**基本ルール：情報管理**

**1. 情報収集の範囲と方法**

* **Factory Overviewデータ収集プロセス:**
  + **生産データ:** 生産システムから自動収集（15分間隔）。
  + **品質データ:** 検査システムから自動収集（検査完了時）。
  + **メンテナンスデータ:** 設備保全システムから自動収集（イベント発生時）。
  + **AIエージェントの役割:** データ収集の監視・異常検知・集計・可視化。
* **Activityログの定義:**
  + **記録対象:** AIエージェントの判断・行動履歴、ユーザー操作、システムイベント。
  + **影響範囲:** 学習データとして使用、判断の根拠として参照、監査証跡として保存。
  + **保存形式:** 構造化データ（JSON）、非構造化データ（テキスト）の両方に対応。

**2. 顧客個人情報アクセス権限管理**

* **アクセス権付与基準:**
  + 業務遂行上の必要性（具体的な業務目的の明示）。
  + 最小権限の原則（必要最小限のデータのみアクセス可能）。
  + 時間制限（目的達成までの期限付き）。
* **アクセス管理プロセス:**
  + **申請手順:** 目的・期間・対象データの明示。
  + **承認フロー:** 直属上長→部門長→情報セキュリティ責任者。
  + **アクセスログ:** 全てのアクセス・操作を記録（5W1H形式）。
  + **権限失効:** 期限到来時自動失効、目的達成時手動失効。

**3. 部門間データ連携**

* **クロスファンクショナルデータ利用:**
  + **生産部門:** 品質データ参照権限（不良率予測）。
  + **品質部門:** 生産データ参照権限（品質トレンド分析）。
  + **メンテナンス部門:** 生産・品質データ参照権限（予防保全最適化）。
* **部門間データ共有ルール:**
  + **共有申請書:** 目的・期間・活用計画の明示。
  + **レビュープロセス:** 両部門責任者の承認。
  + **期間制限:** 最長3ヶ月（更新可）。
  + **利用報告:** 月次で活用成果を報告。

**4. AIエージェント間データ共有**

* **一時ファイル管理:**
  + **命名規則:** [送信元ID]\_[受信先ID]\_[内容種別]\_[タイムスタンプ].tmp
  + **保存場所:** 専用の暗号化一時ディレクトリ。
  + **削除ルール:** 共有完了確認後即時削除、最長24時間で強制削除。
  + **監査:** 一時ファイルの存在を定期スキャン（4時間毎）。
* **内部API連携仕様:**
  + **認証方式:** OAuth2.0ベース内部認証。
  + **データ形式:** JSON構造化データ。
  + **通信暗号化:** TLS 1.3以上。
  + **レート制限:** 1秒あたり最大10リクエスト。
  + **タイムアウト:** 30秒（大容量データ転送は例外設定）。

**5. 外部LLM選定基準**

* **規定LLM選定基準:**
  + **セキュリティ:** SOC2 Type II認証以上。
  + **プライバシー:** GDPR・CCPA準拠。
  + **処理能力:** 応答時間SLA（99.9%が3秒以内）。
  + **コスト効率:** 月間予算内（部門別上限あり）。
  + **特化機能:** 業界特化モデル優先。
* **LLM変更承認プロセス:**
  + **提案書:** 変更理由・費用対効果・セキュリティ評価。
  + **PoC:** 2週間の試験運用。
  + **承認フロー:** IT部門→セキュリティ部門→経営層。
  + **導入計画:** 段階的移行（並行運用期間設定）。

**6. 第三者データ共有ガイドライン**

* **第三者との共有条件:**
  + **目的制限:** 明示的な業務目的のみ。
  + **契約要件:** NDA・データ保護条項の締結。
  + **データ範囲:** 最小限の必要データのみ。
  + **二次利用:** 原則禁止（例外は個別承認）。
  + **共有期限:** 明確な期限設定。
* **共有データの管理:**
  + **匿名化レベル:** k-匿名性（k≧5）。
  + **追跡管理:** 透かし・アクセスログによる監視。
  + **削除確認:** 期限到来時の削除証明要求。
  + **監査権:** 定期的な利用状況確認。

**7. データ保管インフラ詳細**

* **ローカルサーバーセキュリティ:**
  + **物理セキュリティ:** 生体認証入退室管理。
  + **アクセス制御:** 多要素認証。
  + **暗号化:** AES-256（保存データ）、TLS 1.3（通信）。
  + **バックアップ:** 日次差分、週次完全バックアップ。
* **クラウド移行計画:**
  + **移行時期:** 2025年第2四半期開始。
  + **候補プロバイダー:** AWS、Azure、GCP。
  + **選定基準:** セキュリティ認証、地域法規制対応、パフォーマンス。
  + **データ配置:** 国内リージョン優先。

**8. データ保管期間と削除ポリシー**

* **保管期間分類:**
  + **顧客個人情報:** 最長5年（法規制に準拠）。
  + **取引履歴:** 7年（税法要件）。
  + **生産データ:** 10年（製品保証期間）。
  + **ログデータ:** 3年（監査要件）。
* **削除プロセス:**
  + **自動削除:** 期限到来時のフラグ設定。
  + **承認フロー:** 部門長確認→情報管理責任者承認。
  + **削除方法:** 物理的破壊（ハードウェア）、上書き消去（データ）。
  + **削除証明:** 削除完了レポート保管。

**9. UI情報管理体制**

* **コンテンツ管理責任者:**
  + **Documentation:** 技術部門。
  + **Discussions:** コミュニティ管理者。
  + **Help Center:** サポート部門。
* **AI自動更新機能:**
  + **更新可能範囲:** FAQ、使用例、トラブルシューティング。
  + **承認プロセス:** 低リスク（自動承認）、高リスク（人間によるレビュー）。
  + **更新頻度:** 週次（定期）、イベント発生時（臨時）。
  + **品質確認:** 自動言語チェック、定期人間レビュー。

**10. データガバナンス体制**

* **オーナーシップ定義:**
  + **顧客データ:** 顧客（利用権はサービス期間中）。
  + **生成データ:** 会社（顧客との契約範囲内）。
  + **学習データ:** 会社（匿名化処理後）。
* **ガバナンス体制:**
  + **データ管理委員会:** 四半期毎開催。
  + **役割分担:** データオーナー、データ管理者、データ利用者。
  + **監査体制:** 内部監査（半年毎）、外部監査（年次）。
  + **改善サイクル:** PDCAループ（レビュー→改善→実装→確認）。