コンプライアンス基本方針

1. コンプライアンス（法令等遵守）の推進当社は、コンプライアンス（法令等遵守）とは、狭義の法令にとどまらず、
あらゆる社会規範を遵守すること、そして、お客様・社会の信頼に応え、誠実に仕事をしていくことであると考えています。
全役員・社員がコンプライアンスの担い手であり、コンプライアンスが業務遂行の前提であるという基本理念のもと、
コンプライアンスの推進に向けて取り組んでいます。

1.1 コンプライアンス体制当社は、トップマネジメントの下に、「コンプライアンス委員会」を設置し、
コンプライアンス課題に関する対応策の審議、取組状況のモニタリング等を通じ、
コンプライアンス体制の全般的統制・管理を行っています。 加えて、諮問機関として「ISMS委員会」や
「反社会的勢力対策委員会」を設置し、お客様情報を中心とする情報資産保護制度の確立・推進や、
暴力団をはじめとする反社会的勢力との関係遮断に向けた対策の協議・社内啓発の推進等、
各課題毎の具体的な対応策を検討、実施しています。さらに、各部署（チーム）には「法令等遵守責任者」を置き、
コンプライアンスの徹底を業務運営の中に組み込んだ体制をとっています。
そして、不祥事件やその疑わしい行為があった場合には、「法令等遵守責任者」から「コンプライアンス委員会」に
一元的に報告される体制をとる等、コンプライアンスに関する情報の全社的な把握に努めています。

1.2 コンプライアンス・プログラムの策定・実施コンプライアンスを推進する具体的な実践計画として、
毎年、トップマネジメントにおいて「コンプライアンス・プログラム」を策定しています。
そして、各部署では、全社の計画をふまえ、それぞれの固有・業務課題に応じ、
各部署毎にコンプライアンスの取組計画を策定し、日常業務の中で実践しています。
その取組計画の策定・実施状況を、「コンプライアンス委員会」にて定期的に確認・フォローを行うとともに、
新たな課題を取組計画に反映させる運営としています。

1.3 コンプライアンスの理念の教育・徹底当社は、全役員・職員が業務を行うにあたり
守るべき原則・規準を定めた「行動規範」を策定しています。
「行動規範」は、「お客様のためになっているか」「法律的に見て、また社会通念から見て正しいかどうか」
「人権を侵害していないか」等、自らの業務遂行上、判断に迷う場合にいつでも参照できるようにしています。
また、全役員・職員に対して、定期的に研修等を実施し、コンプライアンスの周知・徹底を図っています。

2. 反社会的勢力への対応

2.1 反社会的勢力に対する基本原則当社は、「行動規範」において全役員・職員が
業務の遂行にあたって遵守すべき原則・規準を定めています。
この中で、暴力団等の市民社会の秩序や安全に脅威を与える反社会的勢力とは関係を持たないこと、
反社会的勢力に接した場合は速やかに上司に報告し、毅然とした態度で組織的に対応することを掲げています。

2.2 反社会的勢力に対する取組当社は、「企業行動指針」において市民社会の秩序や安全に脅威を与える反社会的勢力とは
断固として対決することとしています。
また、その実現に向けた社内体制の整備として「反社会的勢力対策委員会」を設置し、
警察をはじめとする外部組織との連携、暴力団等の反社会的勢力にかかわる対策の協議・社内啓発の推進等を行っています。
また、「総務部」を反社会的勢力対応組織として位置付け、不当要求等の事案が発生した際には、
速やかに「総務部」へ報告する体制とする等、反社会的勢力による被害を防止するための一元的な管理体制を構築しています。

2.3 契約書や取引約款への暴力団排除条項の導入政府は、「企業が反社会的勢力による
被害を防止するための指針」（平成19年6月19日付け）の中で、「反社会的勢力が取引先や株主となって、
不当要求を行う場合の被害を防止するため、契約書や取引約款に暴力団排除条項を導入するとともに、
可能な範囲内で自社株の取引状況を確認する」ことを、反社会的勢力による被害を防止するための
平素からの対応のひとつとして掲げています。
当社も、契約の相手方に、①自らが反社会的勢力でないことについて表明及び保証させる、
②契約締結後に反社会的勢力に所属しないことを誓約させる、
③反社会的勢力に該当する場合を契約解除事由として規定する、等の方法により、暴力団排除条項を導入しています。

3. リスク管理の徹底

3.1 リスク管理の重要性近年、IT化の進展に伴い、不正アクセスやコンピュータウイルスによる被害、
及び内部不正者や外注業者による情報漏えい事件など、情報資産を脅かす要因が著しく増加しており、
これらの脅威に対して適切にリスクアセスメントを実施して、企業における総合的な情報セキュリティを確保しなければなりません。
これに加え、自然災害や事故、感染症、インフラ障害、システム障害等をはじめとする様々な事態によりビジネスが中断、
休止することは、企業・組織にとって極めて大きな問題であり、このような事態に事前に備えておかなければなりません。
当社では、お客様ニーズをふまえた品質の高い情報技術サービスを、安全に、継続的に提供するために、
ISMS及びBCMSの構築・運用を行っています。
ISMS（Information Security Management System）：個別の問題毎の技術対策の他に、
組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、
プランを持ち、資源を配分して、システムを運用することです。
BCMS（Business Continuity Management System）：組織にとっての重要な業務・サービスが停止したときの影響を
最小限に抑え、いかに事業を継続するかという視点で、組織の現状を理解し、事業継続計画を策定し、
演習により計画の実効性評価を行い、システムを運用するものです。

3.2 リスク管理体制リスク管理にあたっては、トップマネジメントの下に、ISMS及びBCMSの各委員会を設置し、
各種リスクの特性に応じた適切なリスク管理を行うとともに、各種リスクが全体として経営におよぼす影響について、
統合的な管理を行っています。
各委員会の体制の詳細は、それぞれ、「ISMS組織体制図」及び「BCMS運用範囲定義書」に記載しています。

4. 個人情報の保護当社は、情報システム開発及びコンサルティング等を専門に行う事業者として、
速さに加え品質の高いサービスを提供することにより、更なる顧客満足度を提供できる企業となるべくことを事業理念として掲げ、
それに相応しい組織となるために、「個人情報保護方針」を制定するとともに、当社が取扱う個人情報の保護について、
社会的責任を十分に認識して、本人の権利利益を保護し、個人情報に関する法規制等を遵守してまいりました。
今後も引続き、その徹底・強化に努めてまいります。