

# 情報セキュリティポリシー

制定日：2017年 2月 1日

改定日：2026年 9月 1日

代表取締役社長 松島 聡

シーオス株式会社（以下「当社」といいます）は、企業理念と行動規範に基づき、お客さまのビジネスを支えるサービスを提供しております。これらの事業を推進するにあたり、情報セキュリティ体制を確立し維持することが重要であると認識し、下記のセキュリティポリシー（以下「本ポリシー」）により、お客様からお預かりする情報ははじめとした当社が取り扱う全ての情報資産を適切に保護するための情報セキュリティを確保いたします。

## 1. 基本方針

### 1. 1. 目的

当社は、情報資産を不正なアクセス、意図しない公開・流出、サービスの妨害・不能等の脅威から保護し、情報セキュリティを総合的、体系的かつ継続的に確保することを目的として本ポリシーを定めます。

### 1. 2. 適用範囲

当社の役員、社員、派遣社員、外部委託先の社員を含めた全従業員は、本ポリシーを遵守します。

### 1. 3. 法令などの遵守

当社と全従業員は、情報セキュリティに関連する法令・規制を遵守します。

## 2. 管理体制とインシデント対応

### 2. 1. 管理体制の維持

当社は、保有するすべての情報資産の保護および適切な管理を行うため、全社レベルの情報セキュリティ管理状況の把握と、リスク分析に従った必要なセキュリティ対策を迅速に実施できる体制を維持します。

### 2. 2. インシデント発生後の対応

当社は、セキュリティインシデントに対して対応手順を確立し、万が一発生した場合、速やかに対応および関係者・関係機関への報告を行い、適切な再発防止を行います。

### 3. 技術的セキュリティ対策

#### 3. 1. ゼロトラスト原則に基づく監視

当社は、すべてのアクセスを信頼せず、常に検証するゼロトラスト原則に則り、通信および端末の状態を継続的に監視・制御します。

#### 3. 2. クラウドサービス利用方針

当社は、業務でクラウドサービスを利用する際、会社が認可したサービスのみを使用します。また、厳格なアクセス制御とデータ保護対策を実施し、安全なクラウド利用環境を維持します。

#### 3. 3. AI 利用方針

当社は、生成 AI 等の活用にあたり、入力データが学習に利用されない環境を利用し、機密情報の漏洩を防止します。

### 4. クラウドサービスの提供

4. 1. 当社は、クラウドサービスカスタマとしての責任において、クラウド環境へのデータ保存やマルチテナントの仮想化環境における処理、クラウドサービスプロバイダの特権管理者によるアクセス可能性、ならびにプロバイダの所在地およびデータ保存国の地理的要因を考慮します。

4. 2. 当社は、クラウドサービスプロバイダとして、セキュリティ要求事項を満たしたサービス設計・実装を行うとともに、内部リスク対策、マルチテナント環境の隔離、お客様データやアカウントの厳格なアクセス・ライフサイクル管理を実施します。さらに、システムの変更通知や仮想化セキュリティの強化に努め、万一の違反発生時には、調査やフォレンジックを支援するための迅速な情報共有と通知を行います。

### 5. 業務委託先の管理

#### 5. 1. 業務委託先のセキュリティ要件

当社は、業務を外部に委託する場合、委託先のセキュリティ体制を十分に評価し、当社と同等以上のセキュリティレベルを維持するよう要請するとともに、定期的な状況確認に努めます。

### 6. 事業継続性（BCP/DR）

#### 6. 1. 災害・システム障害時の復旧体制

当社は、災害、システム障害、サイバー攻撃などの予期せぬ事態による事業への影響を最小限に抑え、有事の際は迅速に事業を復旧できる体制を維持します。

## 7. コンプライアンスと教育

### 7. 1. 情報セキュリティに関する社内規定の整備

当社は、本ポリシーに基づいた社内規定を整備し、情報資産の適切な管理を行うための明確な方針・ルールを社内に周知徹底します。

### 7. 2. 情報セキュリティ教育の実施

当社は、全役員、社員、派遣社員、外部委託先の社員を含めた全従業員に対し、情報セキュリティポリシーについての必要な教育を行い、啓発を図ります。

### 7. 3. 情報セキュリティ内部監査の実施

当社は、情報セキュリティマネジメントシステム（以下 ISMS）を構築し、実行・維持・改善をします。ISMS や法令、会社が定めた規定・ルールなどが順守され、有効に機能しているかを検証するため、定期的又は不定期に情報セキュリティ内部監査を実施していきます。それを受け、ISMS や規定・ルールなどを継続的に改善します。

以上