サンプル株式会社
情報セキュリティ基本規程（サンプル）
第1版
施行日：2026年4月1日
文書番号：SEC-POL-001

【この文書について】
本書は研修・デモ用のサンプルです。実運用に使用する場合は、自社の情報資産・委託形態・利用クラウド等

目次

改定履歴
第1版　2026-02-03　新規作成（サンプル）

1. 目的
会社が保有・取扱う情報資産を保護し、機密性・完全性・可用性を確保するための基本事項を定める。

2. 適用範囲
本規程は、会社の役員・従業員・派遣受入者・委託先等（会社の情報資産へアクセスする者）に適用する

3. 定義
情報資産：業務に関連して作成・取得・保管する情報、およびそれを扱うシステム・媒体。
機密情報：公開されていない会社または顧客に関する情報。
個人情報：個人情報保護法に定義される個人情報。
インシデント：情報漏えい、マルウェア感染、不正アクセス、紛失・盗難、誤送信等の事象。

4. 役割と責任
4.1 経営層：方針の承認、体制整備、必要な資源配分を行う。
4.2 情報セキュリティ責任者：規程管理、教育計画、点検、重大インシデントの統括を行う。
4.3 各部門管理者：部門内の遵守状況の管理、権限申請の承認、是正に協力する。
4.4 利用者：本規程を遵守し、疑義・事故を速やかに報告する。

5. 基本方針
5.1 最小権限：業務に必要な範囲でアクセス権限を付与する。
5.2 多層防御：認証、端末、ネットワーク、監視、バックアップ等を組み合わせる。
5.3 記録と監査可能性：重要操作を記録し、必要に応じて追跡できる状態を保つ。

6. 情報分類と取扱い
6.1 情報は重要度により、公開／社外秘／機密　などに分類する（分類基準は別紙）。
6.2 機密情報は、承認された保管場所（会社指定クラウド、暗号化領域等）のみで保管する。
6.3 廃棄は、紙はシュレッダー、電子媒体は消去または物理破壊等、復元不能な方法で行う。

7. アクセス管理
7.1 アカウントは個人に紐づけ、共用アカウントは原則禁止する。
7.2 パスワードは強固なものを設定し、漏えいが疑われる場合は直ちに変更する。
7.3 多要素認証（MFA）を可能な範囲で有効化する。
7.4 退職・異動時は、速やかに権限を変更・停止する。

8. 端末・媒体・持出管理
8.1 業務端末は会社の管理下に置き、OS・ソフトウェア更新を適用する。
8.2 外部記憶媒体（USB等）の利用は原則禁止し、例外は申請承認制とする。
8.3 端末の紛失・盗難時は直ちに報告し、遠隔ロック等の対応を行う。

9. クラウド・外部サービス利用
9.1 新規サービス利用は、情報区分、契約条項、データ所在地、ログ、権限管理等を確認し承認を得る。
9.2 共有設定は最小限とし、公開リンクは必要性と期限を明確にする。

10. インシデント対応
10.1 事故・疑義を発見した者は、直ちに上長および情報セキュリティ窓口へ報告する。
10.2 会社は、封じ込め、原因調査、復旧、再発防止を実施し、必要に応じて関係者へ通知する。

11. 教育・監査
全従業員は年1回以上の教育を受講し、会社は定期的に遵守状況を点検する。

付則
本規程は2026年4月1日より施行する。