王子グループサイバーセキュリティポリシー

2026-11-24　制定

高度情報通信社会の到来により、日々の企業活動を行ううえで、情報通信技術やクラウドサービスや生成ＡＩなどのＩＴサービスの利用が業務効率向上に与える影響は大きなものがあります。その一方で、サイバー攻撃や不正アクセスによる情報漏えい、データの改ざんや資金の流失等、サイバーセキュリティに関するリスクが日々増大しています。サイバーセキュリティ対策は、もはや単なるＩＴ分野の課題にとどまらず、経営課題として捉えるべき時代となっています。私たち王子グループは、サイバーセキュリティの重要性を正しく認識し、情報セキュリティに対する当社グループのポリシーとして「サイバーセキュリティポリシー」を宣言します。本ポリシーは、当社グループの役職員およびその委託を請けて業務を遂行するすべての者（以下、全従業者）に周知徹底し、これを実践、遵守するために、サイバーセキュリティ対策に関する施策を策定・運用するだけでなく、その運用状況について定期的に確認し、サイバーセキュリティ対策に関する施策の継続的改善を図ってまいります。

１．サイバーセキュリティの適用範囲と適用対象者

当社グループが保有する情報資産(情報機器・データ)をサイバーセキュリティポリシーの適用対象とします。また、全従業者をサイバーセキュリティポリシーの適用対象者とします。

２．経営陣の役割

当社グループ各社の経営陣は、サイバーセキュリティの水準を適切に保つため、本ポリシーに基づく施策の実施に必要な経営資源を提供します。

３．法令の遵守

当社グループは、サイバーセキュリティに関する法令および行政官庁が定めた方針・ガイドライン等を遵守します。

４．人権尊重とプライバシー保護

当社グループは、サイバーセキュリティ対策の実施にあたり、すべての関係者の人権を尊重することを基本原則とします。

情報資産の管理、監視、ログ取得、アクセス制御等のセキュリティ措置は、個人の尊厳、プライバシー権、差別されない権利を不当に侵害しないよう適切に実施します。

５．個人情報および機微情報の保護

当社グループは、個人情報保護法、関連法令および社内規定等に基づき、個人情報・機微情報を適切に取得、利用、保管、廃棄します。また、これらの情報を扱う際には、特に厳格なアクセス制御および実施状況の確認を実施します。

６．適切なサイバーセキュリティ対策の実施

当社グループは、サイバー攻撃や不正アクセスによる情報漏えい、データの改ざんや資金の流失等、サイバーセキュリティの物理的、技術的、および人的脅威から情報資産の機密性、完全性および可用性を守るため、適切なサイバーセキュリティ対策を実施します。また、サイバーセキュリティに関する事件・事故が発生した場合は、外部の専門家と連携して再発防止策の検討を含め、速やかに適切な対策を講じます。

７．情報資産の適切な管理と利用

当社グループは、情報資産をサイバーセキュリティ各種規程に従い、適切に管理、運用いたします。情報資産の取得、利用、保管、廃棄の各段階において適切な管理を行い、不要となった情報資産は安全な方法で廃棄または消去します。

８．取引先・委託先事業者への対応

取引先や委託先事業者などとは秘密保持を含めた契約を締結するほか、適切なセキュリティレベルを維持するよう求めます。

９．クラウドサービスおよびAIを含む外部サービス利用に関する方針

当社グループは、クラウドサービスやAIを含む外部の情報システムを利用する際、セキュリティ要件、契約条件、データ保護措置、責任分界を明確化し、適切な管理を行います。

１０．サイバーセキュリティ管理諸規程の策定と周知

当社グループは､サイバーセキュリティリスクを適切に管理するための諸規程を策定し、全従業者が遵守するよう周知徹底します。

１１．管理・監視体制の確立

当社グループは、サイバーセキュリティリスクを適切に管理・監視するための体制を確立し、サイバーセキュリティ対策を速やかに実施します。また、サイバーセキュリティインシデントが発生した場合に迅速かつ適切に対応するため、インシデント対応体制を整備します。

１２．サイバーセキュリティに関する教育・訓練の継続的実施

当社グループは、サイバーセキュリティの重要性を認識し、情報資産を適切に取り扱うことができるよう、サイバーセキュリティリテラシーの向上を目的とした教育・訓練を継続的に実施します。

１３．サイバーセキュリティ検査の実施

当社グループは、業務の遂行においてサイバーセキュリティに関する法令、社内諸規程が遵守され、有効に機能していることを検証するため、定期的に、または必要に応じてサイバーセキュリティに関して継続的な検査を実施します。

１４．サイバーセキュリティマネジメントの継続的な改善

当社グループは、以上の取り組みを定期的に評価、見直すことにより、サイバーセキュリティマネジメントの継続的な改善を実施します。

１５．情報公開

当社グループは、社会的影響を及ぼす重大なサイバーセキュリティインシデントが発生した場合、関係当局への報告および必要な情報公開を適切に行います。