BMS SECURITY

Kaseya BMS is a next-generation IT business management solution built specifically to help IT professionals. BMS allows IT professionals to create, manage and resolve service requests and tickets, to manage project work, to track all aspects of the customer relationship, and to handle billing and finance for their companies.

OUR SECURITY PROMISE

BMS abides by strict measures to protect the security and privacy of your valued data. In addition, we understand that having reliable access to your data, with no downtime, is critical to your business. To ensure that these objectives are met, we have adopted industry-leading security measures, as outlined in this brief.

SUMMARY OF KASEYA BMS SECURITY PRINCIPLES

In support of a holistic and structured approach to managing information security, Kaseya has built an information security management system (ISMS) based on the generally accepted ISO/IEC 27001:2013 framework of the policies and procedures.

SOC 2, TYPE II COMPLIANCE

BMS, under the Kaseya umbrella, has SOC 2 Type II certification with the Trust Services Principles and criteria for Security, Availability and Confidentiality. Service Organization Control 2 (SOC 2) Type II is an internal controls report that captures how well data is safeguarded, and the degree to which those controls adhere to industry best practices. This report ensures that we are meeting stringent requirements set by the American Institute of Certified Public Accountants (AICPA), which developed and administers the SOC 2 program. Kaseya's SOC 2, Type II report can be made available if necessary, under security NDA.

This is one of the many ways that we demonstrate our commitment to security and follow industry best practices to secure your valued data. Type II requires the implementation of the controls over a minimum audit period in addition to the ongoing attestation of the operating effectiveness of the controls. Comparatively for Type I, controls need to be in place, however acceptable security processes only need to be verified at a specific point in time. Our security infrastructure and procedures are tested and audited by third parties on a regular basis as they relate to the Trust Services Principles and Criteria: the security, availability, processing integrity, confidentiality, and privacy of a system.

PRODUCTION INFRASTRUCTURE ACCESS

Role-Based Access Control

The BMS development team has role-based access control, whereby access to the architecture of BMS is allowed on an as-needed basis, as defined by one's role. This separation of duties means that individuals working on BMS only have access to the parts of the system that are required for their individual roles.

LOGICAL ENVIRONMENT SEPARATION

There are different and logically separated environments for Development, Staging and Production.

PRODUCTION MONITORING

The BMS Development Operations Team monitors the availability of production systems through automated systems. Logs and events are then centrally managed and analyzed by the team.

BMS SECURITY

APPLICATION PERFORMANCE MONITORING

To manage the demand for processing capacity and to enable the implementation of additional capacity commitments, we ensure that systematic network and monitoring is in place. Daily and monthly task and event logging is maintained. Automatic backup systems are utilized to perform scheduled system backups of target data while backup jobs are monitored with notification alerts sent out in the event of backup failure. BMS has a backup schedule in place to automatically initiate production backup jobs. Finally, restore operations from backup media are performed as a component of disaster recovery operations to verify that out system components can be recovered.

CHANGE MANAGEMENT

We have implemented a change management process within our production teams, including segregated development, integration, test, and production environments. Our software change control process requires all changes to code to be documented, a risk assessment completed, a code review completed by a senior developer or engineer, and Quality Assurance (QA) processes to be completed which evidences that approval for change was obtained before production. Change management is also implemented on our production servers, including documentation of changes, risk assessments, and approval processes. All incidents are documented, including steps to contain the issue, root cause analysis, long term solutions, and related evidence and communications. High severity incidents require an analyst to determine the root cause and changes are recommended to eliminate the incident from reoccurring.

ENTERPRISE SECURITY FEATURES

BMS employs a number of security features. One of these is full SAML 2.0 support, including single sign-on (SSO) with Passly, Okta, Azure Active Directory (AD), and more. BMS employs encryption at rest for DB sensitive fields, using the SHA-256 encryption standard. SHA-256 (Secure Hashing Algorithm) is a patented cryptographic hash function, ensuring that encrypted data is unreadable. Encryption in transit is done with TLS 1.2

SECURE SDLC (SOFTWARE DEVELOPMENT LIFECYCLE)

The BMS source code utilizes static application security testing (SAST) in order to identify potential security vulnerabilities and quality issues during the development stages so that these issues are corrected even before the testing process is completed.

On the training side, all BMS software developers receive Security Awareness Training, and are familiar with Change Management policies and procedures as well. Testing activities include unit testing, regression, integrations and stress testing.

BMS SECURITY

HIGH AVAILABILITY, RELIABILITY AND DATA RECOVERY

Our goal is to have 100% uptime. To meet this goal, Kaseya and the BMS team have built our infrastructure to be both robust and scalable. We monitor security, uptime and performance 24/7/365 and have a dedicated team proactively managing the environment at all times. Our service is protected from external attacks through Amazon's denial-of-service protection and PCI-level endpoint security measures. Leveraging this low-latency, high-availability cloud infrastructure enables BMS to maintain almost five (5) nines of uptime with a 200ms average response time.

AWS has built its data centers in multiple geographic regions, with multiple Availability Zones within each region. AWS regions are completely isolated from one another for maximum fault tolerance and stability. Even though regions are isolated, they are connected to the rest of the AWS network through low-latency links to offer maximum resilience against disruptions. We have a recovery point objective of 24 hours, and a recovery time objective of 4 hours.

SECURITY AND PRIVACY PRINCIPLES:

Kaseya has built an information security management system (ISMS) based on the generally accepted ISO/IEC 27001:2013 framework of the policies and procedures. We recognize the importance of protecting our customer's privacy and are not in the business of selling information about you. You can read Kaseya's full privacy policy to learn how we limit the use your information, the types of information we collect and your individual rights.

CONCLUSION

BMS adheres to the principle of complete vigilance for the privacy and security of information. We take our internal processes and compliance with enterprise-level security standards seriously. Through our application, BMS offers you a way to maintain the integrity of your data. By building security features into our software and by maintaining rigorous adherence to our third-party audits, we continue to provide you the Professional Services Automation that you use in your business daily.