情報セキュリティ基本方針

Information Security Policy

エムシーオー株式会社

文書番号	MCO-SEC-001
版数	第 1.1 版
制定	2026 年 6 月 30 日
最終改訂	2026 年 6 月 30 日
次回見直し	2027 年 6 月
管理部署	情報管理部
適用範囲	全役員及び全就業者 （正社員、契約社員、派遣社員、出向受入者）

はじめに（情報セキュリティ基本方針）

エムシーオー株式会社（以下、当社）は、不動産賃貸仲介事業を通じてお客様・取引先・社会から数多くの情報をお預かりしております。顧客情報・物件情報・契約情報をはじめとする情報資産は、当社の事業基盤そのものであり、これらを適切に保護することは経営上の最重要課題であると認識しています。

近年、中小企業を標的とするサイバー攻撃が急増しており、情報漏洩・システム停止・ランサムウェア被害等が業種を問わず発生しています。当社はこうした脅威に組織的に対応するため、本情報セキュリティ基本方針を定め、全役員・全就業者が一体となって情報セキュリティの維持・向上に取り組みます。

第１条　経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。経営層は情報セキュリティリスクが経営に重大な影響を及ぼす可能性を認識し、以下のとおり率先してセキュリティ対策を推進します。

- 情報セキュリティの推進を経営上の優先事項として位置付け、必要な経営資源（人材・予算・時間）を確保する。
- 年１回以上、セキュリティ対策の実施状況を確認・評価し、改善計画を承認する。
- 情報セキュリティに関する取り組み状況を全役員及び全就業者へ開示・共有し、組織全体のセキュリティ意識を高める。

第２条　社内体制の整備

当社は、情報セキュリティの維持・改善のための組織体制を整備し、情報セキュリティ対策を社内の正式な規則として定めます。

（１）セキュリティ推進体制

統括責任者	代表取締役社長を情報セキュリティの最終責任者とし、情報セキュリティに関する意思決定を行う。
担当部署	情報管理部をセキュリティ推進活動の担当部署として定め、役割・責任・連絡先を明確にする。
担当者	情報管理担当者（情報セキュリティリーダー）を任命し、日常的なセキュリティ推進活動を担当させる。
体制の点検	情報セキュリティ推進体制については年１回以上の頻度で点検・見直しを行う。

（2）規程・ルールの整備

- 本基本方針に基づき、必要な社内規程・ガイドライン・手順書を別途整備する。
- 策定・改訂した規程は、全役員・全就業者へ速やかに周知する。
- セキュリティに関連する法令（個人情報保護法・不正競争防止法等）・業界基準・取引先の要求事項を定期的に把握し、社内ルールへ反映する（年 1 回以上）。
- セキュリティ対応方針は年 1 回以上の頻度で内容を点検し、必要に応じて改訂する。
- 取引先と機密情報を共有する場合の取扱いを別途定める。
- 個人情報の取扱いについては別途『個人情報保護方針』を参照。

（3）守秘義務

- 全役員・全就業者を対象として守秘義務のルールを定め、入社時または受入れ時に説明する。
- 機密情報を取り扱う者には守秘義務誓約書の提出を求める。（派遣社員・受入出向者については派遣元・出向元との守秘義務契約を業務開始前に締結）

第 3 条　就業者の取り組み

当社の全役員・全就業者は、情報セキュリティのために必要な知識・技術を習得し、情報セキュリティへの取り組みを確かなものにします。

（1）セキュリティ教育

- 全役員・全就業者を対象に、新規受入れ時及び年 1 回以上、以下のテーマについてセキュリティ教育を実施し、実施記録を保管する。（保管期間：5 年）
  - 電子メールによるマルウェア感染の予防
  - Web 閲覧によるマルウェア感染の予防
  - 機密区分の定義と情報の取扱いルール
  - フィッシングメール・不審メールへの対応
  - 情報漏洩・インシデント発生時の報告・対応手順
  - パスワード管理・多要素認証の重要性
- セキュリティインシデント発生時の対応については、e ラーニングまたは集合教育による訓練を年 1 回以上実施する。

（2）パスワード・認証管理

- すべての ID・パスワードは申請・承認制により発行・変更・削除を行い、適切に管理する。
- パスワードは 1 2 文字以上、推測されやすい単語の使用禁止、サービス間の使い回し禁止とし、安全に保管する。
- 重要な機密情報を取り扱うクラウドサービスへのアクセスには多要素認証を適用する。
- PC・スマートデバイスにはロック制御を設定し、デフォルトパスワードを変更する。

（3）アクセス権管理

- 業務システム・PC へのアクセス権及び機密エリアへの入室は申請・承認制とし、必要最小限の範囲に限定する。
- 退職・異動時にはアクセス権・ID を速やかに削除または無効化する。
- 管理者 ID は業務上必要な者のみに限定し、一覧を管理する。

第 4 条　法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令・規制・規範・契約上の義務を遵守するとともに、お客様の期待に応えます。

- 個人情報保護法・不正競争防止法・電子帳簿保存法等、事業に関連する法令の改正動向を継続的に把握し、社内ルールへ反映する。
- 取引先・委託先との契約において、情報セキュリティに関する要求事項を明確にする。
- 行政機関・所管省庁の基準・ガイドライン（経済産業省・IPA のセキュリティ基準を含む）を参照し、対策水準を維持・向上させる。

第 5 条　違反及び事故への対応

当社は、情報セキュリティに関わる法令違反・契約違反・事故（インシデント）が発生した場合には適切に対処し、再発防止に努めます。

（1）インシデント対応体制

- セキュリティインシデント発生時の対応手順（①発見・報告　②初動　③調査・対応　④復旧　⑤最終報告）を定め、全役員・全就業者へ周知する。
- インシデント発生時の社内外連絡先（関係当局・所管省庁を含む）と報告ルートを整備する。
- 対応体制（担当部署・役割・責任）については年 1 回以上の頻度で点検する。
- 重大なインシデント事例は速やかに全社共有し、再発防止策を策定・実施する。
- お客様・取引先等の関係者への適切な通知を行う。

（2）事業継続への対応

- 事業継続上重要なシステムについて、サイバー攻撃を念頭に置いた目標復旧レベル（RTO/RPO）を定め、必要な対策（予備機・クラウド環境・連絡先整備等）を整備する。
- 定期的なバックアップと復元テストにより、インシデント発生時の業務復旧を可能な状態に維持する。

第 6 条　継続的な改善

当社は、本方針に基づくセキュリティ対策を継続的に評価・改善し、常に適切なセキュリティ水準を維持します。

- 情報セキュリティ対策の実施状況を年 1 回以上評価し、改善計画を策定・実施する。
- 本基本方針は制定日より施行し、年 1 回以上の頻度で内容を見直す。
- 内外の環境変化（法改正・脅威動向・組織変更等）に応じて随時改訂し、全役員・全就業者へ周知する。

附則

制定・改訂日	版　数	改訂内容
2026 年 5 月 19 日	第 1.0 版	初版制定
2026 年 6 月 23 日	第 1.1 版	追記（取引先管理に関する規定を整備）

以　上

本方針に関するお問い合わせ窓口：
〒104-0061
東京都中央区銀座 2 丁目 8 番 20 号　ヨネイビル 6F
TEL.03-3538-0821　FAX.03-3538-0823
エムシーオー株式会社 情報管理部