情報セキュリティ基本方針

【基本方針】

1. **経営者の責任**

   経営者は、サイバーセキュリティの重要性を深く認識し、DX 推進の最高責任者として、対策の推進に必要な経営資源を確保します。経営者が主導することで、全従業員が一丸となってセキュリティ対策に取り組む企業文化を醸成します。

2. **社内体制の整備**

   DX 推進責任者である取締役管理部長の監督のもと、情報セキュリティを管理・運用する体制を構築します。システム担当者を中心に、役割と責任を明確にし、実効性のあるセキュリティ管理を徹底します。

3. **情報資産の適正な管理**

   事業活動で利用するお客様、お取引先様、従業員の情報、そして当社の技術情報といった全ての情報資産を、関連法令や規範を遵守し、適正に管理・運用します。

4. **技術的・組織的セキュリティ対策の徹底**

   情報資産への不正アクセス、漏えい、改ざん、紛失などを防ぐため、以下の技術的・組織的対策を講じます。

   - **クラウド活用による防御**： クラウドサービスの導入により、データの暗号化、自動バックアップ、最新のセキュリティパッチ適用といった高度なセキュリティ環境を維持します。
   - **社内教育の徹底**： 全従業員を対象とした情報セキュリティ研修を年 1 回以上実施し、セキュリティ意識の向上を図ります。
   - **アクセスの管理**： 業務上必要な従業員のみが情報資産にアクセスできるよう、厳格な権限管理を行います。

5. **継続的な改善**

社会やビジネス環境の変化、新たな脅威に対応するため、情報セキュリティ管理体制や対策について、定期的な自己点検や内部監査を通じて見直しを行い、継続的な改善に努めます。

6. **インシデントへの対応**

万が一、情報セキュリティに関する問題が発生した場合には、迅速に原因を究明し、被害を最小限に食い止めるための対応策を講じるとともに、再発防止に努めます。