

ENTERPRISE AI USAGE GUIDE

Do not simply ban AI. Create a safe usage framework.

Enterprise AI Usage Guide

Short, practical principles for employees and developers to use AI tools in support of business goals while respecting data-security and corporate-responsibility boundaries.

EMPLOYEES**DEVELOPERS****SECURITY & IT****A SOFTBYT LABS PRODUCT FAMILY • PUBLIC GUIDE**

ENTERPRISE AI USAGE GUIDE

Five core principles

Safe AI adoption depends on behavior, authorization, and verification as much as technology.



ENTERPRISE AI USAGE GUIDE

Daily-use checklist

Four practical controls that fit into normal work without unnecessary friction.

**When writing prompts**

Remove sensitive data, provide only necessary context, and use an approved tool.

**When sharing files**

Check classification, share only what is needed, and never expose secrets or credentials.

**When running AI agents**

Narrow the workspace, limit tools and resources, and review all resulting changes.

**When using MCP or plugins**

Use approved servers and plugins, avoid unnecessary permissions, and stop suspicious instructions.

CRITICAL CAUTIONS

Passwords / API keys

Raw employee data

Customer secrets

Unpublished commercial plans

ENTERPRISE AI USAGE GUIDE

Who is responsible for what?

Sustainable AI security emerges when policy, user behavior, and technical controls work together.

Employees

- Use approved tools.
- Apply data minimization.
- Verify outputs and report suspicious activity.

Developers

- Limit workspace and tool permissions.
- Review code and file changes before acceptance.
- Keep corporate secrets out of prompts and plugin flows.

Security & IT

- Manage inventory and policy.
- Run pilots and awareness programs.
- Monitor events, measure outcomes, and improve controls.

1

Discover

Identify the tools and usage patterns already in the organization.

2

Define

Set boundaries by data class and use case.

3

Pilot

Validate controls and training with selected teams.

4

Improve

Update policy using incidents, feedback, and usage evidence.