KYENAI ENTERPRISE SECURITY RESOURCE

Cursor Enterprise Security Assessment: 30 Administrator Controls

Version 1.0.0 | Verified 2026-07-30 | CC BY 4.0 | PDF, CSV, and JSON editions

Public vendor claims are separated from KyenAI operational recommendations. Buyers must verify account, plan, region, model, workspace, console, and contract-specific behavior.

Responsibility matrix

Owner	Accountable for
Cursor workspace owner	Organization settings, roles, groups, and feature enablement
Identity admin	SSO, SCIM, MFA, lifecycle, and emergency access
Security and privacy	Privacy Mode, data flows, tools, logging, risk acceptance, and incident handling
Platform engineering	Repository, model, MCP, sandbox, hook, and agent policies
Legal and procurement	MSA, DPA, retention, processors, notification, audit, and exit terms

30 administrator controls

01 Enforce SSO Identity

OWNER	Identity admin
GUIDANCE	Require SAML or OIDC SSO and disable local login where the plan permits it.
VERIFY	Sign in with an assigned user and attempt a local-login bypass.
PASS	Assigned users authenticate through the approved IdP and local bypass is blocked.
CHECK	Verify supported IdP, enforcement scope, break-glass behavior, and domain claim in the admin console.
BASIS	Official public basis

02 Automate SCIM lifecycle Identity

OWNER	Identity admin
GUIDANCE	Provision and deprovision users and groups from the authoritative directory.
VERIFY	Create, update, suspend, and delete a test user through SCIM.
PASS	Every lifecycle event reaches Cursor within the documented service window.
CHECK	Verify group mapping, seat removal, token revocation, and plan availability in the contract and console.
BASIS	Official public basis

03 Control break-glass access Identity

OWNER	Security
GUIDANCE	Keep emergency admin access limited, monitored, and tested.
VERIFY	Review named emergency accounts and run a documented access test.
PASS	Emergency access has MFA, a named owner, an expiry or review date, and an audit trail.
CHECK	Cursor's public pages do not define a universal break-glass workflow; verify available controls.
BASIS	KyenAI operational recommendation

04 Minimize admin roles Authorization

OWNER	Cursor workspace owner
GUIDANCE	Assign organization roles according to least privilege.
VERIFY	Export or review every privileged member and business justification.
PASS	Each privileged account has a current owner and required responsibility.
CHECK	Verify the exact role catalog and permissions in the active workspace.
BASIS	Official public basis

05 Separate pilot and production groups Authorization

OWNER	Platform engineering
GUIDANCE	Use identity groups and policies to isolate experimental users from production-facing teams.
VERIFY	Compare membership, repository scope, models, MCPs, and agent rules across groups.
PASS	Pilot permissions cannot silently expand production access.
CHECK	Verify whether every required policy can be scoped by group.
BASIS	KyenAI operational recommendation

06 Enforce Privacy Mode org-wide Data governance

OWNER	Security
GUIDANCE	Enable and enforce Privacy Mode for all covered users.
VERIFY	Inspect the organization setting and test inheritance with a new member.
PASS	New and existing members inherit the enforced setting.
CHECK	Verify plan, workspace, account, and client-specific behavior in the console and agreement.
BASIS	Official public basis

07 Verify training exclusion Data governance

OWNER	Legal and security
GUIDANCE	Confirm that Privacy Mode excludes customer data from Cursor and model-provider training.
VERIFY	Map the public claim to the signed DPA or MSA and active workspace setting.
PASS	Contract language and console configuration support the same exclusion.
CHECK	Required: public marketing alone is not sufficient for the buyer's legal requirement.
BASIS	Official public basis

08 Verify model-provider retention Data governance

OWNER	Privacy
GUIDANCE	Confirm the zero-data-retention arrangement for every enabled provider and model.
VERIFY	Request the provider matrix and compare it with the model allowlist.
PASS	Each enabled model has a documented retention treatment and exception path.
CHECK	Required: validate provider, model, region, abuse-monitoring exception, and change notification in contract or trust evidence.
BASIS	Official public basis

09 Define Cursor-side retention Data governance

OWNER	Privacy
GUIDANCE	Document retention for prompts, code context, indexes, logs, analytics, support records, and backups.
VERIFY	Build a data-flow and retention table from contract, product settings, and trust evidence.
PASS	Every data class has a duration, deletion path, and accountable owner.
CHECK	Unknown until the active agreement, plan, features, and support process are reviewed.
BASIS	KyenAI operational recommendation

10 Review subprocessors Data governance

OWNER	Vendor risk
GUIDANCE	Review Cursor and model-provider subprocessors before rollout and after changes.
VERIFY	Download the current list, record purpose and location, and test change-notice handling.
PASS	All material processors are approved or have a documented exception.
CHECK	Verify contract notice period and objection or termination rights.
BASIS	Official public basis

11 Confirm data residency Data governance

OWNER	Legal and security
GUIDANCE	Map required regions to actual processing, storage, backup, and support locations.
VERIFY	Compare architecture and subprocessor evidence with policy requirements.
PASS	No unapproved region receives protected data.
CHECK	Public pages do not establish a universal customer-selectable residency option; verify contractually.
BASIS	KyenAI operational recommendation

12 Verify encryption controls Data protection

OWNER	Security
GUIDANCE	Confirm TLS in transit and AES-256 at rest claims for covered services.
VERIFY	Review trust evidence and, where available, configuration for customer-managed keys.
PASS	Required data paths meet the organization's encryption standard.
CHECK	Verify feature scope, exclusions, key ownership, and availability of CMEK in the purchased plan.
BASIS	Official public basis

13 Apply repository allowlists or blocklists Repository access

OWNER	Platform engineering
GUIDANCE	Limit which repositories agents and users may access.
VERIFY	Attempt access to one approved and one denied repository.
PASS	Approved access works; denied access fails and is logged.
CHECK	Verify whether policy is allowlist, blocklist, or both and which agent surfaces it covers.
BASIS	Official public basis

14 Protect sensitive files Repository access

OWNER	Repository owner
GUIDANCE	Use repository exclusions and product policy to keep secrets and restricted paths out of AI requests.
VERIFY	Run a controlled test against denied paths and inspect client behavior.
PASS	Restricted files are not intentionally included in prompts, indexes, or agent actions.
CHECK	Cursor describes best-effort exclusions; verify residual risk and do not treat ignore files as a secret boundary.
BASIS	KyenAI operational recommendation

15 Restrict model access Model governance

OWNER	AI platform owner
GUIDANCE	Allow only approved models and providers.
VERIFY	Compare the console allowlist with procurement and privacy approvals.
PASS	Only reviewed models are selectable or routable.
CHECK	Verify new-model defaults, router behavior, provider retention, and change control.
BASIS	Official public basis

16 Restrict MCP servers Tool governance

OWNER	AI platform owner
GUIDANCE	Allow only reviewed MCP servers and remove stale connections.
VERIFY	Attempt to connect an approved and an unapproved MCP server.
PASS	Unapproved servers are blocked; approved servers have an owner and review date.
CHECK	Verify policy coverage for desktop, CLI, cloud agents, plugins, and user-defined servers.
BASIS	Official public basis

17 Protect MCP credentials Tool governance

OWNER	Security
GUIDANCE	Issue scoped credentials per server and avoid long-lived shared secrets.
VERIFY	Inspect the credential store, scopes, rotation record, and revocation test.
PASS	Credentials are least-privileged, non-exported where possible, rotated, and revocable.
CHECK	Verify where tokens are stored and which administrators or agents can reveal them.
BASIS	KyenAI operational recommendation

18 Set global agent rules Agent governance

OWNER	Platform engineering
GUIDANCE	Configure organization-wide agent policies before broad rollout.
VERIFY	Inspect required rules and test behavior with a new user.
PASS	Mandatory rules apply to supported agent surfaces and cannot be silently bypassed.
CHECK	Verify precedence, supported clients, sync timing, and exception workflow.
BASIS	Official public basis

19 Constrain auto-run, browser, and network access Agent governance

OWNER	Security
GUIDANCE	Set conservative defaults for autonomous terminal, browser, and network actions.
VERIFY	Run controlled allowed and denied actions in each supported agent surface.
PASS	Denied actions require approval or fail; allowed actions are traceable.
CHECK	Verify differences among local, CLI, background, and cloud agents.
BASIS	Official public basis

20 Enforce sandbox policy Agent governance

OWNER	Endpoint and platform engineering
GUIDANCE	Use restricted execution for agent terminal commands where supported.
VERIFY	Test workspace boundaries, temporary-file access, network denial, and escape handling.
PASS	The configured sandbox restricts the expected files and network paths.
CHECK	Verify team-wide enforcement, bypass permissions, platform differences, and known exclusions.
BASIS	Official public basis

21 Distribute security hooks Agent governance

OWNER	Platform engineering
GUIDANCE	Use managed hooks to observe or block sensitive agent actions.
VERIFY	Trigger before-prompt and before-command hooks with allowed and denied examples.
PASS	Required hooks run, fail closed where intended, and generate reviewable evidence.
CHECK	Verify server-side distribution, tamper resistance, timeout behavior, and plan availability.
BASIS	Official public basis

22 Test prompt-injection resistance Agent governance

OWNER	Product security
GUIDANCE	Exercise untrusted repository, web, issue, and MCP content against the approved configuration.
VERIFY	Run a documented adversarial test with canary secrets and denied tools.
PASS	The agent does not exfiltrate canaries or cross the configured approval boundary.
CHECK	No public vendor page proves safety for the buyer's exact tools and data; validate locally.
BASIS	KyenAI operational recommendation

23 Enable and export audit logs Logging

OWNER	Security operations
GUIDANCE	Capture access, administrative, rule, and configuration events.
VERIFY	Change a test setting and confirm the event appears in dashboard and CSV export.
PASS	Event identity, timestamp, action, target, and outcome are available for the required period.
CHECK	Verify event catalog, retention, API or export, latency, and plan limits.
BASIS	Official public basis

24 Govern analytics and API exports Logging

OWNER	Data governance
GUIDANCE	Review adoption, usage, and AI-code metrics without over-collecting employee data.
VERIFY	Inventory dashboard fields, API outputs, recipients, and retention.
PASS	Metrics have a declared purpose, access control, retention period, and employee notice where required.
CHECK	Verify exact fields and legal basis before enabling broad reporting.
BASIS	Official public basis

25 Integrate security monitoring Logging

OWNER	Security operations
GUIDANCE	Route available audit evidence into the organization's monitoring and incident workflow.
VERIFY	Generate a high-risk test event and trace it from Cursor to the response queue.
PASS	The event is ingested, enriched, assigned, and retained under policy.
CHECK	Verify supported export or API paths and compensate for unavailable events.
BASIS	KyenAI operational recommendation

26 Obtain SOC 2 and penetration-test evidence Assurance

OWNER	Vendor risk
GUIDANCE	Request current SOC 2 Type II and penetration-test materials from the trust portal.
VERIFY	Record report period, exceptions, complementary controls, and remediation commitments.
PASS	Evidence is current and gaps are accepted by accountable owners.
CHECK	Required: verify report coverage and bridge letters; certification is not a universal guarantee.
BASIS	Official public basis

27 Confirm incident notification Assurance

OWNER	Legal and security
GUIDANCE	Set contractual notification, cooperation, evidence-preservation, and post-incident obligations.
VERIFY	Map the signed agreement to the incident response plan and contacts.
PASS	Timeframes and responsibilities meet organizational requirements.
CHECK	Public pages do not define every customer's binding incident terms; verify the MSA or DPA.
BASIS	KyenAI operational recommendation

28 Test deletion and offboarding Lifecycle

OWNER	Privacy and identity
GUIDANCE	Validate account, workspace, index, token, automation, and retained-data cleanup.
VERIFY	Offboard a test user and submit a deletion request; record each completion.
PASS	Access is revoked promptly and deletion follows the documented schedule.
CHECK	Verify backups, legal holds, logs, shared artifacts, and contract termination handling.
BASIS	KyenAI operational recommendation

29 Monitor material product and policy changes Lifecycle

OWNER	Vendor owner
GUIDANCE	Track changes to models, subprocessors, retention, security features, and acquisition status.
VERIFY	Review vendor notices monthly and compare them with the approved baseline.
PASS	Material changes create a documented reassessment before policy expansion.
CHECK	Verify notification channels and contractual change rights.
BASIS	KyenAI operational recommendation

30 Maintain an exit and portability plan Lifecycle

OWNER	Engineering leadership
GUIDANCE	Keep repository instructions, workflows, evidence, and critical automations portable to another agent.
VERIFY	Run an annual migration exercise on a representative repository.
PASS	The team can revoke Cursor access and continue critical work within the recovery objective.
CHECK	Verify export availability, data return, deletion, license termination, and dependency inventory.
BASIS	KyenAI operational recommendation

Evidence sources and citation

Cursor for Enterprise
Identity, SCIM, admin, repository, model, MCP, agent, analytics, and encryption claims
https://cursor.com/enterprise

Cursor Security
Certifications, infrastructure, Privacy Mode, client and agent security, and trust evidence
https://cursor.com/security

Data Use & Privacy Overview
Privacy Mode, model-provider handling, training, storage, and policy exceptions
https://cursor.com/data-use

Introducing Cursor for Enterprise
Hooks, team rules, analytics, audit log, and sandbox behavior
https://cursor.com/blog/enterprise

Cursor Pricing
Current plan-level enterprise controls and availability
https://cursor.com/pricing

KyenAI. (2026). Cursor Enterprise Security Assessment: 30 Administrator Controls (Version 1.0.0).
https://www.kyenai.com/articles/cursor-enterprise-organizations-governance