Last Updated: September 2020

Information Security Overview

1. Kalderos Security and Risk Governance

Kalderos' Board and Executive Leadership Team understands the importance of the security, confidentiality, availability and integrity of Kalderos' critical information assets and customers' confidential information. With a top-down organizational commitment to this notion, Kalderos has invested the appropriate resources and controls to protect and service our customers. The dedicated information security team is focused on defining new security controls while also refining those which already exist. Furthermore, the information security team continuously enhances the Kalderos security framework and maintains an active and effective risk management program.

2. Kalderos Security and Risk Management Objectives

We have developed our security framework using industry best practices for SaaS applications. Our key objectives include:

- Protect customer information and data: Provide exceptional service to our customers while protecting the privacy and confidentiality of their information.

- Services availability: Ensure ongoing availability of services to all customers and proactively minimize security and cyber threat risks that threaten service continuity.

- Information and data integrity: Provide assurance that security and internal controls over customer information are adequate to ensure data consistency and that data is not inappropriately altered.

- Standards and regulatory compliance: Implement and continuously improve policies, procedures and internal controls that align to our business objectives and regulatory and industry best practice. The information security team has developed the security program around the SSAE18 SOC1 and SOC2 standards while aligning to the guidance outlined within the ISO 27001 and NIST SP 800-53 standards.

3. Kalderos Security Controls

With the purpose of protecting our customers' data while maintaining financial reporting integrity, we have implemented more than 200 security and processing internal controls. These controls have been designed to maximize our workforce efficiency while minimizing risk.

3.1 Infrastructure for Kalderos Products and Services

3.1.1 Data Center Security

Kalderos is 100% deployed to cloud services, utilizing the Microsoft Azure cloud for product and service delivery and Google G Suite for corporate office back-end services. These platforms provide for the highest level of physical and network security. Currently, Kalderos' Microsoft Azure cloud deployment resides entirely within the borders of the U.S. Both Microsoft Azure and Google G Suite cloud service providers maintain audited security programs that require periodic attestation and compliance to the SSAE18 SOC 2, ISO 27001 and HIPAA standards and rules.

Additionally, these market-leading infrastructure providers leverage the world's most advanced datacenter architectural capabilities such as power, networks, cooling, fire suppression and state-of-the-art physical security that support guaranteed facilities uptime between 99.95% and 100%. Physical access to these datacenter facilities follows a layered approach to reduce the risk of unauthorized users gaining access to data and datacenter resources and is supplemented with periodic physical security reviews to ensure compliance to security requirements.

Kalderos takes datacenter security seriously and performs an annual review of each of the datacenter provider's annual SSAE18 SOC 2 Type II reports for control exceptions that may have a direct or indirect impact on Kalderos' security, confidentiality, availability and processing integrity. Control exceptions are documented internally and tracked until mitigation or remediation has been reached.

3.1.2 Network Security and Perimeter Network Architecture

Kalderos' products and services leverage the advanced networking capabilities, protections and internet-scale offered by the Microsoft Azure cloud platform. In particular, our network access controls were designed to prevent unauthorized access to Kalderos' systems and applications from external and internal sources. Network security is actively monitored 24/7/365.

3.1.3 Configuration Management

Our commitment to the use of cloud serverless infrastructure allows Kalderos to quickly and securely scale our highly automated application environment to meet the demands of our customers' requests and transactions. Changes to configuration and standard images are managed through a controlled change management process.

Patch management is fully automated within our Azure environment, including on our database servers which always have the latest update version and experience very little impact on workloads during the update process.

3.1.4 Availability, Alerting and Monitoring

Azure's rich native monitoring and alerting capabilities for service health compliments Kalderos' investments in best-in-class automated monitoring capabilities to alert engineers and administrators when anomalies occur. As unexpected or malicious activities are detected and logged, addressable alerts are raised to the right support personnel to ensure that the issue is addressed and remediated as quickly and as effectively as possible. The notification system is fully redundant with built-in call tree and escalation functionality.

3.1.5 Infrastructure Access

Access to Kalderos' systems are strictly controlled and monitored on a real-time basis to prevent a host of potential threats to the confidentiality, availability and integrity of the information maintained by Kalderos.

Kalderos enforces role based access controls (RBACs) in combination with multi-factor authentication (MFA) and minimizes access by requiring proper approvals for access only on a need-to-know basis make up part of the corporate access control policy that have been implemented across the entire Kalderos workforce. Furthermore, remote user access to Kalderos systems is controlled and restricted to the approved IP whitelisting of the remote user's source IP address with limited access to only specific systems.

3.2 Application Security

3.2.1 Web Application Security

As part of our commitment to protecting customer data and website transactions, Kalderos has implemented a best-in-class Web Application Firewall (WAF). The WAF automatically identifies and protects against attacks aimed at Kalderos web applications and APIs. The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP) in the OWASP Top 10 and similar recommendations.

Protections from Distributed Denial of Service (DDoS) attacks have also been implemented, helping to ensure that Kalderos' web applications and APIs remain highly available. These tools actively monitor real-time traffic at the application layer with ability to alert or deny malicious behavior based on behavior type and rate.

3.2.2 Development and Release Management

- SonarQube: An open-source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs, code smells and security vulnerabilities in all programming languages we use.
- Code reviews: We protect mainline branches so that no code can be committed without someone other than the author reviewing proposed changes.
- Pull request approvals: All proposed commits require pull request approval by another developer.
- Control environments: Development, internal testing, external beta testing and production are all hosted in separate, access controlled environments.
- Separation of duty: Developers write code and technical operations staff create/configure and promote compiled versions to production environments.
- Post-deployment vulnerability scans: We use Rapid7's Insight AppSec to automatically crawl and assess deployed applications to identify code and architecture vulnerabilities. Results from these scans can be forwarded to our project management and DevOps tools for remediation. We regularly engage external security vendors to perform software code analysis and penetration tests against our systems and environments.

3.2.3 Vulnerability Management Program

Native Azure vulnerability scanning has been enabled across Kalderos' entire Azure deployment, providing the perfect complement to the use of market-leading expert third-party vulnerability scanning services. Weekly scan reports are received and addressed by Kalderos technical teams. Web application penetration testing is carried out at least annually by independent contracted third-party cybersecurity teams.

Kalderos documents and tracks reported vulnerabilities, and develops and executes remediation plans. Additionally, remediation plan progress and issue resolution are addressed during semi-monthly DevSecOps meetings and during quarterly IT Risk Management meetings.

3.3 Customer Data Protection and Classification

3.3.1 Policies on Data Protection and Classification

Kalderos recognizes the importance and criticality of protecting our customers' confidential data and has developed a data protection and classification policy that is comprised of several sub-policies, including a Data Handling Policy, Data Retention Policy, Data Destruction Policy and Organizational Privacy Policy.

These policies are required to be reviewed and accepted by the entire Kalderos workforce at the time of hire and then at least annually thereafter. Data at Kalderos can be classified as public, private and confidential.

3.3.2 Third-Party Vendor Risk Assessment

The Kalderos information security team maintains a robust vendor risk management program, performing security and privacy risk assessments for each candidate vendor prior to vendor contract execution. Each candidate vendor is required to complete Kalderos' online vendor security assessment questionnaire and is assigned a risk score based on questionnaire responses. From there, Kalderos supplies vendors with verifiable security attestation documentation.

3.3.3 Data Encryption In-Transit and At-Rest

Kalderos' web applications are deployed utilizing end-to-end encryption. API calls, user login activities and authenticated user sessions are encrypted in-transit using TLS 1.2 and 2048 bit keys. Data stored at-rest on servers and within databases use AES-256 encryption.

Encryption key management and key rotation for both data in-transit and data at-rest encryption are managed by Kalderos via key vault. Encryption keys are hashed using SHA256 hash with eight character randomized salt.

3.3.4 Application Login Security

Kalderos applications require users to authenticate over a TLS 1.2 encrypted session using a username and password. A uniform password policy is enforced, requiring a minimum of eight characters and a combination of lower and upper case letters, special characters and numbers. Users cannot change the default password policy.

Upon successful login the user receives a cryptographically signed token that is then submitted and verified on all calls to services that allow for reading and writing of data.

3.4 Privacy

The privacy of our customers' user information is one of our top considerations. As described in our Privacy Policy, the purposely minimized amount of personal information we collect is for the sole purpose of supporting customers and improving customer experience when using our products and services. Kalderos will never sell or share your personal information with third parties.

3.4.1 Data Retention Policy

Customer data is retained for only as long as required for us to provide contracted services. In some cases, regulatory or statutory requirements may require we maintain your data for one (1) year after your agreement with us has ended in which this data is anonymized, encrypted, and backed up into an offline repository until the expiration of the one (1) year period has been reached.

3.4.2 Privacy Program Management

Kalderos' security, human resources, outside counsel and several other teams collaborate to ensure we maintain an effective and continuously improving privacy program. Information on our commitment to your privacy and your data is described in more detail in our Privacy Policy.

3.5 Disaster Recovery and Business Continuity

3.5.1 System Reliability

Our Web UI applications are Single Page Applications (SPA) and so are downloaded in their entirety on-time per single-user session. After the download, the app effectively runs in the user's web browser and only exchanges data with the API. Kalderors' APIs are configured to scale both up and out using a combination of automatic load-based scaling and manual configuration based scaling. Our APIs are further configured for multi-region failover.

3.5.2 System Recovery

Web applications are entirely stateless, scaled and configured for failover across geographic regions. Individual instances are entirely recoverable by code deployment.

Databases are configured for Zone Redundancy (automatic failover within a geographic region) and Geo Replication (failover to a continuously updated replica in a different geographic US region).

3.5.3 Backup Strategy

Databases are point-in-time recoverable any time within the last 35 days.

3.6 Corporate Security

3.6.1 Workforce Authentication and Authorization

Kalderos enforces an industry standard password policy. Our policy requires changing passwords every 90 days with a minimum password length of eight characters that include complexity requirements, including special characters, upper and lower case characters, and numbers.

All Kalderos workforce members are required to register and utilize the company-issued password management tool on the date of hire – no exceptions. Furthermore, all Kalderos workforce user accounts are provisioned with MFA fully enforced that requires the use of authenticator.

3.6.2 Access Management

Access to systems and applications at Kalderos is granted via an approved request and level of access is granted based on a role-based access control (RBAC) model. Furthermore, assess is granted only on a need-to-know basis and for only as long as required to complete an assigned task or assignment. Periodic access reviews are completed and documented across the enterprise.

3.6.3 Background Checks

Kalderos' Hiring Policy requires all candidate employees and contingent workers to complete a pre-screening background check prior to their start date. Kalderos has contracted with a reputable third party agency to conduct pre-employment background verifications on our behalf that consist of previous employment, education, credit reports, identity and criminal history. Kalderos and our third party agency adhere to local laws that prohibit or restrict certain types of background checks.

3.6.4 Security Policy Training

Kalderos workers are required to review and accept numerous policies at the time of hire and remain accessible to the workforce via our governance, risk and compliance online platform. Training compliance is periodically measured and reported to Kalderos management. Policies and internal controls are reviewed at least annually and undergo continuous improvement to accommodate changes in technology and company structure.

3.6.5 Security Awareness

Kalderos takes the security of its workforce seriously and has partnered with a best-in-class security awareness platform vendor to provide structured, effective, and measurable security awareness training across the Kalderos enterprise.

3.7 Incident Management

Kalderos has enabled 24/7/365 monitoring, detection and response for security related events (e.g., malicious activity or anomalous alerts). Kalderos triages and escalates incidents based on risk.

For critical incidents, the Kalderos CIRT (Central Incident Response Team) is notified and deployed to develop an action plan quickly and effectively. The CIRT conducts periodic incident response tabletop exercises as part of our commitment to incident management and continuous process improvement.

4.0 Compliance

Operating entirely in the US, Kalderos maintains compliance to all federal and state privacy laws. More Information on our commitment to privacy can be found within our Privacy Policy.

Kalderos' information security program aligns to the ISO 27001/2 and NIST 800-53 Frameworks. Our SSAE18 SOC1 Type I and SSAE18 SOC2 Type I attestation reports can be made available to qualifying requestors under NDA.