Trust Center

Cursor

Modern engineering organizations of all sizes use Cursor to accelerate and reshape the way code is written, read, and edited. Over 30,000 companies trust Cursor as their IDE of choice.

Cursor operates a continuously monitored and 3rd-party audited security program. This page provides access to trust resources including policies, audits, pentests, and real-time status against security controls.

Cursor Security Page

Overview Resources Controls Subprocessors FAQ

Controls

Infrastructure security

CONTROL	STATUS
Encryption key access restricted The company restricts privileged access to encryption keys to authorized users with a business need.	
Remote access encrypted enforced The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	
Network segmentation implemented	

The company's network is segmented to prevent unauthorized access to customer data.

Network firewalls reviewed

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

Network firewalls utilized

The company uses firewalls and configures them to prevent unauthorized access.

Organizational security

CONTROL	STATUS
Confidentiality Agreement acknowledged by contractors The company requires contractors to sign a confidentiality agreement at the time of engagement.	
Confidentiality Agreement acknowledged by employees The company requires employees to sign a confidentiality agreement during onboarding.	
Performance evaluations conducted The company managers are required to complete performance evaluations for direct reports at least annually.	

Product security

CONTROL	STATUS
Data encryption utilized The company's datastores housing sensitive customer data are encrypted at rest.	
Control self-assessments conducted	

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.

Penetration testing performed

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

Data transmission encrypted

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

Vulnerability and system monitoring procedures established

The company's formal policies outline the requirements for the following functions related to IT / Engineering:

- vulnerability management;
- system monitoring.

Internal security procedures

CONTROL	STATUS

Continuity and Disaster Recovery plans established

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.

Continuity and disaster recovery plans tested

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

Cybersecurity insurance maintained

The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

Configuration management system established

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

Change management procedures enforced

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

Production deployment access restricted

The company restricts access to migrate changes to production to authorized personnel.

SOC 2 - System Description

Complete a description of your system for Section III of the audit report

Whistleblower policy established

The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.

Board oversight briefings conducted

The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.

Board charter documented

The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.

Board expertise developed

The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.

Board meetings conducted

The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.

System changes externally communicated

The company notifies customers of critical system changes that may affect their processing.

Organization structure documented

The company maintains an organizational chart that describes the organizational structure and reporting lines.

Roles and responsibilities specified

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

Support system available

The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.

System changes communicated

The company communicates system changes to authorized internal users.

Access requests required

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

Incident response plan tested

The company tests their incident response plan at least annually.

Company commitments externally communicated

The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).

External support resources available

The company provides guidelines and technical support resources relating to system operations to customers.

Service description communicated

The company provides a description of its products and services to internal and external users.

Risk assessment objectives specified

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

Risks assessments performed

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

Data and privacy

CONTROL	STATUS

Customer data deleted upon leaving

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.