Security Policy

情報セキュリティ基本方針

株式会社東海損保（以下、当社）は、お客さまに満足いただける商品とサービスを提供するために、お客さまからお預かりした情報資産を事故・災害・犯罪などの脅威から守り、お客様さまならびに社会の信頼に応えるべく、以下の方針に基づき全社をもって情報セキュリティに取り組みます。

1.経営者の責任
代表者は本ポリシーの運用に対して正当な意識と責任をもって組織的かつ継続的に情報セキュリティの改善・向上と適切な管理に努めます。

2.社内体制の整備
当社は、情報セキュリティの維持及び改善のために必要な組織の設置および管理体制を整備し、必要な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。

3.従業員の取組み
当社の従業員は、情報セキュリティの維持と改善ために必要とされる知識、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。

4.法令及び契約上の要求事項の遵守
当社は、事業活動で利用する情報資産に関連する情報セキュリティに関わる法令、規制、規範、お客さまとの契約上のセキュリティ要求事項と義務を遵守するとともに、その取組を確かに遂行しお客さまの信頼と期待に応えます。

5.違反及び事故への対応
当社は情報セキュリティ事故への対応のための体制を整備し、情報セキュリティに関わる法令違反、規約違反、お客さまとの契約に関わる違反及び情報セキュリティ事故が発生した場合には適切に対処し、影響の低減と再発防止に努めます。

情報セキュリティ対策基準

1.情報資産について
組織や個人が保有する価値のある情報と資源であり、それらが正当に保護されて機能するために関連する資源を総じたもので、ハードウェア・ソフトウェア・ネットワーク・各種データファイル・システム開発・運用のために必要な要素を含むドキュメント・社員が業務上知り得た顧客情報等をも含むものである。

2.情報資産の分類について
情報資産は、機密情報、非機密情報の 2 つに分類し、機密情報は機密性（限られた人だけが情報に接触）・完全性（不正な改ざんから保護）・可用性（利用者が必要な時に安全にアクセスできる環境）の視点から重要度別に適切に管理しなければならない。

3.情報資産へのアクセス
情報資産がその目的に沿って適切に使用されるよう、正当な必要性に基づくアクセスに対して正当な認証を必須とする。また、すべての従業員は当社の情報資産を業務以外に利用することを禁じる。

4.情報システムの安全対策
情報資産の保護のため、情報セキュリティに関連するすべての法律および当社規程を遵守し、アクセス制御・ネットワークセキュリティ・ID/パスワードの管理・情報廃棄の完全化を徹底する。

5.情報セキュリティ事故対応
すべての従業員は、情報の紛失および情報システムの盗難等の情報資産にトラブルが発生した場合は、速やかに（30 分以内）情報セキュリティ責任者に報告しなければならない。
情報セキュリティ責任者は、トラブルへの対策を実施し、解決と再発防止策を講じる。

制定日 2025 年 8 月 1 日

株式会社 東 海 損 保
代表取締役 多田 大木