

BIOVIA SCIENCECLOUD SECURITY

Whitepaper

BIOVIA ScienceCloud is a cloud-based information management and collaboration workspace designed to support globally networked life science R&D. **ScienceCloud** allows customers and partners to efficiently access, share and communicate critical information in a secure and timely manner.

The confidentiality, integrity and availability of customer data are paramount to the operations and success of **ScienceCloud**. Our **ScienceCloud** security team is committed to applying all the technologies, standards, guidelines and best practices widely used by the cloud industry to protect our customer's data.

ScienceCloud has achieved and maintains ISO/IEC 27001:2022 & ISO/IEC 27701:2019 Certifications. ISO 27001 is the most widely recognized and internationally accepted standard for an independently verified Information Security Management System (ISMS). ISO 27001 enables **ScienceCloud** to identify risk and implement appropriate controls to preserve confidentiality, integrity and availability of information assets. ISO 27701 is an extension of ISO 27001 and it is focused on developing a Privacy Information Management System (PIMS). It sets additional guidelines on how personally identifiable information should be managed and processed. The **ScienceCloud** Information Security and Privacy Information Management System

(ISPIMS) includes the business processes and technology that guide the security and operations of the **ScienceCloud** SaaS platform. Our compliance with the ISO standard is certified by BVC Management Systems Solutions.

www.bureauveritas.com



ScienceCloud uses a multi-layered approach to protect sensitive information transmitted or stored by our applications, networks, systems, and processes to meet the growing demands and challenges of security. Our security program goes through regular internal and third-party penetration testing and assessments including successful audits from our main customers. Below, we describe in more detail the security approaches employed in **ScienceCloud**.

INFORMATION SECURITY MANAGEMENT

Information Security & Privacy Information Management System (ISPIMS)

The **ScienceCloud** Security Team has developed and operates an ISO/IEC 27001:2022 & ISO/IEC 27701:2019 Certified ISPIMS to provide the best security and assurance possible for our cloud-based Software-as-a-Service (SaaS) environment.

An independently verified and accredited ISPIMS ensures **ScienceCloud** is following and improving upon industry best practice for Information Security Management. ISO 27001:2022 outlines the requirements for establishing and maintaining an ISPIMS, and is utilized by major cloud providers to integrate risk evaluation into daily operations, offering confidence and assurance to tenants.

ScienceCloud's security team is comprised of dedicated full time security engineers who maintain qualifications such as CISSP

and GIAC certifications. Senior executives and management fully support **ScienceCloud**'s ISPIMS initiatives. **ScienceCloud**'s ISPIMS is independently tested and verified by both customers and International Certification Agencies. Lead Auditor role is required for Certification and Internal Audits.

Risk Management

Assets and Risk to those assets are continually identified and mitigated based on a proven ISO/IEC 27001:2022 certified risk management and assessment process. The **ScienceCloud** Risk Management Process received high recommendation from certification and internal auditors. The ongoing risk assessment process is reviewed and approved by executive management and includes members from all relevant departments to evaluate, mitigate and reduce risk.

All access to the cloud management interface is monitored with automated alerts for suspicious behavior.

External Parties

ScienceCloud identifies requirements for external parties relevant to **ScienceCloud** operations and security. **ScienceCloud** policies require risk to be evaluated for all external parties including Cloud Service Providers (CSP). **ScienceCloud** continuously evaluates Cloud Service Providers to ensure **ScienceCloud** security requirements are being met and continue to be met. Cloud service providers must maintain ISO 27001 Certification and are subject to both physical and electronic security audits. Cloud Service Providers must provide assurance that data is adequately protected and available when needed.

Computer System Validation

The Good Automated Manufacturing Practice (GAMP) is the definitive standard for validating computer systems in the pharmaceutical industry. The **BIOVIA ScienceCloud** platform allows our customers to deploy validated software installations in accordance with GAMP5. The **ScienceCloud** ISPIMS includes instructions for installing and operating **ScienceCloud** in a way that adheres to the computer system validation needs in GAMP5.

Change Management

ScienceCloud Security Team ensures appropriate controls are in place to ensure that risks can be mitigated and controlled to acceptable levels on an on-going basis. Risks are to be re evaluated prior to the launch of new service, major changes to the existing platform, or Cloud Service Provider. Changes are managed, reviewed and approved through a change control workflow with electronic signature capability, which is also maintained as a validated system.

SECURITY BEST PRACTICE

Access Control

Access to **ScienceCloud** IT systems is strictly controlled with Access Management Procedures, Least Privileged Access, and Separation of Duties. Management must approve access prior to account creation using proven Access Management Procedures. Least Privileged Access refers to granting users accesses minimally required to perform their duties. Separation of Duties is a process that divides roles and responsibilities so that a single individual cannot subvert critical processes unnoticed. All access to **ScienceCloud** systems is continuously monitored and audited on a regular basis.

The first line of defense starts with
ScienceCloud employees and contractors.

Role-based access is used for cloud management. Identity and access management is managed by the security team. No one person has full access to all aspects of the cloud infrastructure. To gain full access, an attacker would need to break into multiple accounts. All access to the cloud management interface is monitored with automated alerts for suspicious behavior.

ScienceCloud has recognized the need for federated identity in today's threat landscape. Federated identity such as SAML allows customers to manage and store their user's credentials for Authentication, Authorization, and Accounting with secure access to **ScienceCloud** Services.

Multi-Tenancy with Security Built-in

Multi-tenant architecture allows for secure auditable separation of customer data, quick upgrades, lower cost, and elasticity between customers. The **ScienceCloud** multi-tenant applications have been developed with security built-in for over a decade. **ScienceCloud** has worked with a number of large Pharmaceuticals and CRO Corporations to comply with stringent security requirements. Multiple layers of security are used to guarantee separation of data in a multi-tenant environment. Fine grained security provides customers with a means of granting and restricting access at all stages of collaboration.

With the added ability for automation and control of the virtual infrastructure, pre-configured security settings are automatically built into virtual machines at the time of provisioning. Strict policy enforcement guarantees no server is created anonymously or without security built-in. Security tools are cloud aware with Host Intrusion Detection (HIDS) and Host Intrusion Prevention (HIPS) automatically installed and configured.

Multi-layered Approach

ScienceCloud uses a Hybrid Cloud approach with layered security for the different physical and electronic layers. A Hybrid Cloud allows for highly confidential data to be stored and processed using dedicated hardware that is physically isolated from other zones. Multi-layered defense-in-depth security reduces the risk of compromise or loss of data. The first line of defense starts with **ScienceCloud** employees and contractors. Employees and contractors must follow security policies and are continuously made aware of the increasing threats to the organization.

In addition to traditional firewalls, Web Application Firewalls (WAF) are used to address security risk that are specific to Web Application Servers. Security zones within the trusted environment are further separated with application layer firewalls in addition to local host firewalls. Every endpoint is protected with Intrusion Detection and Prevention measures. Security policies follow the virtual machine insuring the appropriate protection set forth by the **ScienceCloud** Security Team.

Data in transit is transmitted over Transport Layer Security (TLS) using only strong security protocols. Backups are secured in multiple isolated locations and encrypted using strong AES encryption.

Data Classification and Isolation of Customer Data

The protection of customer data is of the utmost importance to **ScienceCloud**. All customer data is identified, classified and isolated from less secure environments. Data classification is used to identify and protect sensitive data. Customer data is stored and processed in an isolated database with dedicated hardware. **ScienceCloud** applications were built from the ground up to safeguard customer data from the loss of confidentiality, integrity, or availability. All access to sensitive data is continuously monitored with Security Information and Event Management (SIEM) and Data Loss Prevention (DLP) measures. Strict security policies require all employees and contractors to safeguard sensitive data with additional focus on customer owned data.

Security Testing

Penetration testing is conducted both internally and externally using reputable companies with industry experts. Controlled penetration tests allow for risk analysis beyond the initial compromise to help identify and mitigate risk presented by the trusted insider. Security threats are proactively identified and mitigated. Members of the **ScienceCloud** Security Team receive ongoing training and are Certified Information Systems Security Professional (CISSP) (ISC2) and Global Information Assurance Certification (GIAC) certified.

Business Impact Analysis and Disaster Recovery

Continual evaluation for the loss of Confidentiality, Integrity, or Availability of data is conducted by **ScienceCloud**. Formal Business Impact Analysis is conducted with senior executives and directors to ensure the appropriate level of protection is applied. Data retention is tailored to meet the needs of customers. Geographically located redundant Disaster Recovery sites provide assurance of uninterrupted availability of **ScienceCloud** Services.

Disaster recovery tests are conducted periodically to identify areas for continual improvement to the Disaster Recovery Plan. Periodic test are conducted to insure encrypted backups are secured and available when needed.

Software Development Life Cycle (SDLC)

The BIOVIA Software Development Lifecycle (SDLC) is governed by a Quality Management System (QMS) that includes considerations for security. The SDLC process is continuously evaluated and updated to stay current with industry standards and best practices. For more information, please contact your Account Representative for a copy of the BIOVIA Quality Statement document.

BIOVIA SCIENCECLOUD FOR LABORATORY INFORMATICS

BIOVIA ScienceCloud provides a secure, scalable, and validation-ready environment for BIOVIA's laboratory informatics solutions. With the **BIOVIA ONE Lab** on **ScienceCloud**, research, development, analytical and QA/QC laboratories have a unique opportunity to remove paper processes and better support end-to-end analytical and process workflows. Unified, harmonized and standardized laboratory/resource management and procedure execution can help achieve your business goals by improving collaborative innovation, increasing productivity, reducing regulatory compliance and safety risk and accelerating time to market.

Cloud deployment of **ONE Lab** increases security, while decreasing the necessary IT overhead and total cost of ownership, providing a dynamic infrastructure for your laboratory informatics.

BIOVIA ONE Lab offers research, development, analytical and QA/QC laboratories a unique opportunity to truly digitalize their lab processes and to connect analytical and process workflows end-to-end. There is no longer a need for the artificial boundaries between traditional point solutions such as ELNs, LIMS, LES, Inventory Management, and Instrument Management/Integration. The unified, harmonized, and standardized laboratory/resource management and procedure execution capabilities of **BIOVIA ONE Lab** can help achieve your business goals by improving collaborative innovation, increasing productivity, reducing regulatory compliance and safety risk and accelerating time to market.

Deployment of **ONE Lab** on **ScienceCloud** increases security, while decreasing the necessary IT overhead and total cost of ownership, providing a dynamic infrastructure for your laboratory informatics. **ONE Lab** can also integrate with existing lab informatics systems for a true digital transformation.

BIOVIA SCIENCECLOUD FOR QUALITY AND COMPLIANCE

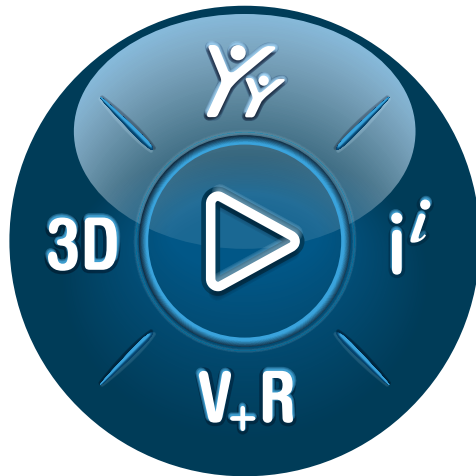
While Quality and the implementation of a Quality Management System (QMS) are often perceived as a costly burden, an integrated cloud-based QMS is easy to deploy, contains costs and effort, and contributes to better and more efficient processes. With QUMAS Cloud, customers can focus on the usage of the application rather than on its management. Based on the **ScienceCloud** infrastructure managed by BIOVIA and built on Amazon Web Services (AWS), the responsibility for security, application access, operations, and maintenance will be removed from your IT organization freeing up valuable time, resources, and budget.

The core of this integrated offering is QUMAS EDMS (Electronic Document Management System) for data-centric Documentation and Content Management and QUMAS EQMS (Enterprise Quality Management System) for Quality Process Management. Both systems are accessible through the user-friendly MyQUMAS interface.

From MyQUMAS you can manage and collaborate in real-time on all regulatory and quality content, create and perform tasks from incident logging through investigation to approval and remediation and access eLearning to browse, view and mark documents as read and understood and to print and search.

QUMAS manages the entire range of quality content and processes supporting SOP updates necessitated by a Deviation or CAPA, all within one unified validated solution. Its scalability and ability to be deployed in the cloud make it suitable for small to large enterprise implementations.

Designed for regulated industries, QUMAS supports regulatory compliance with US FDA, EMA and PMDA requirements, while reducing validation efforts and inspection/audit times. Additional Quality Intelligence capabilities allow you to search and analyze your Quality data for proactive quality decision-making.



3DEXPERIENCE®

Dassault Systèmes is a catalyst for human progress. Since 1981, the company has pioneered virtual worlds to improve real life for consumers, patients and citizens.

With Dassault Systèmes' 3DEXPERIENCE platform, 370,000 customers of all sizes, in all industries, can collaborate, imagine and create sustainable innovations that drive meaningful impact.

For more information, visit: www.3ds.com

Europe/Middle East/Africa

Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Asia-Pacific

Dassault Systèmes
17F, Foxconn Building,
No. 1366, Lujiazui Ring Road
Pilot Free Trade Zone, Shanghai 200120
China

Americas

Dassault Systèmes
175 Wyman Street
Waltham, Massachusetts
02451-1223
USA

**Virtual Worlds
for Real Life**

