WHITEPAPER

SCIENCECLOUD SECURITY

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.

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 27001:2013 Certification. 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. ScienceCloud ISMS includes the business processes and technology that guide the development and support of the ScienceCloud platform. Our compliance with the ISO standard is certified by Bureau Veritas Certification http://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 Management System (ISMS)

The ScienceCloud Security Team has developed and operates an ISO/IEC 27001:2013 Certified Information Security Management System (ISMS) to provide the best security and assurance possible for our cloud-based Software-as-a-Service (SaaS) environment.

An independently verified and accredited ISMS insures ScienceCloud is following and improving upon industry best practice for Information Security Management. ISO/IEC 27001:2013 provides requirements for establishing, implementing, maintaining, and improving an ISMS. ISO 27001 is used by all major cloud providers, for integrating risk evaluation into the daily operations of running a cloud infrastructure, and providing confidence and assurance to tenants.

ScienceCloud's security team is comprised of dedicated full time security engineers. Experienced security engineers maintain qualifications such as CISSP and GIAC certifications. Senior executives and management fully support ScienceCloud's ISMS initiatives. ScienceCloud's ISMS is independently tested and verified by both customers and ISO/IEC 27001 Lead and Master Auditor certified organizations.

Risk Management

Assets and Risk to those assets are continually identified and mitigated based on a proven ISO/IEC 27001:2013 certified risk management and assessment process. The ScienceCloud risk management process received a high recommendation from the Lead ISO 27001 Auditor. The ongoing risk assessment process is reviewed and approved by executive management and includes members from all relevant departments within ScienceCloud to identify risk and asset owners.

> "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 works closely with the CSP to insure ScienceCloud policies and security requirements are being met and continue to be met. Cloud service providers must possess ISO 27001 Certification and are subject to both physical and electronic security audits conducted by ScienceCloud and its partners. Cloud Service Providers must provide assurance that data is adequately protected and available when needed.

Software Development Life Cycle (SDLC)

ScienceCloud software development follows the Agile software development practice with Scrum. Strict policies and procedures are followed for the secure design, development, and deployment of software. Security is built into all phases of the software development process. Developers receive periodic training for secure coding practices. Source code is reviewed by peers and automated systems to identify issues early in the SDLC process.

Vulnerability and penetration testing are done at pre-determined stages of the SDLC with the ability to stop deployment if a security risk is discovered. The SDLC process is continuously evaluated and updated to stay current with industry standards and best practice. ScienceCloud's Security and DevOps Teams work closely with the development team to insure secure configuration and policy enforcement. Fully autonomous environments are maintained for Development, Quality Assurance, Staging, and Production.

SECURITY BEST PRACTICE

Access Control

Access to ScienceCloud IT systems is strictly controlled with Change Management, Least Privileged Access, and Separation of Duties. Management must approve access prior to account creation using proven change 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. All access to ScienceCloud systems is continuously monitored and audited on a regular basis.

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 Preventions (HIPS) automatically installed and configured.

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

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 in the private cloud zone 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 Secure Socket Layer (SSL), using only strong security protocols, such as SSLv3 and Transport Layer Security (TLS). Offsite backups are 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 the private cloud using 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

Red Team versus Blue Team penetration testing exercises are conducted to determine real world risk analysis. 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.

Cloud Controls Matrix (CCM) by the Cloud Security Alliance

ScienceCloud meets the security and risk management requirements for Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). The CCM provides fundamental security principles to guide cloud vendors and to assist cloud customers in assessing the overall security risk of a cloud provider. The CCM also normalizes security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud. The matrix provides a detailed understanding of the security and privacy concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. The ScienceCloud Security Team understands the need for organizations such as the Cloud Security Alliance and is an active contributor.