Security & Architecture Flycode

Table of Contents

Security & Architecture

Introduction

Enterprises increasingly rely upon third-party software and services to handle business-critical processes and operations. Whether on-premises or in the cloud, these solutions must provide a level of security that protects critical company data and minimizes risk.

Flycode Inc helps engineers ramp-up to new codebases at ease and speed optimizing team productivity, independent work and time-to-value...

Flycode Inc provides a secure, reliable and resilient Software-as-a-Service platform, which has been designed from the ground up based on industry best practices. Flycode Inc's security standards and practices are backed by a multi-layered approach that incorporates best practices for preventing security breaches, as well as ensuring data integrity, availability, confidentiality and privacy.

The below reviews the network and hardware infrastructure, software and information security that Flycode Inc includes as part of this platform.

Data Center Infrastructure

Flycode Inc hosts the Software-as-a-Service production environments in the Google Cloud Platform global infrastructure. Servers at the data center are located in a secured location with security measures implemented to protect against environmental risks or disaster. Google Cloud Platform (GCP) designs and manages its infrastructure in alignment with the following regulations, standards, and best-practices: ISO 27001, SOC 1/SSAE 16 (former SAS70), SOC 2, SOC 3, PCI DSS Level 1, HIPAA, FedRAMP.

GCP constantly updates its compliance programs. For full and up to date list see:

https://cloud.google.com/security/compliance

GCP Data Centers

Google Cloud Platform data centers are serving the highest industry standards in perimeter, infrastructure, data and environmental layers. Controls are implemented to cover secure design, business continuity and disaster recovery, physical access, monitoring and logging of data center access, surveillance and detection, device management, operational support systems, infrastructure maintenance as well as governance and risk. GCP constantly updates its efforts and controls. For full and up to date list see:

https://cloud.google.com/security/infrastructure/design

Data Centers – Physical Security

Access is scrutinized – GCP restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who have a need to be present at a data center must first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once necessary work is completed.

GCP security operations centers monitor global security - GCP Security Operations Centers are located around the world and are responsible for monitoring, triaging, and executing security programs for Flycode Inc's data centers. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data center security teams. They support Flycode Inc's security with continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyze a potential security incident.

Environmental Protection

Redundancy - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to an N+1 standard.

Fire Detection and Suppression - Automatic fire detection and suppression equipment has been installed to reduce risk.

Redundant Power - The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptable Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature Controls - Maintains a constant operating temperature and humidity level for all hardware.

Flycode Inc Office - Physical Security

Physical access is limited only to approved employees and contractors with a legitimate business purpose. The Physical access to the Flycode Inc office is restricted via electronic card system to authorized personnel and by video face recognition. Visitors are accompanied while on premises.

Infrastructure Security

End-to-End Network Isolation – The Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud being intercepted.

External & Internal enforcement points - All servers are protected by restricted GCP Security Groups allowing only the minimal required communications to and between the servers. The configuration of GCP Security Groups is restricted to authorized personnel.

Subnet Segregation – Flycode Inc's environment is separated into public and private zones. Only the web servers in the public zones are accessible from the Internet by HTTPS on port 443. HTTP traffic on port 80 is used to redirect customers to a secure connection over HTTPS. All other servers, such as database, storage and services machines are restricted to the private zone.

Server Hardening – Servers are hardened according to industry best practices.

Vulnerability Management – Vulnerability scans are performed continuously. Their reports are sent to relevant personnel for risk analysis & remediation. In addition, Flycode Inc is subscribed to several relevant bulletins and notifications services which are monitored by the relevant personnel. When a relevant vulnerability has been discovered, the incident response team is alerted to determine the appropriate response.

Intrusion Prevention – Monitoring tools are implemented to detect unusual or unauthorized activities and conditions at ingress and egress points. These tools monitor server and network usage, port scanning activities, application usage and unauthorized intrusion attempts.

Distributed Denial of Service (DDOS) Protection – Multiple services to mitigate DDOS attacks are in place, as well as multi-homed network connection across multiple transit providers to achieve Internet access diversity.

Segregation between Office and Production Networks – there is a complete separation between the Flycode Inc Corporate network and the Production network. Access to the production environment is granted to authorized personnel only, and traffic between the networks is sent over an encrypted tunnel.

Regular Penetration Tests – Penetration tests are performed to the Flycode Inc Application on an annual basis, in order to determine, among others, that customers, groups of individuals, or other entities only have access to their own confidential information. The penetration test is performed by an information security consultancy group on Flycode Inc’s application and. Any identified critical and high-risk security vulnerabilities are mitigated as soon as possible after each penetration test.

Application Security

Data Encryption - Traffic between the customer client and the Flycode Inc platform is encrypted through TLS using a 128-bit AES cipher. Stored data is encrypted on a disk using a 256-bit AES cipher. Encryption between Flycode Inc customers and the Flycode Inc Application as well as between Flycode Inc sites is enabled using an authenticated SSL tunnel.

Web Application Firewall - Flycode Inc uses a WAF in order to protect against various forms of hacking and intrusion. By using an advanced behavioral analysis detection mechanism, both automated and manual intrusion techniques such as SQL Injections, Cross Site-Scripting, known vulnerabilities and DoS/DDoS attacks are detected and blocked. Zero-day exploits are mitigated by denying all traffic which does not conform to a strict, fine-grained rule-set of application specifications. Based on a large, comprehensive, and growing database of web-related vulnerabilities, mitigation for new attack patterns are continuously added. The system automatically blocks suspicious activities and issues alerts 24/7.

Password Policy - Users are identified using a user ID/password combination. Strong password configuration settings, where applicable, are enabled on the Flycode Inc's production servers, application and database servers including: (1) forced password change at defined intervals, the password expires after 4 months (2) a minimum password length must be at least 8 characters long (3) a limit of five(5) incorrect attempts to enter a password before the user ID is suspended/locked, (4) password complexity, contain at least one uppercase, lowercase and digit character and (5) password history, the last three passwords may not be re-used. For most critical resources Multi-Factor authentication (MFA) is enforced.

Segregation of Customer Data - Flycode Inc employs a login system and authorization mechanism based on industry best practices which has been validated by third-party security consultants. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data.

Operational Security

Secure Data Transfer - Any communication and data transfer between the different Flycode Inc servers, the corporate network and the production environment is sent over encrypted connections, such as IPSec and SSH.

Access Restrictions - The data analysis processes are monitored and conducted by Flycode Inc personnel for business needs only. Access to Flycode Inc's production environment is restricted to personnel belonging to the Operations team and requires multi-factor authentication.

Anti-Virus and Anti-Malware Protection - Flycode Inc employs centrally managed endpoint anti-virus and anti-malware solutions for the entire infrastructure.

Configuration and Patch Management - Flycode Inc employs a centrally managed configuration management system through which a predefined configuration is enforced on its servers, as well as the desired patch levels of the various software components.

Risk Management - Risks and threats are identified and evaluated by key Flycode Inc stakeholders during a quarterly risk assessment meeting. Meeting minutes and action items for mitigation are documented, reviewed and escalated to senior management if deemed necessary.

Security Incident Response Management - Whenever a security incident of a physical or electronic nature is suspected or confirmed, Flycode Inc's engineers are instructed to follow appropriate procedures detailed in the Security Incident Response Policy. Customers and legal authorities will be notified as recurred by Privacy regulations.

Log Management - Flycode Inc has implemented a central read-only log repository which provides easy search and alerting capabilities. Actions in the Flycode Inc system are logged and log data is reviewed on a regular basis. Flycode Inc does not allow customers to access logs. However, in case of a court order or official investigation, Flycode Inc provides the required information.

Disaster Recovery – Flycode Inc has both a disaster recovery plan and a business continuity plan in place, and regularly tests them to ensure they are working properly. The disaster recovery plan includes a comprehensive and established series of actions to take before, during and after a disruptive event. It includes an alternative processing site and an approach to return to the primary processing site as quickly as possible. The business continuity plan includes a comprehensive approach to quickly restore computer systems upon the event of any service interruption.

Human Resource Security

Security Awareness Training – Flycode Inc's employees undergo an information security awareness training upon joining the company, as well as periodically in conformance to Flycode Inc's information security policy. The training ensures that each group of employees receives security training according to its technical knowledge and its needs.

Secure Coding Standards and Training – Flycode Inc’s R&D team is regularly trained in secure coding practices and automatic static code analysis scanning is implemented.

Need to Report a Vulnerability?

Please email us directly at: security@flycode.com.

Responsible Disclosure: We would like to keep Flycode safe and secure. If you have discovered a security vulnerability we would greatly appreciate your help in disclosing it to us in a responsible manner. Publicly disclosing a vulnerability can put the entire Flycode users at risk. If you have discovered a possible vulnerability we would greatly appreciate you emailing us at security@flycode.com.

Any security emails are treated with the highest priority as the safety and security of our service is our primary concern.

Contact Us

Have a question, concern, or comment about Flycode security? Please contact us.