

SMK情報セキュリティポリシー

SMK株式会社及びその国内外子会社等(以下、SMKグループという)は、すべての情報および情報システム(以下、情報資産という)を適切に取り扱い、保護することが事業活動において重要な社会的責務と認識し、以下にSMK情報セキュリティポリシーを定め、情報セキュリティの確保・向上に取り組みます。

1. 経営者の責任

SMKグループはCIOを最高責任者とする体制を確立し、最高責任者のもと情報セキュリティマネジメントシステムの確立と継続的な改善を行います。

2. 情報資産の保護と管理

SMKグループは、事業活動のために保有する情報資産の機密性・完全性および可用性を確保し、物理的、技術的、人的セキュリティ対策を講じます。また、情報資産を適切に分類し、リスク評価に基づき管理します。

3. 情報セキュリティ教育・訓練の実施

SMKグループは、SMK情報セキュリティポリシーの周知徹底を図るため、SMKグループが保有する情報資産を取り扱う全従業員に対し、情報セキュリティの必要性、情報資産の適正な取扱いと管理、緊急時の対応等に関する教育・訓練を定期的実施します。

4. 情報セキュリティの監視と監査

SMKグループは、情報セキュリティ上の脅威を把握するため、情報システム・ネットワークの状況を継続的に監視し、異常の検知および必要な対応を行います。また、情報セキュリティの維持・向上のため、適宜、内部監査および必要に応じて第三者による監査を実施し、指摘事項については速やかな改善に努めます。

5. 情報セキュリティ事故への対応

SMKグループは、情報セキュリティ事件・事故、災害等の発生に備え、緊急時の体制と手順を整備します。万が一、情報セキュリティの問題が発生した場合、速やかに関係者へ報告を行い、被害を最小限に抑えるとともに再発防止に努めます。

6. サプライヤーへの要求

SMKグループは、サプライチェーン全体の情報セキュリティ対策の把握に努めるとともに、適切な情報セキュリティ対策が講じられていることをサプライヤー対して求めます。

7. 法令等の遵守

SMKグループは、各国の情報セキュリティに関する法令、規制および契約上の義務を遵守し、その他の社会的規範やガイドラインなどについても準拠に努めます。

SMK情報セキュリティポリシーは、社会環境や事業環境の変化に応じて定期的に見直し、継続的な改善を図ります。

SMK株式会社
2026年6月12日

常務執行役員(CIO)
宇佐美 博