情報セキュリティ基本方針（セキュリティポリシー）

制定日：2024年4月1日
保険デザインパートナーズ株式会社
代表取締役 安井 義幸

1. 目的

保険デザインパートナーズ株式会社（以下「当社」）は、保険代理業を営む上で、お客様の氏名、住所、健康状態などの極めて重要な機微情報を取り扱っています。これらの情報資産をサイバー攻撃や漏洩等の脅威から守ることは、当社の社会的責務であり、事業継続の基盤です。
当社は、お客様からの信頼に応え続けるため、本情報セキュリティ基本方針（以下「本ポリシー」）を定め、全従業員（役員、正社員、契約社員、アルバイト等を含む）がこれを遵守することを宣言します。

2. 適用範囲

本ポリシーは、当社が業務上取り扱うすべての情報資産（電子データ、紙媒体、顧客情報、経営情報等）、および情報資産を取り扱うすべての従業員、ならびに当社が管理する情報システム、ネットワーク機器、事務所施設に適用します。

3. 情報セキュリティ管理体制

当社は、情報セキュリティに関する統括責任者として「情報セキュリティ責任者」を配置し、組織的かつ継続的な情報セキュリティ対策を推進する体制を構築します。

4. 情報資産の保護とサイバー対策

当社は、情報資産の機密性、完全性、可用性を維持するため、以下の物理的・技術的対策を講じます。
(1) マルウェア・ランサムウェア対策: 業務で使用するすべてのPC等の端末に、常に最新のウイルス対策ソフトを導入・更新し、不審なメールの開封や危険なWebサイトへのアクセスを禁止します。
(2) パスワード管理: システム等のログインには推測されにくい強固なパスワードを設定し、適切に管理します。
(3) 持ち出し制限: 顧客情報を含むデータの入ったUSBメモリ等の外部記憶媒体やPCの社外への持ち出しは、原則禁止とし、やむを得ない場合は責任者の許可を得た上で暗号化等の措置を講じます。
(4) クリアデスク・クリアスクリーン: 離席時の画面ロック、および退社時の机上の重要書類の施錠保管を徹底します。

5. 従業員の教育・訓練

当社は、全従業員に対して情報セキュリティに関する教育・研修を定期的に（年1回以上）実施します。また、昨今のサイバー攻撃の手口を学ぶため、標的型攻撃メール訓練等の実践的な訓練を取り入れ、従業員のリテラシー向上に努めます。

6. 事故発生時の対応

万が一、情報漏洩やサイバー攻撃への感染等の情報セキュリティインシデントが発生した場合、またはその疑いを発見した場合は、従業員は速やかに情報セキュリティ責任者に報告します。
責任者は、被害の拡大防止、原因究明、復旧作業を迅速に行うとともに、保険会社および関係当局への報告を遅滞なく行います。また、再発防止策を策定し、全社に周知徹底します。

7. 法令・規範の遵守と継続的改善

当社は、「個人情報の保護に関する法律」をはじめとする情報セキュリティに関する法令、国が定める指針、および所属保険会社の定める規程を遵守します。また、事業環境や脅威の変化に合わせて、本ポリシーおよびセキュリティ対策を定期的に見直し、継続的な改善に努めます。