安全管理措置の内容

当社は、個人情報等の漏えい、滅失またはき損の防止その他の個人情報等の安全管理のために、以下に掲げる必要かつ適切な措置（以下「安全管理措置」といいます。）を講じます。

1　基本方針の策定

- 個人情報の適正な取扱いの確保のため、プライバシーポリシーのほか、個人情報等を含む情報セキュリティに関する基本方針を策定しています。

2　個人情報等の取扱いに係る規律の整備

- 個人情報等の取扱いの段階ごとに、その取扱方法、責任者・担当者、及びその任務等について定めた取扱規程を策定しています。

3　組織的安全管理措置

- 個人情報等を含む情報セキュリティの管理責任者を任命するなど、個人情報等の安全管理に関する従業員の責任と権限を明確にする組織体制を整備しています。
- 個人情報等の内容に応じた保管場所・保管要件の明確化、及びシステムログの記録・保管を通して、個人情報等の取扱状況を確認する手段を整備するとともに、これらが個人情報等の取扱規程に従った運用であるか検証を行います。
- 個人情報等の漏えい等のインシデントが発生した場合における対応フローを定め、速やかに調査・報告・対策等を行うような体制を整備しています。
- 個人情報等の取扱状況について、社内でセキュリティレビューを行うとともに、外部専門家による監査を行う等、安全管理措置の見直しを行います。

4　人的安全管理措置

- 個人情報等を含む情報セキュリティに関する研修・訓練等の社内教育を定期的に実施し、従業員の個人情報等の保護への意識の向上、啓発に努めています。

5　物理的安全管理措置

- 社員証の携帯および訪問者記録を用いて執務フロアへの入退室制限・管理を行い、取り扱う情報や業務の内容に応じてフロアを分ける等、個人情報等を取り扱う区域の管理を行っています。
- 資産管理システムを用いて情報端末を管理するとともに、情報端末の記憶装置の暗号化や外部から内容を消去できるリモートワイプ機能を備える等により、情報端末の盗難・紛失等、及びこれによる情報漏えいを防止するための措置を実施しています。

- 個人情報等を削除し、又は個人情報等が記載・記録された書類や電子記録媒体等を破棄等する際は、個人情報等が復元不可能又は容易に復元できない方法でこれを行います。

6　技術的安全管理措置

- 従業員ごとにクラウドへのアクセスに必要となる ID を交付し、クラウド上の個人情報等へのアクセス権限を付与する従業員を限定する等のアクセス制御を行います。また、当該 ID に紐づけて記録したネットワークログ、認証ログ、アクセスログ等により、個人情報等にアクセスした者の識別と認証を行います。
- ファイアウォール等による境界防御の構築、個人情報等を取り扱う端末へのウイルス対策ソフト等導入、専門エンジニアによるログの監視等、外部からの不正アクセスを防止するための措置を実施しています。
- 当社の全てのサービスにおいて通信の暗号化を行う等、情報システム利用時に個人情報等の漏えいを防止するための措置を実施しています。

以上

（2022.4.1 制定）