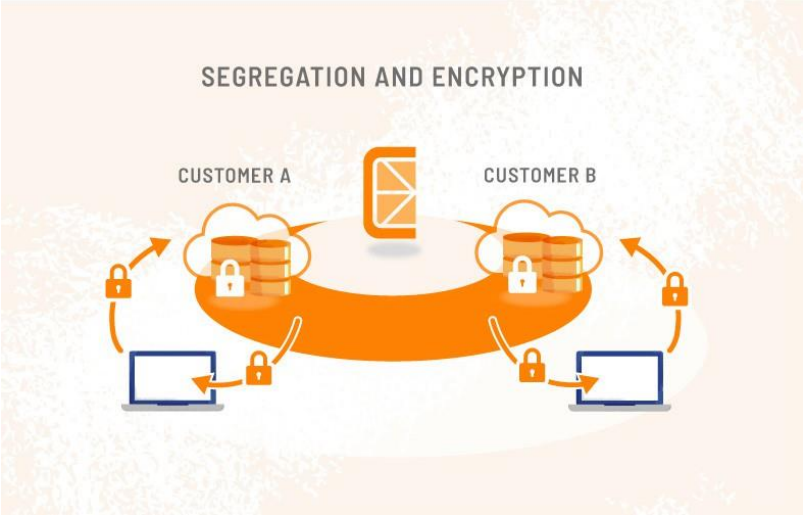
Customer data, models, formulations and Intellectual Property are the property of our customers. Customer data are never reused for other customers, or for Citrine's Internal purposes. Data is encrypted at rest and In Transit. Data stored on the Citrine platform is encrypted with keys unique to each Customer and AES 256 algorithms.

Access and Privileges are Strictly Controlled

The principles of **"A Demonstrated Need to Know" and "Least Privileged Privilege Access"** are the foundation of Granting access and privileges to resources. Business Justification is always required for Change Requests and a consensus of Security, Data Owners and System Owners must be reached and documented prior to granting privileges.

Segregation & Defense-in-depth

The Citrine Platform is a Single Tenant, Private Deployment for each customer. Each customer Deployment is created with a unique AWS Account and Virtual Private Cloud Encryption used for Data at Rest is configured with Keys unique to that customer. Encryption for data in transit is configured at each connection using Transport Layer Encryption (TLS version 1.3 with Version 1.2 available for fall back if necessary.)



Security Controls:

CHANGE MANAGEMENT

Citrine Informatics has a Strict change management process where All production Configuration and Privilege changes are pre-approved, documented and validated. Development is segregated by Dedicated AWS accounts from Production the way Customers are segregated from each other.

Secure Software Development Lifecycle

Application code is scanned for weaknesses at every Build job, Code Libraries have automated scanning for Vulnerabilities, completed code is Peer Reviewed by the Development teams and Pull Requests require Approval and Trigger change control. This highly disciplined approach is at the core of our Continuous Integration and Continuous Deployment (CI / CD) methodology.

PENETRATION TESTING

Citrine Informatics regularly performs Web Application penetration testing. Our Third-Party testing firm follows through Test-Discuss- Remediate-Test methods. Testing includes:

1. Backbox testing, where no information is provided to the test team
2. Greybox testing, where User credentials are provided to a pre-production environment that is on the same release version as Customer Platforms.
3. Admin credential testing, that simulates a compromised elevated account.

ACCOUNT SECURITY

Citrine Informatics Provides for Federated Authentication and SSO using SAML where multi-factor authentication at the custom systems passes a secure token for authentication to the Platform. Authorization is then accomplished without any requirement to see customer user credentials. Where local authentication is requested, Complex passwords with 2FA is supported.

CONTINUOUS IMPROVEMENT

At Citrine Informatics, the security and resiliency of our Platform and infrastructure is a top priority. Continuous improvement of our Information Security Management System is required under ISO 27001. Annual Improvement plans are Submitted to Executive Management. Our "secure by design" principles are key to the development and deployment of the Citrine Platform. Our Employees collaborate to secure and continuously improve our systems, processes and operational discipline.

Vulnerability Management:

Citrine Informatics Vulnerability management is implemented at many levels. Library code is examined for vulnerabilities (CVEs) in the Version Control and Repository system. Our Custom code is scanned for coding Weaknesses (CWEs) automatically at system Build. Peer review is conducted on every release, no matter how small and the deployments follow strict Change Management. Our Business supporting systems are delivered via SaaS. We share the responsibilities for security for these services and have multiple layers of controls in place.

Continuous monitoring program

Citrine Informatics achieves continuous monitoring by utilizing several controls. We have Log Aggregation and analysis for our System health and performance management. We have implemented Next Generation SIEM that detects anomalies in logged events, alerting on new and unplanned events. We have deployed Cloud Application Security Broker (CASB) t monitor and react to SaaS systems indications of compromise and to provide change validation through the development of proactive and detective controls. Our employees are trained in Security awareness and Phishing attacks and have exceptionally low susceptibility ratings.

Incident Response Program

Citrine Informatics Incident Response Policy and Plans are part of our ISO 27001 ISMS. The annual audit of the Information Security Management System (ISMS) Includes a review of all declared incidents and all activities from Start of Finish.

PHYSICAL SECURITY

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

Data center security

Citrine Informatics Serves All instances of the Citrine Platform from AWS Regional Data Centers.
AWS is also Certified under ISO 27001 and several other International Standards.
For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper:
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

SaaS Security

Citrine Informatics is a SaaS native company. We do not operate Data Centers, or on premises facilities of any kind. Our Workforce is remote and follows our policies and procedures to maintain a secure work environment in their home offices. Our Positive controls for our laptop fleet ensure Full disk Encryption Screen lock, Removable Device controls, etc. The Shared Security Model for SaaS is well documented, and procedures are followed without exception.

BUSINESS CONTINUITY / DISASTER RECOVERY

Citrine Informatics SaaS Native business model takes full advantage of the high availability of SaaS services. Our Employees can connect to the Applications served to us from practically any place where there is Internet connectivity. Should a SaaS Provider have a service outage in a given region, only Employees in that region are impacted.
Citrine Informatics maintains formal Business Continuity and Disaster Recovery plans that are regularly reviewed, tested 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.

THIRD-PARTY SECURITY

Third parties and the applications or services they provide are Vetted and Approved before on boarding to validate that prospective third parties meet Citrine Informatics' security requirements and existing vendors are reviewed regularly.

Citrine Informatics reviews Vendors, & Service Providers annually For Security and Privacy Compliance, Financial health and Breach & other security Incidents.

PEOPLE SECURITY

The people of Citrine Informatics are critically important to the security of our Enterprise. All candidates must pass stringent background checks and a series of structured interviews. Security Awareness training and Security Policies must be reviewed and attested to prior to being granted privileges to Citrine Systems. Annual reviews of the same are required for all employees.

Updated 6/3/2024