情報セキュリティ基本方針

第１章　総則

第１条（目的）

本方針は、株式会社アスク（以下「当社」という。）が業務上取り扱う情報資産を適切に保護し、情報漏えい、改ざん、紛失、破壊等のリスクを低減することにより、お客様および取引先からの信頼を確保することを目的とする。 当社は、情報セキュリティの重要性を認識し、役職員全員が本方針を遵守する。

第２条（適用範囲）

本方針は、当社が管理するすべての情報資産（電子データ、紙媒体を含む）および、当社の役職員（正社員、契約社員、パート・アルバイト等）に適用する。

第２章　情報セキュリティ管理体制

第３条（情報セキュリティ責任者）

1. 当社は、情報セキュリティを統括する責任者として、事務管理責任者を情報セキュリティ責任者として任命する。
2. 情報セキュリティ責任者は、当社における情報セキュリティ対策の策定、実施、運用管理および見直しを統括する。
3. 情報セキュリティ責任者は、必要に応じて代表取締役および業務統括責任者と連携し、情報セキュリティ体制の維持・向上を図る。

第４条（役職員の責務）

1. 役職員は、本方針および関連ルールを遵守し、業務に必要な範囲でのみ情報資産を取り扱う。
2. 情報セキュリティ上の問題や事故の兆候を認識した場合は、速やかに情報セキュリティ責任者へ報告する。

第３章　情報資産の管理

第５条（情報資産の分類）

当社の情報資産は、以下の区分を基本として管理する。

- お客様の個人情報・保険契約情報（重要情報）
- 業務上の内部情報（社内情報）
- 公開可能な情報（公開情報）

第６条（アクセス管理）

1. 情報資産へのアクセスは、業務上必要な役職員に限定する。
2. ID およびパスワードは個人ごとに管理し、第三者と共有しない。
3. 退職・異動等により不要となったアクセス権は速やかに削除する。

第 7 条（物理的管理）

1. 重要書類は施錠可能なキャビネット等で保管する。
2. PC、USB メモリ等の情報機器の持ち出しは、業務上必要な場合に限り、情報セキュリティ責任者の管理のもとで行う。

第 4 章　サイバーセキュリティ対策

第 8 条（不正アクセス対策）

当社は、以下の基本的な対策を講じる。

1. OS およびソフトウェアを最新の状態に保つ。
2. 推測されにくいパスワードを設定する。
3. 社内ネットワークおよび端末に適切なセキュリティ設定を行う。

第 9 条（マルウェア対策）

1. すべての業務用 PC にウイルス対策ソフトを導入する。
2. 不審なメールの添付ファイルや URL を開かない。

第 10 条（情報漏えい対策）

1. 個人情報・重要情報を私用メールや私物端末で取り扱うことを禁止する。
2. メール送信時は、宛先および送信内容を十分に確認する。
3. 当社は、電子メールにより個人情報または重要情報を送信する場合、セキュリティ機能を備えた外部ファイル共有・送信システムを利用し、URL 経由での閲覧方式を採用する。
4. 前項のシステムにおいては、受信者が当該 URL にアクセスし、自身のメールアドレスを入力のうえ認証コード（ワンタイムパスワード）を取得・入力する方式により本人確認を行い、情報漏えい防止を図る。

第 5 章　インシデント対応

第 11 条（インシデント発生時の対応）

1. 情報セキュリティ事故またはそのおそれがある場合、役職員は速やかに情報セキュリティ責任者へ報告する。
2. 情報セキュリティ責任者は、被害拡大防止、原因調査および再発防止策を講じる。

第 6 章　教育・見直し

第 12 条（教育）

当社は、役職員に対して情報セキュリティに関する教育・注意喚起を年 1 回以上実施する。

第 13 条（見直し）

本方針は、社会情勢、法令改正、業務内容の変化等を踏まえ、必要に応じて見直す。