jahia

Information Security Management
Information Sheet

Section I – Generic Information Security Requirements

Introduction

Jahia provides a **Digital Experience Platform (DXP)** to its customers, often via a PaaS deployment in the Cloud. To meet the expectations of our customers, Jahia is committed to preserving the confidentiality, integrity and availability of all physical and electronic information assets throughout the company. This is defined and managed within an Information Security Management System (ISMS).
This ISMS then ensures that all relevant regulatory, legislative, legal and other applicable requirements related to information security are met.

Appropriate Business Continuity arrangements are in place to counteract interruptions to business activities and these take account of information security. Information security education, awareness and training is provided to staff and others working on behalf of the company.

Breaches of information security or security incidents, actual or suspected, are reported and investigated through appropriate processes. Appropriate access control is maintained and information is protected against unauthorized access.

Continual improvement of the ISMS is made as and when appropriate.

Compliance Program

Jahia has implemented the ISMS in accordance with the international standard ISO/IEC 27001:2013 requirements. Jahia was audited and certified as compliant with ISO/IEC 27001:2013 in September 2019. The audit and certification was carried out by IT Governance, a UK-based ISO 27001 compliance body and Coalfire, an accredited ISO/IEC 27001:2013 certification body.

Jahia has also self-certified against PCI DSS SAQ A and is certified HIPAA compliant. The HIPAA compliant certification comes after the successful completion of the HIPAA compliance assessment carried out by Coalfire, an independent auditor.

Jahia has appointed a dedicated Compliance Manager to oversee day-to-day operation of the ISMS and report on all security-related matters to the Jahia Board of Management.

Physical security

The **Jahia Cloud** infrastructure and systems are hosted entirely at secure **Amazon Web Services** (AWS) and **Microsoft Azure** facilities. Jahia offices are protected by entry badge access, visitor sign-in, and security cameras. Physical assets such as laptops, which may temporarily contain customer data, are protected by automatic disk encryption and have auto-locking of the workstation if left unattended.

Security Incident Procedure

As part of the ISMS, Jahia has defined a Security Incident Procedure. All staff are required to report (via a ticket) any suspicious activity or possible breach of information security. A Security Team then assesses each ticket and identifies any security incidents. The first step is to mitigate any risk associated with the incident but then the lessons learned are fed back as part of the ISMS Continual Improvement Program.

Continual Improvement Program

Any business environment is subject to change with new information assets being added on a regular basis. Jahia's approach to the ISMS requires that all new assets are assessed for potential risks and a risk treatment plan is defined to ensure any risks arising from the new assets are mitigated.

The ISMS is also subject to continuous, systematic review and improvement. Process owners are encouraged to look for ways in which the ISMS can be improved, and these improvements are logged and managed by the Compliance Manager and the ISMS Team.

User Access Controls

User access must meet the following conditions:

- Authentication needs to happen with a personal account
- Multi-Factor Authentication must be enforced with at least 2-factor authentication

Where an accessed system resides inside the Jahia network, only privileged access from inside the Jahia Network is permitted. Permissions granted to individuals may be role-based and dependent on their role within the team. Jahia operates a strict on/off boarding procedure for all staff that reflects their role and required permissions for that role.

Section 2 – Security in the Jahia Cloud

Integrity and Confidentiality

The integrity of the Cloud assets is maintained using a strict authentication and permissions policy. There is a granular permissions system whereby sensitive data and functions are segregated from users with low-access requirements. All system and software logs are centralized and stored in read-only access for a minimum of 14 days. Administrative functions are only available to privileged users, using the SSL / HTTPS protocol for publicly available interfaces with non-auto signed SSL certificates. Passwords are stored using a hashed, salted encryption.

Availability

The Jahia Cloud service is built to deliver guaranteed 99.9% availability. To achieve this, the design of the Jahia Cloud follows a set of key guiding principles. Components are replicated, at least once, in a different data centre. Components are stateless or their state is either replicated or offloaded to a different backend. There is constant monitoring where alerts are generated in case of resource shortage or unavailability and all components have a clear and tested disaster recovery strategy.

Protection against malicious software

Data import integrity is checked prior to the import taking place. AWS and Azure WAF (Web Application Firewall) scan the data against malicious instances. Part of Jahia Cloud's managed services involves the Jahia team identifying and remediating vulnerabilities. Threats are shared with the tenant on a 'need-to-know' basis.

For security monitoring, Jahia uses an external service - **BitSight**. BitSight Security Ratings are a measurement of an organization's security performance. Much like credit ratings, BitSight Security Ratings are generated through the analysis of externally observable data.

Encryption

Customer environments are stored on a multi-layer infrastructure - AWS or Azure physical storage, AWS or Azure volumes, Docker volumes and application servers/databases. Encryption needs to happen on at least one of these layers.

All HTTP communication going through a public network uses HTTPS with TLS V1.2 or V1.3 with a third-party approved SSL certificate (self-signed is prohibited). All customer-defined passwords are encrypted at rest.

Encryption key management

Encryption key access is reserved to only the Jahia Cloud teams. The maximum expiration period for a cryptographic key is 3 years. All expired or compromised cryptographic keys shall be deleted within 48 hours. Cryptographic keys are only stored in one of the following systems: Jahia's dedicated password manager, AWS's Secrets Manager, or the system using the key to encrypt communication.

Audit Logs

The Jahia Cloud infrastructure is designed in a highly auditable way. All actions executed are logged along with the outcome (success/failure) of the action. These logs are read-only to ensure that they cannot be altered. Logs do not reveal the state of the application or the file structure of the server and all authentication activities are logged. All permission attribution or privilege changes are logged. All access to sensitive data is logged but credentials or sensitive data are never logged. Logs are reviewed on a regular and scheduled basis.

Continuous Monitoring and Alerts

All physical servers or virtual machines forming part of the Jahia Cloud ecosystem are monitored using Datadog, a commercial "Cloud Monitoring as a Service" offering. Each client needs to have their own Datadog sub-organization.

Key metrics are monitored with automated alerts being triggered via email when thresholds are breached in areas such as network synchronization, disk utilization, CPU, and memory usage.

Secure update procedure for the Jahia Cloud

The Jahia Cloud Virtual Machine (AWS EC2 and Azure) upgrade process ensures critical updates that will not impact on business operations are deployed straight away using an automated tool. Those that are seen to have an impact on business are scheduled for deployment in development, then in production after validation and scheduling with the business. Non-critical updates are deployed on a regular, scheduled basis.