ＴＨＫグループ　情報セキュリティポリシー

ＴＨＫグループ（以下、「ＴＨＫ」という。）は、日々深刻化する情報セキュリティリスクに対処すべく、情報セキュリティに関する各国の法令・ガイドラインおよびその他の社会的規範を遵守したうえで、ＴＨＫのお客様、ＴＨＫの役員および従業員（以下、「従業員等」という。）等のステークホルダーの皆様、ならびにＴＨＫの事業を守ることを目的として、以下の方針に沿った情報セキュリティに関する取組みを推進します。

１．情報セキュリティ管理体制の整備

ＴＨＫは、情報セキュリティを重要な経営課題として捉え、ＴＨＫの情報セキュリティを推進すること、情報セキュリティリスクを管理すること、および組織横断的に各種施策の実施を徹底することを目的として、情報セキュリティ管理体制を整備します。

２．情報セキュリティルールの制定

ＴＨＫは、ＴＨＫの事業環境を取り巻く情報セキュリティリスクを踏まえ、ＴＨＫが保有する情報資産を保護し、漏えい・紛失・破壊等の情報セキュリティインシデントが発生する可能性を抑制することを目的として、情報セキュリティに関するルールを制定のうえ、全ての従業員等に周知徹底します。

３．情報セキュリティ対策の実施

ＴＨＫは、ＴＨＫが置かれている事業環境から想定される情報セキュリティリスクを効果的に低減し、ＴＨＫの事業を安定的かつ継続的に推進することを目的として、人的・組織的・技術的・物理的観点から、ＴＨＫの情報セキュリティルールに沿った適切な情報セキュリティ対策を実施します。

４．業務委託先の管理

ＴＨＫが業務の全てまたは一部を委託する場合には、ＴＨＫが定める情報セキュリティレベルを維持するよう、業務委託先としての適格性を十分に審査します。また、これらの情報セキュリティレベルが適切に維持されていることの確認を目的として、業務委託先への定期的な点検、管理体制の見直し等を継続的に実施します。

５．情報セキュリティ教育および訓練の実施

ＴＨＫは、ＴＨＫの業務に従事する全ての従業員等が情報セキュリティに関する高い意識を持ち、ＴＨＫが保有する情報資産を適切に取り扱うことを目的として、情報セキュリティの最新の動向を踏まえた教育および訓練を継続的に実施します。

６．情報セキュリティインシデントへの対応

ＴＨＫは、情報セキュリティインシデントが発生した際には、関係各所に迅速に報告したうえで、被害の更なる拡大や二次被害の発生を抑制するよう、初期対応を実施するとともに、発生原因を究明し、適切な再発防止策を講じます。

７．情報セキュリティ対策の監査および改善

ＴＨＫは、ＴＨＫの情報セキュリティレベルの維持および向上を目的として、管理体制やルールの遵守状況、情報セキュリティ対策の有効性等、ＴＨＫの情報セキュリティに係る取組み全般について定期的な監査を実施し、課題を認識した場合には、改善のために必要な対策を講じます。

2024 年 12 月制定