エイジェックグループ情報セキュリティポリシー

1. 目的

エイジェックグループ（以下、「当グループ」）は、情報セキュリティを重要な経営課題と位置付け、当グループの事業活動に関わる全ての情報資産を保護し、適切に管理することを目的とします。本ポリシーに基づき、情報漏えいや不正アクセス、サイバー攻撃などのリスクに対する強固な対策を講じるとともに、お客様・取引先・従業員など、すべてのステークホルダーから信頼される企業グループを目指します。

2. 情報セキュリティ管理体制の確立

当グループは、情報セキュリティ委員会を中心に、全社的なセキュリティ対策を推進します。これにより、各グループ会社の情報セキュリティレベルを均一に保ち、継続的な改善を図ります。

3. 情報セキュリティ方針

当グループは、情報資産を保護するため、以下の原則に基づいて情報セキュリティを維持・強化します。

機密性の確保：情報が許可された者のみアクセスできる状態を維持します。
完全性の維持：情報の正確性および完全性を保ち、不正な改ざんを防ぎます。
可用性の確保：業務上必要な情報が、必要なときに適切に利用できる状態を確保します。

4. 最高情報セキュリティ責任者（CISO）の設置

当グループは、情報セキュリティ管理を統括する最高情報セキュリティ責任者（CISO）を設置し、グループ全体のセキュリティ対策を主導します。また、各グループ会社に情報セキュリティ担当者を配置し、ガバナンスを強化します。

5. 情報セキュリティ規程の整備と遵守

当グループは、情報セキュリティポリシーに基づき、詳細な社内規程を策定し、これを遵守することを全従業員に義務付けます。

6. セキュリティ監査と継続的改善

情報セキュリティの遵守状況を定期的に監査し、必要に応じて外部監査機関の評価を受けることで、継続的な改善を図ります。

7. サイバー攻撃および不正アクセス対策

最新のセキュリティ技術を活用し、サイバー攻撃や不正アクセスから情報資産を守るための防御策を強化します。特に、ファイアウォールの導入、多要素認証（MFA）の活用、ゼロトラストセキュリティ

の考え方を取り入れたアクセス管理を徹底します。

8. 情報セキュリティ教育の推進

全従業員および業務委託先を対象に、定期的なセキュリティ教育・訓練を実施し、情報リスクに対する意識向上を図ります。また、新しい脅威に対応するため、研修プログラムを随時更新します。

9. 業務委託先の管理

業務委託先と契約を締結する際には、情報セキュリティ基準を満たしているかを事前に確認し、定期的な監査を行うことで、適切な情報管理が行われるよう徹底します。

10. 情報セキュリティインシデント対応

万が一、情報漏えいやシステム障害などのセキュリティインシデントが発生した場合、情報セキュリティ委員会が迅速に対応し、原因究明・影響分析・被害拡大防止・再発防止策の策定を行います。また、必要に応じて関係当局や取引先へ報告を行い、適切な対応を実施します。

11. 情報セキュリティポリシーの適用範囲

本ポリシーは、エイジェックグループのすべての役員・従業員・派遣社員・業務委託者・協力会社に適用されます。また、業務上知り得た情報資産の取り扱いについては、退職後も適用されるものとします。

12. ポリシーの改定

当グループは、情報セキュリティの重要性を鑑み、社会情勢・技術動向・法規制の変更に対応するため、本ポリシーの定期的な見直しを行い、必要に応じて改定します。

施行　　2025 年 4 月 1 日
発行　　グループリスクマネジメント統括本部　情報セキュリティ管理委員会