Sourcegraph

Security Exhibit

Sourcegraph has developed and implemented and will consistently update and maintain as needed: (i) a written and comprehensive information security program in compliance with Law; and (ii) reasonable policies and procedures designed to detect, prevent, and mitigate the risk of security incidents (the "**Security Program**"). Sourcegraph will implement the Security Program on an organization-wide basis and will include, at a minimum, the following safeguards. Sourcegraph will not make any material changes to the Security Program during the Term of the Agreement that would adversely impact Customer or the protection of Customer Confidential Information without Customer's prior written consent. Capitalized terms used below have the meaning set forth in the Terms.

Security Control Category	**Safeguard**
Securing Customer Content	
Encryption	1. Implement encryption key management procedures. 2. Encrypt Customer Content in transit (TLS 1.2+) and at rest using a minimum of AES-128 bit cipher.
Access controls	3. Maintain technical, logical, and administrative controls designed to limit access to Customer Content. 4. Restrict privileged access to the Customer Content to authorized users with a business need. 5. Review personnel access rights on a periodic basis. 6. Maintain policies requiring prompt termination of access to Customer Content after termination or reassignment of an employee. 7. Implement access controls designed to authenticate users and limit access to Customer Content. 8. Maintain multi-factor authentication processes for Sourcegraph employees with access rights to Sourcegraph production systems containing Customer Content. 9. Assign unique User IDs to authorized individual users to access systems that contain Customer Content. 10. Maintain technical controls and audit policies to ensure that any access to Customer Content is logged.
Communications security	11. Require internal segmentation to isolate production systems hosting the Service from non-production networks. 12. Require periodic reviews and testing of network controls, at least annually.
System control	13. Assign responsibility for security, changes, and maintenance for all information systems processing Customer Content.
Data retention	14. Maintain policies establishing data retention and secure destruction requirements.
Audit and logging	15. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

	16. Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Securing our software and business	
Software development	17. Establish and follow a secure software development lifecycle to ensure that security and privacy considerations are factored into each phase of the development process.
Annual penetration tests	18. Contract with independent third parties to perform penetration testing and vulnerability scanning on the Services at least annually. 19. Any remediation items identified as a result of the assessment are resolved as soon as possible on a timetable commensurate with the risk. 20. Upon request, Sourcegraph will provide summary details of the tests performed, findings, and whether the identified issues have been resolved.
Vulnerability management	21. Perform periodic network and application vulnerability testing, manual or automated, at least once every year. 22. Implement procedures to document and address vulnerabilities discovered during vulnerability and penetration tests.
Security and privacy training	23. Require all employees to undergo information security awareness training at time of hire and on an annual basis. 24. Require all employees to acknowledge in writing, at the time of hire, that they will adhere to information security policies and protect Customer Content.
Information security incident management	25. Monitor the access, availability, capacity and performance of the Services, and related system logs and network traffic using monitoring software and services. 26. Maintain incident response procedures for identifying, reporting, and acting on Security Incidents. 27. Conduct exercises to simulate security incident and response at least once a year. 28. Implement plans to address gaps discovered during incident response exercises. 29. Establish security incident response capabilities and train personnel to respond to incidents.
Risk assessment	30. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls. 31. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur.
Asset management	32. Maintain a data classification standard based on data criticality and sensitivity. 33. Implement procedures to clearly identify assets and assign ownership of those assets. 34. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 35. Centrally manage workstations via endpoint security solutions for deployment and management of endpoint protections.

Keeping our Services reliable	
Business continuity and disaster recovery	36. Establish, document, implement, and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. 37. Conduct scenario-based testing annually.
Security governance and compliance	
Security control testing	38. Engage an independent external auditor to conduct annual reviews of Sourcegraph's security practices against recognized audit standards, such as SOC 2 Type II audits.
Verification rights	39. No more than once per calendar year, use commercially reasonable efforts to respond to reasonably scoped questionnaires from Customers to verify Sourcegraph's security practices.
Information security policies	40. Create information security policies, approved by management, published and acknowledged by all employees. 41. Review and update policies at planned intervals to maintain their continuing suitability, adequacy, and effectiveness.
Vendor security management	42. Maintain a risk-based review and approval process of vendors to ensure they are taking appropriate technical and organizational measures. 43. Third-party service providers whose services involve access to confidential information or Customer Content must agree contractually to data privacy and security commitments based on their level of access and handling of information.
Governance	44. Assign roles and responsibilities for information security to respective owners to develop, implement, and manage Sourcegraph's administrative, physical, and technical safeguards to protect the security, confidentiality, and integrity of Customer Content.
Compliance	45. Establish procedures designed to ensure applicable statutory, regulatory, and contractual requirements are adhered to across the organization.