Public Security Policy

Click here for the latest online version:
https://www.gitguardian.com/legal/public-security-policy

Security is part of our DNA, along with transparency. We're transparent with our security program so our users can be informed and feel safe using our products and services.



Since 2022, GitGuardian has successfully maintained compliance with AICPA Service Organization Control (SOC) 2 Type II audit standard. Annual audits confirms that GitGuardian's information security practices, policies, procedures, and operations meet the SOC 2 standard.

GitGuardian is audited by Prescient Assurance, a leader in security and compliance certifications for B2B, SaaS companies worldwide. Prescient Assurance is a registered public accounting in the US and Canada and provide risk management and assurance services which includes but not limited to SOC 2, PCI, ISO, NIST, GDPR, CCPA, HIPAA, CSA STAR.

The document below provides a high-level overview of the security practices put in place at GitGuardian.

GitGuardian Security Program

GitGuardian’s security program includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data and is appropriate for the nature, size and complexity of GitGuardian's business operations.

GitGuardian follows the AICPA’s SOC2 Type II security standard’s requirements and reviews its controls annually with qualified and impartial independent external auditors.

GitGuardian’s security team develop, maintain, review and approve GitGuardian security policies. GitGuardian policies and operating procedures related to security, confidentiality, integrity and availability are accessible by all GitGuardian personnel via its documentation management tool. Security policies are reviewed, updated (as needed), and approved on an annual basis. GitGuardian personnel are required to review and acknowledge security policies during onboarding and annually thereafter.

Human Resources Security

During hiring, all GitGuardian contractors and employees undergo background checks prior to being engaged or employed by us in accordance with local laws and industry best practices. In addition, GitGuardian enters into employment contracts that require protection of personal data and confidential information both during and after the employment period.

All GitGuardian personnel are required to complete security awareness and privacy training at least annually. GitGuardian conducts periodic security awareness education to give personnel direction for creating and maintaining a secure workplace.

GitGuardian maintains a disciplinary process to take action against personnel that do not comply with company policies, security policies included.

During offboarding, access to GitGuardian systems and networks is disabled promptly upon notification of termination of personnel.

Asset Management

GitGuardian uses endpoint detection and response (EDR) technology on all GitGuardian endpoints to monitor for viruses and malware. Endpoint devices are scanned in real-time and anti-virus agent monitoring ensures that regular scans are conducted. The EDR technology automatically pushes updated virus definitions to all endpoints.

All endpoints have full-disk encryption and are monitored using industry recognized tools which alert IT administrators of discrepancies between GitGuardian security policies and a user's endpoint settings.

GitGuardian maintains an inventory of its corporate hardware, software and cloud infrastructure assets. Additionally, GitGuardian classifies information in accordance with its Data Management Policy.

Access Control

GitGuardian grants access to assets and sensitive information on a need-to-know basis based on role. Access is controlled based on the principle of least privilege, meaning users have only the level of access required to perform their job functions. Additionally, we enforce single-sign on and multi-factor authentication. GitGuardian third parties do not have access to production systems.

We monitor and log access to all production environments for security purposes. Additionally, access is audited and baselined to meet our security and compliance requirements.

Physical Security

GitGuardian’s offices are collaboration spaces for its employees and none of the Services are hosted from its offices.

GitGuardian grants office access based on employees’ geographic location and removes access as part of the offboarding process. Access to GitGuardian offices is managed by a badging system that logs access, including any unauthorized attempts, which are denied.

GitGuardian production infrastructure is hosted in AWS data centers. AWS manages physical and environmental security controls for GitGuardian production servers, including back-up power, physical access control, HVAC

systems, and fire suppression equipment to help protect servers and ultimately your data. Lean more about AWS' data center controls here or here. These controls are annually validated to ensure they comply with SOC2 physical security standards.

Data Security

GitGuardian uses industry-standard encryption techniques to encrypt Customer Data at rest and in transit using TLS1.2, AES-256-CBC or greater encryption standards. All connections are authenticated and encrypted using industry standard encryption technology.

GitGuardian removes all customer data at the end of service relationship.

Logging and Monitoring

GitGuardian continuously monitors application, infrastructure, network, data storage space and system performance. GitGuardian utilizes a security information event monitoring (SIEM) system to pull real-time security log information from servers, firewalls, routers, intrusion detection system (IDS) devices. The SIEM is configured to send the GitGuardian security team alerts and is monitored on an ongoing basis. Logs contain details on the date, time, source, and type of events. Logs are retained for 365 days. GitGuardian reviews this information and remediates, as appropriate, potential security risks.

Network Security

GitGuardian utilizes AWS network perimeter defense solutions, as well as internal IDS and firewalls, to monitor, detect and prevent malicious network activity. GitGuardian's security team takes appropriate action to respond to anomalous activity.

Our network security architecture consists of multiple entirely separate environment. Each environment has its own VPC and each service within that environment is isolated on a dedicated subnet. By default, all communication between services and subnets are denied. Necessary communication is configured with security groups. Rule changes follow the GitGuardian change

management process and require approval by designated approvers. Rules are annually reviewed to ensure that only necessary communications are allowed.

Secure Development

GitGuardian's software development life cycle (SDLC) process governs the acquisition, development, implementation, configuration, maintenance, modification and management of GitGuardian's Services, including ensuring alignment with GitGuardian security policies.

All development of new products, tools, and services, and major changes to existing ones, undergo a design review to ensure security requirements are incorporated into proposed development. All new systems and services are evaluated prior to being deployed to production.

GitGuardian utilizes a code versioning control system to maintain the integrity and security of the application source code. Prior to the final release of a new version of the Services to the production environment, code is tested in non-production environments.

GitGuardian deploys third party penetration testing and vulnerability scanning of all production and Internet facing systems on a regular basis. More specifically, we perform static and dynamic software application security testing of all code, including open source libraries, as part of our software development process.

GitGuardian follows secure coding guidelines which are reviewed and updated regularly and available to employees via GitGuardian's documentation management tool. GitGuardian developers receive annual secure coding training.

Third Party Security

GitGuardian leverages a number of third party applications and services in support of the delivery of our products to our customers. GitGuardian's Security team has established a vendor management program that sets forth the requirements to be agreed upon when GitGuardian engages with third parties or external vendors. These engagements are designed to assess the technical, physical, and administrative controls in place and to ensure they are commensurate with the expectations of GitGuardian and its customers.

GitGuardian evaluates the security controls and assurance reports for its vendors on an annual basis.

For a complete list of GitGuardian's subprocessors, please visit https://www.gitguardian.com/legal/subprocessors.

Incident Response and Notification

GitGuardian has an incident response plan, including a process, to assess, escalate, and respond to identified security incidents that impact GitGuardian, GitGuardian customers, or any GitGuardian or customer data. The incident response plan is reviewed and updated at least annually. Customers affected by a security incident are notified within 48 hours of GitGuardian becoming aware.

Risk Management

GitGuardian's security risk assessment policy and process enable GitGuardian to identify and remediate potential threats to its infrastructure. GitGuardian assigns risk ratings to all identified risks, and remediation is managed by security personnel. Executive management is kept apprised of the risk posture of the organization.

Vulnerability Management

GitGuardian monitors for vulnerabilities across its tech stack and assets on an ongoing basis. GitGuardian conducts monthly internal and external vulnerability scans using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated, documented and remediated to address the associated risks. GitGuardian also manages a private bug bounty program and annual external penetration tests conducted by an independent third party. Findings from these tests are evaluated, documented and remediated.

Change Management

GitGuardian's change management procedures require planning and testing of changes, managerial approval, and communication to stakeholders where necessary. Emergency changes are documented and reviewed, and a rollback process is in place for unsuccessful deployments. These measures ensure that

changes do not negatively impact information security or operations. Change documentation and approvals are maintained in a ticketing system.

GitGuardian uses dedicated environments separate from production for development and testing activities. Access to move code into production is limited and restricted to authorized personnel.

Business Continuity Plan

GitGuardian relies on AWS' redundancy & hot-standby features. Our compute and storage resources are spread across multiple separate AWS data centers, and are capable of seamless fail-over, to ensure maximum availability. In addition, all mission critical data stores are backed up daily to a remote AWS location, and backups are kept for 14 days. All backups are encrypted, and restoration tests are carried out annually to ensure disaster recovery readiness.

GitGuardian maintains a Business Continuity Plan and a Disaster Recovery Plan to manage significant disruptions to GitGuardian operations and infrastructure. These plans are reviewed, updated (as needed) and approved annually. GitGuardian conducts business continuity exercises at least annually to evaluate GitGuardian tools, processes and subject matter expertise in response to specific incidents.

Disclosure

GitGuardian hosts its private Bug Bounty Program with YesWeHack. If you're an independent security expert or researcher and believe you've discovered a security-related issue on our platform, we appreciate you disclosing the issue to us responsibly and thank you for your time and expertise. To do so, please follow our public Vulnerability Disclosure Policy, and use this form to submit your report.

GitGuardian does not currently invite members of the wider public to its private Bug Bounty Program.

Questions? Feedback?

If you have questions or feedback, feel free to reach out to us at security@gitguardian.com.