セキュリティポリシー（基本方針）

Ⅰ 会社の声明

当セキュリティポリシーは、情報資産（Ⅱ2‐1で定義）の安全対策に関する会社の基本方針を示すものであり、社内情報のセキュリティ維持のための必要な指示を含み、会社の保有するすべての情報資産の適切な保護と活用を実現するためのものである。
役員及び全社員は、このセキュリティポリシーが有効に機能するよう努め、これを支持しなければならない。

Ⅱ 情報資産

2－1. 情報資産とは

情報資産とは、社内情報（営業秘密情報、秘密情報、一般情報等の有用な情報）及び社内情報を記録し、保存し或いはこれを媒介する情報システム並びに、これらを正当に保護し活用するために必要な社内体制を含むものをいう。すなわち、業務上必要な或いは有用なビジネス情報（開発情報、顧客情報等）、社内文書、各種データファイル、ネットワーク、ハードウェア・ソフトウェアのみならず、秘密情報の管理･活用、システム開発・運用のために必要な要員等をも含むものである。
これらは会社の重要な資産であり、正当性・信頼性或いは秘密性が失われると会社はビジネス上の損害を被る可能性が大きい。このため、会社はこれらに対する管理者を設置し、さまざまな脅威（不正活用、損失、破壊、故障、誤処理、災害、盗難、漏洩等）による被害を排除するために、これらの重要性に応じた適切な管理が行われなければならない。

2－2. 情報資産へのアクセス

会社は、情報資産がその目的に沿って適切に活用されるよう、正当な必要性のある者のみにアクセスを許可する。会社はこのために必要な時間と資源を投入し、情報資産へのアクセスを管理し、監視する。

2－3. 会社による確認

会社は、情報資産が適切に管理・保護・活用されていることを確認する必要がある。このため会社は定期的にそれらの調査を行い、報告を求める。

2－4. 会社の意思決定

会社の意思決定は、情報資産の適切な活用と保護に背反するものであってはならない。
すべての役員・管理者は、社員に対してセキュリティポリシーに違反する行為を命じてはならない。

Ⅲ セキュリティ管理体制

3－1. 全社セキュリティ管理

会社は、セキュリティの維持管理を全社統一的な視点で行うために統括的セキュリティ管理部門として法務部を指定し、必要なセキュリティ管理体制を整備させる。
法務部は、セキュリティポリシーやセキュリティに関する各種の規程を整備し、有効に機能させる職務を担う。

3－2. 各部門のセキュリティ管理

各部門においては、部門毎の管理責任者を設置する。管理責任者は、自部門における情報資産の活用と適切な管理について責任を負う。
各部門の管理責任者は、部門のセキュリティ担当として管理担当者を任命する。管理担当者は、部門における安全対策の周知・維持・管理を実施し、それを有効に機能させる義務がある。
法務部は、各部門における情報資産の管理を統括・支援する。

3－3. 監査体制

監査室は、各部門がセキュリティポリシー及びそれに基づいた取決めや手順を遵守しているか調査し、報告する。

Ⅳ 全社員の参加と義務

4－1. 役員及び社員の義務
　情報資産に対する安全対策の実施には、すべての役員及び社員が参加しなければならない。
すべての役員及び社員は、当セキュリティポリシーに準拠した手続を実施し、安全対策を有効に機能させる義務を負っている。

4－2. 違反の防止
　会社は、情報資産の安全対策に対する違反を防止・抑制するための体制を整備する。違反をした者は、当事者個人のみならず、該当の管理責任者も含めて法令、就業規則等に照らし処罰する。

Ⅴ 情報資産に関する法令等の遵守

　役員及び社員は、職務の遂行において活用する情報資産に関連する法令、社内規程等を遵守し、これに従う。関連する法令の周知は各部門の管理責任者がその責任を負い、法務部がこれを支援する。

以上