# セキュリティ・ポリシー（基本方針）

## Ⅰ．経営者の声明

ビジネスを継続的・安定的に行う上で、会社の情報資産に対し、適切な安全対策を実施することは、ビジネス上の重要な要件です。情報資産は当社にとって最重要で必要不可欠な資産であり、これを高い品質と信頼性で適切に保護していくことが、発展向上につながると考えます。

当セキュリティ・ポリシーは情報資産の安全対策に関する当社の基本方針であり、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を実現するためのものです。

このセキュリティ・ポリシーが有効的かつ安定的に機能するよう、経営者を含め全ての社員がこれに関与し、これを支持します。また、当セキュリティ・ポリシーはいかなる事象もこの例外としません。

## Ⅱ．情報資産

### 2‐1．情報資産とは

情報資産とは、情報と情報システム、ならびにそれが正当に保護され使用され機能するために必要な要件の総称です。ハードウェア、ソフトウェア、ネットワーク、各種データファイルのみならず、業務遂行のために必要な要員やドキュメントをも含むものです。また、情報資産には、顧客の個人情報、顧客企業に関する機密情報及び顧客企業から預かっている個人情報や企業情報等の情報資産も含みます。さらに、グループ社員の個人情報、採用前の履歴書等の個人情報、協力会社及びその協力社員の個人情報も含みます。

### 2－2．情報資産の分類

情報資産はそれらの重要性に応じて区別し管理が行われます。

### 2－3．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使用されるよう、正当な必要性に基づくアクセスのみを許可します。

### 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利用と保護に背反しません。また、すべての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ることを禁止します。

## Ⅲ．セキュリティ管理体制

当社におけるセキュリティ管理体制は、全社セキュリティ管理、部門セキュリティ管理、セキュリティ監査で構成します。

### 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セキュリティ委員会を設置し、必要なセキュリティ管理体制を整備します。

セキュリティ委員会は、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定を確立し、有効に機能させる職務を担います。

### 3－2. 各部門のセキュリティ管理

各部門においては、セキュリティ対策の周知、維持・管理遂行義務を各部部長が負い、これを実施します。また、この機能を他の社員に委譲することは許しません。セキュリティ委員会は各部門における情報資産管理を指導支援します。

### 3－3. セキュリティ監査

会社はセキュリティ対策関連業務の監査役としてセキュリティ監査担当者を任命します。監査担当者は各部門がセキュリティ対策に基づいて業務遂行していることを監査します。

## Ⅳ. 情報セキュリティマネジメントシステムの継続的改善

当社は、情報セキュリティマネジメントシステムを継続的に改善します。

## Ⅴ. 全ての社員の参加と義務

### 5－1. 社員の義務

セキュリティ対策の実施には、全ての社員（役員、外部委託者を含む）が参加します。

### 5－2. 教育の実施

会社は全ての社員に対し、セキュリティ対策に関する適切な教育を実施します。

### 5－3. 第三者とのセキュリティ

会社は業務に係わる業務委託先等の第三者とのセキュリティに関しても、必要なセキュリティ対策が実施されていることを確認します。

### 5－4. セキュリティ管理要領及び ISMS マニュアルの策定とその実施

会社は、本セキュリティ・ポリシーに基づいた具体的な実施要領としてのセキュリティ管理要領、ISMS マニュアルを策定し、これらを有効に機能させるものとします。

### 5－5. 罰則

全ての社員は、本セキュリティ・ポリシー及び、これに基づくセキュリティ管理要領及び ISMS マニュアルを遵守し、これらに違反した場合は、就業規則に基づく懲罰の対象となります。

懲罰の対象は違反当事者個人のみならず、該当する情報資産管理者も対象となることがあります。

## Ⅵ. 情報資産に関する法令の遵守

全ての社員は、職務の遂行において使用する情報資産に関連する法令を遵守し、これに従います。

２０１８年3月２６日改定
２０１８年3月２６日施行

株式会社 K-ZONE
代表取締役社長　堀内　誠