BRISKDATA ENGINEERING TEMPLATE | DOC ID: BD-SEC-AIAUP-008 | ADAPTABLE TEMPLATE

AI Acceptable Use Policy (AUP) Template

Approved AI Workspaces, Data Classification Rules, Human Review Standards, and Staff Sign-Off

ADAPTATION INSTRUCTIONS

Replace every bracketed field with your organization's approved tools, owners, and contractual commitments before adoption. Confirm model training opt-outs, log retention windows, access controls, and data-processing agreements (DPA or HIPAA BAA) separately for each vendor tier.

1. Policy Metadata and Scope

Policy Field	Organization Entry
Organization Name	[Organization Name]
Policy Owner and Contact	[Role / Email, e.g., Security Lead - security@example.com]
Executive / Legal Approver	[General Counsel / Managing Partner / CTO]
Effective Date and Review Cycle	[YYYY-MM-DD] | Review Cadence: [Semi-Annual / Annual]
Covered Personnel and Systems	All employees, contractors, and third-party personnel accessing company data, source code, or client records across LLMs, coding assistants, meeting transcription tools, and embedded SaaS AI features.

2. Approved AI Tools Register

Only company-provisioned workspaces listed below are authorized for internal business work. Personal or free-tier accounts must not be used for non-public company or client records.

Tool & Account Tier	Approved Use Cases	Permitted Data Tier	Required Account Controls	System Owner
[EXAMPLE - REPLACE] Enterprise LLM Workspace	Drafting internal docs, summarizing non-regulated notes	Public & Internal	SAML SSO, SCIM, training disabled, DPA signed	[IT / Security Lead]
[Approved Coding Assistant]	[Code completion, unit test drafting]	[Public / Internal repo scope]	[Business tier, training disabled, PR scan]	[Engineering Lead]
[Approved Meeting Assistant]	[Internal team call summaries]	[Internal]	[Explicit host opt-in, auto-join disabled]	[IT Operations]
[Private / VPC Model Host]	[Approved restricted workflows]	[Per written approval]	[Isolated tenant/VPC, audit logging]	[Platform / Security]

3. Data Classification and Input Rules

A vendor setting that disables model training does not automatically eliminate temporary abuse-monitoring retention, cross-border processing, or compliance obligations. Review training, log retention, and contractual terms separately.

Data Classification	Representative Records	Public / Free AI Tools	Approved Enterprise Workspace
Public	Published web copy, public documentation, open-source syntax examples, public filings.	Permitted within approved tasks	Permitted
Internal	Internal SOP drafts, non-sensitive operational notes, anonymized schemas, internal templates.	Prohibited	Permitted when SSO, retention, and DPA terms are verified
Restricted / Regulated	Customer PII, HIPAA PHI, PCI cardholder data, CUI/ITAR, M&A financials, privileged legal work, proprietary algorithms.	Prohibited	Prohibited unless covered by specific written Security/Legal approval and applicable BAA/enclave controls
Secrets & Credentials	API keys, passwords, OAuth tokens, private keys, connection strings, session cookies.	Strictly Prohibited	Strictly Prohibited (never paste secrets into prompts or uploads)

4. Operational Guardrails and Human Verification

- **Identity and Provisioning:** Approved AI workspaces must authenticate through company SSO with multifactor authentication so access revokes promptly upon role change or offboarding.
- **Meeting Recording and Transcription Bots:** Automated transcription or note-taking bots must not auto-join client, legal, board, HR, or financial calls without advance notice and host consent.
- **AI-Assisted Software Development:** Code generated or refactored with AI tools must pass peer pull-request review, automated tests, dependency license checks, static analysis, and secret scanning before deployment.
- **Human Review and Accountability:** AI tools can invent citations, legal references, calculations, and edge-case behavior. The person using an AI output remains responsible for verifying every fact, calculation, permission check, and statement before external delivery or production use.

5. Exceptions, Incident Reporting, and Staff Sign-Off

Report accidental submission of Restricted data, credentials, or client records immediately to [Incident Channel / security@example.com] so credentials can be rotated and vendor deletion procedures initiated. Written exception requests must identify the business task, data classification, vendor terms, compensating controls, and expiration date.

Employee Name & Title	Department	Signature	Date
[Printed Name and Title]	[Department]	_____	YYYY-MM-DD

Template Reuse Note: You may copy and adapt this template for internal operations within your organization. Replace bracketed placeholders and remove example entries before adoption. briskData branding and third-party trademarks remain the property of their respective owners.