AI ガバナンスポリシー — Layer 1（Foundation）

10-rules-ja から自動生成（GENERATED）— 手動で編集しないこと

全社ポリシー — すべての従業員・すべての部署に常に適用される。原則：リスクが高いほど管理を強める。以下は Foundation ティア（L1）に適用される最低限のルール（レッドライン）である。

ID と承認済みツール

AUTH-001 — 会社承認済みのAIツールのみを使用すること

tiers: L1, L2, L3, L4

会社業務に使用できるのは、**会社と契約済みで、入力データが学習に使用されない**AIツールのみである。会社のデータを扱う際に**個人のAIアカウントを使用することは厳禁**である（「Shadow AI」、L1 §8）。

現行リスト（`30-registry/ai-tools.yml`）：

- Google Workspace Gemini (company)
- Claude (Team / Enterprise)

AUTH-002 — すべてのツールは @vitalify.asia アカウントでサインインすること

tiers: L1, L2, L3, L4

AIと併用するすべてのツール、すなわちAIツール（`AUTH-001`）と業務ツール／コネクタは、`@vitalify.asia` アカウントで認証すること。個人アカウントの使用は禁止する。従業員の退職時に IT がアクセス権を失効（revoke）させることができず、データの所有権を担保できず、インシデント調査のための監査ログも残らないためである。

現行リスト（`30-registry/connectors-mcp.yml`）：

- Figma
- Google Docs/Sheets/Slides/Drive
- Draw.io

AUTH-003 — 入力前に、ツールが会社管理下にあり、かつデータの入力が許可されていることを確認すること

tiers: L1, L2, L3, L4

非公開の情報を入力する前に、次の**両方**を確認すること：ツールが会社管理下にある（契約済みで、入力データが学習に使用されない）こと、**かつ**そのデータがポリシー上許可されていること。いずれかを満たさない場合 → 作業を止めて PMO に確認すること。*有料だからといって安全とは限らない。*

AUTH-004 — 新規AIツールは承認フローを経ること

tiers: L1, L2, L3, L4

新規AIツールを独断で導入してはならない。承認フロー：担当者が提案 → 直属の上長 → CoE が取りまとめ → **Dev Director** が決定 → CoE が結果を通知。承認されるまで、そのツールは**使用不可**として扱うこと。

AI に入力してよいデータ／いけないデータ

DATA-001 — 顧客データ／本番シークレットをAIに入力してはならない

tiers: L1, L2, L3, L4

次のものを入力してはならない：本番／テスト環境の認証情報（ID、パスワード、APIキー）、エンドユーザーの個人データ／顧客の生データ（テストログ、取引履歴）、社内の極秘情報（未公開の財務情報、M&A）。これは会社の **レッドライン #1** である。L2では、settings.json の `deny` リスト（シークレットファイルのパターンに対する Read/Write）によって部分的に強制される。

DATA-002 — データの3段階分類

tiers: L1, L2, L3, L4

レベル	入力してよいか
極秘（認証情報、エンドユーザーのPII、M&A）	❌ 不可 — 会社のツールであっても不可（`DATA-001` 参照）
社内業務データ（議事録、提案書、仕様書）	⚠️ 可 — **会社のツールのみ**。顧客名などの固有名詞は、社内で通常共有されているものであれば入力してよい。プロジェクト固有の例外はマネージャーに確認すること
一般情報（公開情報、調べもの、機密でない文章の校正）	✅ 可 — 制限なし

DATA-003 — 匿名化は機密度に応じて行う（一律には行わない）

tiers: L1, L2, L3, L4

COE決定（#2）：L1に従い、L2の匿名化ルールを緩和する。 すべての顧客名を匿名化する必要はない。具体的には次のとおり：

- 顧客名／固有名詞は、社内で通常共有されている（例：メール／チャットで）ものであれば **そのまま入力してよい。**
- RFP／仕様書／提案書は、シークレット、PII、社内IPを除去した後であれば **アップロードしてよい**（`DATA-004` 参照）— プレースホルダーへの置き換えは不要。
- **機密性の高い商業上の数値**（価格、単価、予算、マージン）と、`DATA-001/DATA-002` の極秘データに該当するもののみ **匿名化しなければならない。**

DATA-004 — ドキュメントのアップロード手順（RFP／仕様書／設計書）

tiers: L1, L2, L3, L4

ドキュメントをAIにアップロードする前に：**(1)** 契約上、そのドキュメントをAIで利用することが認められているかを確認すること — 不明な場合は顧客に確認するか、使用しないこと。**(2)** パスワード、APIキー、社内IPアドレス、個人データを除去すること。**(3)** 承認済みツールのみを使用すること。機密性の高いケースはPMOとともにレビューすること。

DATA-007 — AI支援によるコードはIP（知的財産）上クリーンでなければならない

tiers: L1, L2, L3, L4

成果物に含まれるAI生成コードは、**ライセンス／独自性についてレビューおよびスキャン** されなければならず（IPを「汚染」しうる GPL/AGPL コードの再現を避けるため）、人が書いたコードと同じ品質・セキュリティ基準を満たさなければならない。顧客のIP帰属条件は、他のすべてのコードと同様に、AIによるコードにもそのまま適用される。

DATA-008 — 商用ブランド資産に生成AIを使用しない

tiers: L1, L2, L3, L4

顧客に納品する、または自社のアイデンティティとして使用する最終的なブランドデザイン（ロゴ、マスコット、商標）に生成AIを使用してはならない — AIは保護された著作物を検出できない形で再現する可能性があり、「クリーン」であることを検証できない。AIはインスピレーション／ムードボード／ドラフトには使用してよいが、最終的な資産は人間のデザイナーが制作する。顧客から要望があった場合はPMOにエスカレーションすること。

DATA-011 — 業務コンテンツは承認済みAIツールにのみ送信する

tiers: L1, L2, L3, L4

ソースコード、ドキュメント、データ、ログを、現在作業に使用している承認済みAIツール以外の外部サービスに送信してはならない — pastebin、オンラインのフォーマッターや変換ツール、他のAI/LLM API、webhook テスター、公開ファイル共有リンクは使用しないこと。複数のAIツールが同じコンテンツを扱う場合は、そのすべてが承認済みでなければならない（`AUTH-001`）。エージェントは承認済みドメインからのみ取得（fetch）する（`RULES-006`）。

AI ツールの安全な設定

RULES-007 — AI は本番環境、会社または顧客のシステムを操作してはならない

tiers: L1, L2, L3, L4

AI は、会社のシステム、顧客のシステム、または本番（Production）環境に対して自律的に操作を行ってはならない。人間の承認なしに、メール送信、API 呼び出し、クラウドシステムの操作を行ってはならない。AI は、本番環境に対して直接のアクセス、操作、変更、デプロイ、コマンド実行を決して行ってはならない。対象には、デプロイスクリプトと CI/CD パイプライン、設定ファイルと環境変数、認証情報/シークレット/トークン/API キー、インフラ、データベース、クラウドリソース、運用システムが含まれる。本番用のスクリプト、認証情報、設定がソースコードやリポジトリ内に存在する場合でも、AI に許されるのは**それらのレビューと変更の提案**のみであり、本番環境に対してそれらを実行、適用、テスト、使用してはならない。特に、AI は次のことを行っては

ならない：本番のデプロイスクリプトまたはマイグレーションスクリプトの実行、本番の認証情報を使ったコマンドの実行、本番のインフラ・データベース・設定・シークレットの変更、本番のセキュリティ制御の無効化または回避、本番を対象とする CI/CD ジョブの起動。本番に関わるすべての操作は、権限を持つ人間がレビュー・承認し、**手動で実施**しなければならない。

インシデント対応

RES-001 — セキュリティインシデントを直ちに報告する

tiers: L1, L2, L3, L4

インシデント（データ漏えい、GitHub へのシークレット/認証情報のプッシュ、顧客データの露出、不審なアクセスなど）を発見した場合は、気づいた時点で `[SECURITY] Incident Report` チャンネルにて、直属の上司**および** CoE に同時に**直ちに報告**すること。詳細の確認を待たないこと。先に自分で修正しようとしないこと。報告では、何が起きたか、どこで（リポジトリ/ツール/システム）、いつ気づいたかを簡潔に説明する。

RES-002 — インシデント発生時：タスクを停止し、アクセスを失効させ、影響を追跡する

tiers: L1, L2, L3, L4

報告に加えて、対応には次の手順を含めなければならない：実行中のタスク/エージェントの**停止**、関与したエージェント/人のアクセス権・認証情報の**失効（revoke）**、影響範囲をきっかけとなった人/コマンドまで遡る**追跡**。現行の L1 §11 には「上司 + CoE への報告」しかなく、停止/失効/追跡の手順が**欠けている**。