情報セキュリティポリシー（基本方針・運用ルール）

アサヒモータース

制定日：2026年2月9日　/　版数：1.0　/　管理責任：経営責任者（最高情報セキュリティ責任者）

1. 目的

本ポリシーは、アサヒモータース（以下「当社」）が保有・利用する情報資産を、漏えい・改ざん・滅失・毀損・不正利用等の脅威から保護し、事業継続性および社会的信頼を確保することを目的とします。

2. 適用範囲

本ポリシーは、当社の役員・従業者（正社員、契約社員、パート、アルバイトを含む）、業務委託先・派遣等で当社情報資産を取り扱う者（以下総称して「利用者」）に適用します。また、当社が管理する端末、ネットワーク、クラウドサービス、紙媒体を含む全ての情報資産に適用します。

3. 用語・基本原則

情報資産：当社の業務により取り扱う、データ、文書、帳票、顧客情報、システム、端末、クラウドアカウント等の総称。

情報セキュリティの3要素（CIA）：機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）。

当社は、リスクに応じた対策を段階的に実施し、継続的に改善します。

4. 体制と責任

当社は、情報セキュリティを経営課題として位置づけ、以下の体制で推進します。

4.1 役割

- 経営責任者（最高情報セキュリティ責任者）：方針承認、資源配分、重大事故時の最終判断
- 情報セキュリティ責任者（IS責任者）：運用統括、教育、点検、インシデント対応の指揮
- システム管理者（必要に応じて任命）：端末・アカウント管理、設定標準化、ログ保全
- 利用者：ルール遵守、異常時の速やかな報告、自己管理（パスワード等）
- 委託先：契約で定めるセキュリティ要求事項の遵守、事故時の連絡義務

4.2 教育・周知

入社時および年1回以上、利用者に対し情報セキュリティ教育（標的型メール、パスワード、端末紛失、個人情報等）を実施します。

5. リスク管理と見直し

当社は少なくとも年1回、または業務・システム変更時に、情報資産の洗い出し、脅威・脆弱性の確認、リスク評価（影響×発生可能性）を実施し、対策優先順位を決定します。

本ポリシーは、法令改正、事故発生、業務変化等に応じて適宜見直し、版管理のうえ更新します。

6. 情報資産の管理

6.1 分類（ラベル）

情報は重要度に応じて分類し、取扱いを区別します。

- 公開：公表しても差し支えない情報（Web掲載等）
- 社外秘：社外への無断開示を禁止する情報（社内一般）
- 機密：業務上重要で、限定された範囲にのみ開示する情報（顧客情報、契約、見積等）
- 極秘：漏えい時の影響が大きく、厳格に管理する情報（口座情報、認証情報、重大インシデント資料等）

6.2 保管・廃棄

- 紙媒体は施錠保管を基本とし、不要となった紙はシュレッダー等で復元不能にして廃棄する。
- 電子データは、承認された保存先（社内共有、指定クラウド）に保存し、個人端末や私的クラウドへの保管を禁止する。
- USB等の可搬媒体は原則使用禁止。業務上必要な場合は、暗号化された媒体に限定し、IS責任者の承認を得る。

7. アクセス制御・認証

当社は最小権限（必要最小限のアクセス権）を原則とし、アカウントは個人単位で付与します。共有アカウントは原則禁止します。

- 重要なクラウドサービス／メール／重要データへは多要素認証（MFA）を必須とする。
- 退職・異動時は、当日中にアカウント権限の変更・停止を行う。
- パスワードは本書「付録A」に従う。パスワードの使い回しは禁止する。
- 管理者権限は業務上必要な者に限定し、利用状況を定期点検する。

8. 端末・モバイル・BYOD（私物利用）

業務は原則として当社が管理する端末で行います。私物端末（BYOD）利用は、IS責任者の承認と、以下条件を満たす場合に限ります。

- OS・アプリを最新状態に保ち、画面ロック、ディスク暗号化、ウイルス対策（EDR/AV等）を有効にする。
- 紛失・盗難時に遠隔ロック／ワイプ可能な設定を行う。
- 業務データを端末ローカルへ保存しない（必要時は暗号化・期限付きとする）。
- 端末の第三者利用（家族含む）を避け、やむを得ない場合は業務アカウントを必ず分離する。

9. ネットワーク・テレワーク

- 社外からの業務アクセスは、承認された方法（VPNまたはクラウドの安全なアクセス）を使用する。
- 公衆Wi-Fi利用は原則禁止。やむを得ない場合はVPNを必須とし、機密情報の閲覧・送信は避ける。
- 自宅Wi-Fiは強固な暗号化（WPA2/WPA3）と強いパスワードを設定し、初期設定のまま使用しない。
- オンライン会議は、会議ID・パスコード・待機室等の機能を活用し、無関係者の参加を防止する。

10. クラウドサービスの利用

当社は、業務で利用するクラウドサービス（メール、ストレージ、CRM等）を指定し、利用者は承認されたサービスのみを使用します。

- クラウド管理者は、MFA、アクセス権、共有リンク、外部共有設定を定期点検する。
- 顧客情報等の機密情報は、外部共有の前に承認を得る。共有は必要最小限・期限付き・パスコード付与を基本とする。
- SaaSの退会・解約時は、データの回収と削除手順を確認し、必要な証跡を保管する。

11. マルウェア・脆弱性対策

- OS・アプリ・ブラウザ・セキュリティソフトの更新を徹底し、サポート切れ製品の利用を禁止する。
- 不審なメール添付・URLを開かない。疑わしい場合はIS責任者へ転送し確認する。
- 重要システム／クラウドの設定変更は変更管理（記録・承認）を行う。

12. バックアップ・事業継続（BCP）

当社は、ランサムウェア等の被害に備え、重要データについてバックアップを取得し、復旧手順を整備します。

- 重要データは少なくとも日次でバックアップする（可能な範囲で3-2-1：3世代、2媒体、1つはオフライン/別環境）。
- バックアップからの復元テストを四半期に1回以上実施し、結果を記録する。
- 災害・停電・通信障害時の代替手段（モバイル回線、代替拠点、連絡網等）を整備する。

13. 委託先管理

当社が情報の取扱いを外部に委託する場合、委託先の選定・契約・監督を行います。

- 秘密保持契約（NDA）および再委託制限、事故時の報告義務、削除・返却、監査協力等を契約に明記する。
- 委託先のセキュリティ対策（MFA、アクセス権、保管場所等）を確認し、必要に応じ改善を要求する。

14. セキュリティインシデント対応

インシデント（疑い含む）を認知した利用者は、速やかにIS責任者へ報告します。初動の速さが被害を左右します。

- 報告目安：発見後30分以内（営業時間外も可能な範囲で連絡）。
- 初動：ネットワーク切断／端末隔離／アカウント停止等の被害拡大防止を優先。
- 証跡保全：ログ、メール、画面、時刻、操作履歴等を可能な限り保存し、自己判断で削除しない。
- 外部連絡：個人情報漏えい等が疑われる場合、法令・契約・関係先要件に従い、代表社員の判断で通知・公表・行政相談等を行う。
- 再発防止：原因分析、是正措置、教育・設定変更等を行い、記録を残す。

15. 物理的セキュリティ・オフィス運用

- 執務スペースの施錠、入退室管理、来客対応（同行、受付記録）を行う。
- 机上整理（クリアデスク）を徹底し、離席時は画面ロックする。
- 印刷物の放置を禁止し、複合機のパスコード印刷等を活用する。

16. 法令・契約の遵守

当社は、個人情報保護法をはじめとする関連法令、ガイドライン、取引先との契約・規約を遵守します。個人情報およびセンシティブ情報は、別途定めるプライバシーポリシーおよび取扱手順に従います。

17. 違反時の措置

本ポリシーに違反した場合、就業規則・契約等に基づき、指導・教育、権限停止、懲戒、損害賠償請求等の措置を行うことがあります。

付録**A**：パスワード・**MFA**運用基準

- MFA：メール、クラウドストレージ、重要SaaSは必須。可能な限り認証アプリ方式を優先。
- 長さ：12文字以上（推奨16文字以上）。複雑性より長さを優先（パスフレーズ可）。
- 使い回し禁止：サービス間で同一パスワードを使用しない。
- 管理：パスワード管理ツールの利用を推奨。共有が必要な場合は管理ツールの共有機能を用いる。
- 漏えい疑い時：直ちに変更し、IS責任者へ報告する。

付録**B**：インシデント報告に必要な情報（最低限）

- 発見日時／発見者
- 事象（何が起きたか：不審メール、誤送信、端末紛失、改ざん疑い等）
- 対象（端末名、アカウント、サービス、ファイル名、顧客名等）
- 直前の操作（クリックしたURL、開いた添付、実行したアプリ等）
- 現在の状態（継続中／収束、ネット接続状況、画面表示）
- 証跡（メール原文、スクリーンショット、ログ、通知文等）

付録**C**：情報資産台帳（最小項目）

以下の項目を、台帳（スプレッドシート等）で管理します。

- 資産名（例：業務用PC-01、メール、クラウドストレージ、会計SaaS等）
- 所有者（担当者）／管理者
- 重要度（公開/社外秘/機密/極秘）
- 保管場所（クラウド名・共有フォルダ・書庫等）
- バックアップ有無／頻度
- 最終点検日（更新・権限・棚卸し）