

## 1 基本方針

当社は、保険代理店業務を通じて取り扱う顧客情報および業務情報を重要な経営資産と位置づけ、これらの情報を適切に保護することを経営上の重要課題と認識しています。

当社は、情報の漏えい、滅失、毀損、不正アクセスおよび不正利用を防止するため、組織的・人的・物理的・技術的な安全管理措置を講じ、情報セキュリティの維持および継続的改善に取り組めます。

また、情報保護は単なるIT対策にとどまらず、責任体制の明確化、記録管理、定期点検および是正措置を通じて、実効性のある情報保護態勢を構築します。

## 2 情報セキュリティの公開

当社は、本情報セキュリティポリシーを対外的に公開し、顧客および関係先に対して当社の情報保護の基本方針を明確にします。

また、社会環境や技術環境の変化、法令改正等に応じて、本ポリシーを適宜見直し、継続的な改善に努めます。

## 3 情報セキュリティの対象

本ポリシーにおける対象情報は、以下を含みます。

- 顧客情報および契約関連情報
- 保険募集および契約管理に関する業務情報
- 当社の営業・経営に関する情報
- 電子データ、紙媒体、クラウドサービス上の情報

これらの情報は、業務遂行上必要な範囲でのみ利用し、目的外利用、不必要な複製および不要な持出しを行いません。

また、情報管理においては「保存情報の最小化」と「事故発生時の被害極小化」を基本原則とします。

## 4 管理

当社は、情報セキュリティ管理体制を整備し、顧客情報管理責任者および個人データ管理責任者を中心とした責任体制のもとで、情報セキュリティの統括管理を行います。

管理責任者は、当社の情報システム、クラウドサービス、端末管理および情報セキュリティ対策の状況を把握し、必要に応じて改善措置を講じます。

また、実務運用においては担当者を定め、責任の所在が不明確にならないよう適切な管理を行います。

## 5 対策

当社は、情報セキュリティを確保するため、以下の対策を講じます。

- ネットワークおよびシステムの安全管理
- ウイルス対策ソフト等の導入および更新
- 認証管理およびアクセス制御
- クラウドサービスの適切なアカウント管理
- モバイル機器の適切な管理
- 情報の外部持出しの制限
- 電子メール送信時の誤送信防止対策
- 外部記憶媒体の使用制限

また、業務用端末は、社内ネットワークまたはクラウド環境へアクセスするための端末として位置づけ、顧客情報の恒常的な保存は行わない運用を基本とします。

## 6 社内規程

当社は、本ポリシーに基づき、情報保護に関する社内規程を整備し、情報管理の具体的運用を定めます。

- 個人情報保護規程
- 情報セキュリティ管理に関する規程
- モバイル機器管理ルール
- 情報漏えい発生時の対応手順

従業員はこれらの規程を遵守し、適切な情報管理を行うものとします。

## 7 教育・研修

当社は、従業員および募集人に対して、情報セキュリティおよび個人情報保護に関する教育・研修を継続的に実施します。

これにより、情報漏えいの防止および適切な情報管理に対する意識の向上を図ります。

## 8 業務委託先管理

当社は、業務委託先に顧客情報等を取り扱わせる場合には、委託先の情報管理体制を確認し、必要な契約および監督を行います。

委託先においても、当社と同等の情報保護水準が確保されるよう適切に管理します。

## 9 法令遵守

当社は、個人情報保護法その他の関係法令および業界ガイドラインを遵守し、情報の適正な取扱いを行います。

また、政治的見解、信教、保健医療等のセンシティブ情報については、法令等に基づく場合を除き取得・利用・第三者提供を行いません。

## 10 内部監査の実施

当社は、情報セキュリティ対策の実効性を確保するため、定期的な内部点検および内部監査を実施します。

監査結果に基づき、必要な是正措置および再発防止策を講じ、情報保護態勢の継続的改善を図ります。

## 11 情報漏えい・サイバー攻撃発生時の対応

情報漏えい、紛失、ウイルス感染、不正アクセス、サイバー攻撃等が発生またはそのおそれがある場合には、速やかに事実関係の確認および被害拡大防止措置を講じます。

必要に応じて保険会社、専門機関および関係機関と連携し、適切に対応します。

また、事故対応の経緯を記録し、再発防止策を講じます。