

セキュリティポリシー

(目的)

第1条 このセキュリティポリシーは、株式会社東京カーリース(以下「当社」という。)におけるすべての情報資産のセキュリティを確保するために講じるべき基本的な事項を明示するとともに、その実効性を確保するために必要となる取り組みを定め、もって事業活動の継続および社会的信用の維持に資することを目的とする。

(定義)

第2条 このポリシーにおいて、「情報資産」とは、次の各号に定めるものをいう。

(1) 情報

当社が保有、管理、使用等によって取り扱うすべての情報(それらを保存または記録している記録媒体、設備、書類等のすべてを含む。ただし、次号に該当するものを除く。)をいう。

(2) 情報システム

コンピュータ(ホストコンピュータ、サーバー、ワークステーション、パソコン等の総称)、端末機器、周辺装置、通信系装置、回線およびプログラム等の全部または一部により構成されるデータを処理するためのコンピュータシステムをいう。

2 この規程において、「セキュリティ確保」とは、紛失・盗難・漏洩・不正使用等の情報資産に関するリスクを最小限に抑えるべく、適切な管理態勢を確保することをいう。

(セキュリティ確保のための措置)

第3条 当社は、次の各号に従って自社の情報資産のセキュリティ確保を図るとともに、必要に応じて更なる改善に努めるものとする。

(1) 自社の取り扱う情報資産について想定されるリスクを洗い出し、重要度に応じて取り扱いの水準を区分する。

(2) リスクの特定結果を踏まえ、次の措置を重要度に応じて講じる。

- ①技術的安全管理措置 情報資産へのアクセスの制御・権限の管理・記録・監視などの措置。

②組織的安全管理措置 このポリシーの周知・遵守を図るとともに、情報資産を適正に取扱うために必要となる権限・手順等を定めた規程・マニュアル等を整備する。また、セキュリティ管理部門および各部門における情報資産管理者を設けるなどの措置。

③人的安全管理措置 技術的安全管理、組織的安全管理が実効性をもって法令等を遵守して、適切に行われるよう社員に必要な教育・訓練を実施するなどの措置。

(3) 重要な事象の発生が経営陣に適切に報告される体制を整備するとともに、内部監査等により、措置の実施状況の検証を適宜行う。

(4) 外部委託の場合(代理店業務委託を含む)など、社外の者に情報資産の取り扱いを許可する場合は、自社と同様のリスクの制御が図られるよう求め、契約に定めるなどの措置を講じる。

(規程等の整備)

第4条 当社は、前条に定める措置の実効性を確保すべく、次の各号に従って規程等の整備に取り組む。

(1) 情報資産のうち、顧客情報および情報システムについては、このポリシーに従い、その重要性に留意して規程等にセキュリティ確保に関する取り扱いを定める。

(2) 前号以外の情報資産については、このポリシーの趣旨を踏まえ、その情報資産の特性に応じて規程等にセキュリティ確保に関する取り扱いを定める。

(改廃)

第5条 このポリシーの改定または廃止は、代表取締役社長の決裁による。ただし、軽微な改定については、コンプライアンス部長の決裁によることができる。

(所管)

第6条 このポリシーの所管は、コンプライアンス部(情報資産のセキュリティ管理の統括部門)とする。

附則 制定 2025年 10月 1日