CODEKEEPER

Security Overview

Codekeeper 2019

Source Code Escrow for Developers

www.codekeeper.co

Security Practices

As you might imagine security related system procedures are at the core of our organization.

Cloud Security

Infrastructure

Our data center partner provides several security capabilities and services to increase privacy and control network access. These include:

- Network firewalls and web application firewall capabilities
- Encryption in transit with TLS across all services
- Connectivity options that enable private, or dedicated, connections from your office or on-premises environment

DDos Mitigation

Availability is of paramount importance in the cloud. A combination of services may be used to implement a defense in depth strategy and thwart DDoS attacks. Services designed with an automatic response to DDoS help minimize time to mitigate and reduce impact.

Data Encryption

We utilize encryption to add an additional layer of security to your data at rest in the cloud, using scalable and efficient encryption features. They include:

- Data encryption
- Flexible key management
- Encrypted message queues

Data Center Security

Our data center partners provide you with multi-leveled security and practices.

SECURE DESIGN

SITE SELECTION

Prior to choosing a location, our data center partner performs initial environmental and geographic assessments. Data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our storages are built to be independent and physically separated from one another.

REDUNDANCY

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to a N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AVAILABILITY

Our data center partner has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations. Each location is engineered to operate independently with high reliability. Locations are connected to enable you to easily architect applications that automatically fail-over between locations without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of locations and data replication, our data center partner can achieve an extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

CAPACITY PLANNING

Our data center partner continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. Our data center partner maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

BUSINESS CONTINUITY & DISASTER RECOVERY

BUSINESS CONTINUITY PLAN

The Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios.

PANDEMIC RESPONSE

Our data center partner incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

PHYSICAL ACCESS

EMPLOYEE DATA CENTER ACCESS

Our data center partner provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

MONITORING & LOGGING

DATA CENTER ACCESS REVIEW

Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

DATA CENTER ACCESS MONITORING

Our data center partner monitors our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs.

They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

SURVEILLANCE & DETECTION

CCTV

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

DATA CENTER ENTRY POINTS

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilizes multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

INTRUSION DETECTION

Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication.

DEVICE MANAGEMENT

ASSET MANAGEMENT

Assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

OPERATIONAL SUPPORT SYSTEMS

POWER

Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. Data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

CLIMATE AND TEMPERATURE

Data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

FIRE DETECTION AND SUPPRESSION

Data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

LEAKAGE DETECTION

In order to detect the presence of water leaks, our data center partner equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

INFRASTRUCTURE MAINTENANCE

EQUIPMENT MAINTENANCE

Our data center partner monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

ENVIRONMENT MANAGEMENT

Our data center partner monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

GOVERNANCE & RISK

ONGOING DATA CENTER RISK MANAGEMENT

Our data center partner performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

THIRD-PARTY SECURITY ATTESTATION

Third-party testing of data centers, as documented in our third-party reports, ensures our data center partner has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.