Lotame Security Summary

As the world's leading data solutions company, Lotame takes security and privacy very seriously. Our clients trust and depend on our products to manage and protect their data, so Lotame designs and operates them against strict requirements for privacy, security, and data protection. We do this by implementing an Information Security Management System (ISMS) program that is certified to meet the ISO 27001 standard. Our ISMS defines a set of policies and processes that ensure confidentiality, integrity, and availability for client and Lotame data. This brief provides a summary of the approaches used by Lotame to mitigate risks to our clients' data assets.

Risk Analysis and Mitigation

As required by the ISO 27001 standard, Lotame's ISMS program begins with a comprehensive analysis of the risks to data, both within the platform and in the management activities surrounding it. Our Risk Analysis and Risk Treatment processes ensure high priority threats and vulnerabilities are identified and prioritized for treatment, not only on the Spherical platform, but on all of the data assets that we utilize to service our clients' data needs. The results of these analyses provide the baseline for the policies, processes, and technical safeguards we employ throughout our enterprise to protect data. The remaining sections describe some of these safeguards.

Communications Security

Lotame utilizes a combination of secure architectures and secure processes to ensure that all computing services provide sufficient protection of data. We designed our network to permit only the required external interface points, and utilize a DMZ for any Lotame resource requiring an external interface. All other resources are maintained in private networks within our virtual private clouds (VPCs) defined in the Amazon Web Services (AWS) cloud.

We protect all external communications through the use of industry-standard encryption protocols. Transport Layer Security (TLS) version 1.2, commonly referred to as SSL/TLS, provides this protection for all web-based transactions. We also employ TLS encryption for server-to-server communications with clients that require SSH File Transfer Protocol (SFTP) endpoints.

We implement encryption at rest for the data in our primary and replica databases using AES with a 256-bit key. We rotate these keys through an automatic process annually, and maintain the encryption for our backups as well. Backups are stored in a separate physical datacenter in support of disaster recovery, and all backup and restore processes are tested regularly.

Access Control

Lotame follows the principles of least privilege and separation of concerns with respect to granting access rights for administrative and operations personnel. We track all platform access requests and manager approvals in our JIRA ticketing system, with our security team reviewing and implementing

these requests. Elevated privileges are granted to engineers with specific operational duties, and require multi-factor authentication to access the AWS provisioning system.

For our corporate accounts, the Lotame IT team performs employee provisioning and de-provisioning from a central user store, ensuring appropriate approvals are in place. The team also performs quarterly audits of the IT systems, to ensure continued access is appropriate for all accounts. All new employees must pass a third-party background check, and complete security training to ensure awareness of our policies and processes for corporate and production systems use.

Lotame's policies for password and account management follow best-practices for security, employing password standards combined with multi-factor authentication for all employee accounts. The password standards ensure a high level of complexity for single passwords (3 of 4 character groups, no repeats, no dictionary words) but also permit for longer pass-phrases (greater than 20 characters) to provide sufficient entropy.

Physical Security

Lotame defines strict requirements for our vendors to pre-qualify to host the Spherical platform. Our cloud service providers must maintain globally-recognized audits on the security and reliability of their services, such as ISO 27001 or SOC 2/Type I/II. Currently, Spherical is hosted on the Amazon Web Services (AWS) cloud, and you can find more information about their service's compliance here: https://aws.amazon.com/compliance/.

Lotame also defines policies for our corporate offices to ensure security of business data. The policies require automatic locking doors, individual scans for entry, 24x7 monitoring and escalation, and clean-desk and computer policies that limit accidental exposure of data.

Systems Development

Lotame's Spherical platform is a proprietary system, with over a decade of enhancement and refinement built into its core. We built our software with data security in mind, knowing that we are caring for the fuel to our clients' businesses. As such, we have implemented best practices in software and systems development, often referred to as a Systems Development Lifecycle (SDLC), that ensure changes are made in a safe and secure manner.

Our product management team and engineering teams specify and develop new functionality within a development environment that is completely separate from any production systems. All code changes are peer-reviewed, and significant architecture changes go before an architecture review process for approval. This review process ensures that security and privacy policies are followed by checking against the appropriate industry-standard guidelines such as OWASP.

A separate quality assurance (QA) environment allows our engineering team to execute automated and manual quality assurance checks, and ensures that all tests pass before staging code for production. We utilize a git-based source control system to maintain the full history of the changes made to

application configurations and code.

Our operational staff manages both releases and application configuration changes using automated and audited tools. They perform final vetting of all changes, and ensure that availability and security are maintained. Once a release is approved, it is deployed to the relevant application hosts via automated configuration management tools.

We have designed both the architecture of the platform and the release procedures to deploy both code and configuration changes without interrupting client facing services. In the event that Lotame must perform maintenance that could interrupt service, we provide several days notice prior to commencing such maintenance through our status tracker at https://status.lotame.com.

Business Continuity

Lotame has built automated redundancy and elasticity into our products, ensuring that we maintain our services through the most likely failure scenarios for hardware, networks, and other systems. We utilize several tools and services to monitor every aspect of the platform at all times, both from outside of the firewall and from within. Our operations team is on-call 24x7 to respond to failures or incidents. Behind the firewall, we monitor thousands of system and application metrics using DataDog for collection, visualization, and alerting. Outside the firewall, we utilize a variety of third parties to monitor system-level performance from multiple physical testing locations in each geographic region.

In addition to built-in redundancies, we have also defined a separate Business Continuity and Disaster Recovery Plan that addresses larger-scale interruptions that may occur, and how our team will respond to restore service. This plan defines the business-critical systems that clients depend on, and covers a variety of scenarios that could present large-scale interruptions on those systems that would exceed our redundancy approach's ability to maintain service. The plan includes both automated responses as well as steps that Operations Personnel would take to restore services when automated approaches do not suffice.

Incident Management

Lotame has defined and follows an Information Security Incident Response Process for all security events. This process provides a framework for ensuring security events are investigated thoroughly and proper precautions are followed to safely return the affected systems to service. Additionally, if an incident is determined to be a breach, the workflow ensures escalation to the appropriate management team members and third parties. This escalation engages members of Lotame’s executive team to ensure all information is efficiently collected and managed, all legal responsibilities are upheld, and customers are notified in a timely fashion of any threats to their data.