無料資料

AI 利用ルールのひな形

ChatGPT・Claude・Gemini・Copilot などを、禁止せずに安全に使うためのルールです。色のついた［会社名］などの部分を書き換えれば、そのまま社内ルールとして使えます。

1
区分を決める
自社の書類を「一般・社外秘・最重要」に当てはめる（第 4 条）

2
使う AI を決める
区分ごとに使ってよい AI と設定を表にする（付録 1）

3
周知して見直す
社員向け 1 枚で説明し、年 2 回見直す（第 10 条）

本文

このルールの範囲とデータの区分

第 1 条（目的）

このルールは、［会社名］（以下「会社」）の業務で生成 AI を使うときに、情報の漏えいや誤った利用を防ぎながら、AI を活用するために定めます。

第 2 条（対象者）

役員、社員、契約社員、派遣社員、業務委託先など、会社の業務で AI を使うすべての人に適用します。

第 3 条（対象となる AI）

文章・画像・コードを生成する AI、ブラウザの拡張機能、他のサービスに接続する AI（コネクタ・MCP・エージェント）、開発用の AI ツール（Claude Code、GitHub Copilot など）を含みます。

第 4 条（データの区分）

	例	AI での扱い
一般	公開済みの資料、一般的な調べもの、議事録の下書き（固有名詞なし）	**会社が許可した AI なら使ってよい**
社外秘	取引先の担当者名・連絡先、見積・契約書、社内の数字、ソースコード	**会社契約で学習に使われない設定の AI だけ**
最重要	個人のお客様の情報（住所・健康・与信など）、マイナンバー、依頼者・患者の情報、図面、認証情報・鍵 ［自社の例を足す］	**外部の AI に入れない。使う場合は社内で動く AI だけ**

本文

使い方と運用のルール

第 5 条（使ってよい AI）

会社が付録 1 に載せた AI とアカウントだけを使います。個人で契約した AI に、会社のデータを入れたり、会社のアカウント（Google・Microsoft など）を連携させたりしてはいけません。新しい AI を使いたいときは、［情シス担当］に申請します。

第 6 条（してはいけないこと）

1. 最重要のデータを、外部の AI に入力・アップロードすること
2. 社外秘のデータを、学習に使われる設定の AI に入れること
3. 他人のアカウントや共有アカウントで AI を使うこと
4. AI の出力を、確認せずに社外へ出すこと
5. 会社が許可していない拡張機能・コネクタ・MCP サーバーを接続すること

第 7 条（AI エージェントと開発ツールの設定）

1. ファイルの削除・外部への送信・コマンドの実行を、確認なしで行う設定（自動承認）をオフにします。例：Claude Code の自動承認、エージェントの自動実行
2. AI が触れるフォルダ・リポジトリを、作業に必要な範囲に限ります
3. 接続する MCP サーバー・コネクタは、付録 2 の一覧に載せたものだけにします
4. API キーやパスワードを、AI への指示やリポジトリに書きません

第 8 条（出力の扱い）

AI の出力の正しさ・権利・機密は、使う人が確認します。社外に出す資料・コード・回答は、人が確認してから出します。

第 9 条（事故のとき）

入れてはいけないデータを AI に入れた、AI が意図しない操作をした、と気づいたら、すぐに［情シス担当・連絡先］に報告します。速やかに報告したことを理由に不利益に扱いません（故意・重大な過失を除く）。会社は、必要に応じてアカウントの停止や履歴の削除を行います。

第 10 条（運用）

情シス担当は、使っている AI と接続の一覧（付録 2）を管理し、年 2 回［4 月・10 月］このルールと一覧を見直します。新しく入った人には、付録 3 で説明します。

第 11 条（他の規程との関係と記録）

このルールは就業規則・情報セキュリティ規程・個人情報保護方針と合わせて適用します。会社は、AI の利用状況（使っている AI と接続、管理画面で確認できる記録）を確認することがあり、そのことを社員に周知します。

附則

このルールは［2026 年〇月〇日］から施行します。

ルールを作るだけでは守られているか分かりません。Securiy の「AI 利用の安全設計」では、第 7 条の設定をこちらで組み、テストで本当に止まるかを確かめます。

付録 1・付録 2

使ってよい AI と、接続の一覧

付録 1　使ってよい AI

記入例

AI・アカウント	一般	社外秘	最重要	条件
ChatGPT（会社契約）	○	○	×	学習オフ・会社アカウントでログイン
Claude（会社契約）	○	○	×	同上。Claude Code は自動承認オフ
Microsoft 365 Copilot	○	△	×	開ける範囲＝AI の範囲。共有設定を先に見直す
Gemini（Workspace 契約）	○	○	×	開ける範囲＝AI の範囲。ドライブの共有を先に見直す
会議の録音・議事録 AI	○	△	×	参加者に録音を伝える。保存先と保存期間を決める
個人契約・無料版の AI（Copilot Chat 無料版を含む）	△	×	×	会社のデータ・アカウントは使わない
社内で動く AI ［導入した場合］	○	○	○	ネットにつながない端末・サーバー

付録 2　AI と接続の一覧

様式

名前	種類	使う人	読める・できること	持ち主	確認日
ChatGPT ドライブ連携	コネクタ	営業部	共有ドライブの読み取り	佐藤	2026/10/20
社内 Wiki 用 MCP	MCP	開発	Wiki の読み取りのみ	田中	2026/10/20

付録 3

社員向け 1 枚まとめ

していい

- 会社が許可した AI を、会社のアカウントで使う
- 一般のデータで、文章・調べもの・下書きに使う
- 出力は自分で確かめてから使う

しない

- 個人の AI に会社のデータを入れる
- 最重要のデータを外部の AI に入れる
- 許可していない拡張・コネクタをつなぐ

迷ったら、入れる前に［情シス担当］へ。

入れてしまったら、すぐ報告してください。報告したことで不利益にはなりません。