情報セキュリティ基本方針

1. 基本理念

AMAZY INC.（以下、「当社」）は、情報資産の適切な保護を経営の重要課題の一つと位置付け、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）を確立し、継続的な改善を図ることで、顧客、取引先、および社会からの信頼を確保します。

2. 適用範囲

本方針は、当社の全事業活動および情報資産を対象とし、当社の従業員（役員、正社員、契約社員、派遣社員、業務委託を含む）および関係者に適用します。

3. 情報セキュリティ管理体制

当社は、情報セキュリティ責任者（CISO）を任命し、以下の管理体制を確立します。

- 情報セキュリティ委員会を設置し、ポリシーの運用、リスク評価、対策の策定、監査、改善活動を実施
- ISMS マネジメントレビューを定期的に実施し、方針・運用状況を見直し、継続的な改善を推進

4. 情報資産の分類と管理

当社は、情報資産（データ、システム、ネットワーク、設備等）を特定し、以下の方法で分類・管理します。

- 情報資産を機密性・完全性・可用性の観点から分類
- 情報資産ごとに適切な管理策（暗号化、バックアップ、アクセス制御等）を適用
- 定期的なリスクアセスメントを実施し、リスク低減策を講じる

5. アクセス管理

- 最小権限の原則（Least Privilege Principle）に基づき、アクセス権限を設定
- ID・パスワード管理ポリシーを策定し、多要素認証（MFA）を導入

- 物理的アクセス（サーバールーム、オフィス等）も適切に管理し、監視・ログ管理を実施

6. 情報の取り扱い

- 機密情報、個人情報、取引先情報などの取り扱いに関する明確なルールを策定
- GDPR、CCPA、個人情報保護法などの関連法令・規制を遵守
- 情報の送受信・保管時には暗号化技術を適用し、機密性を確保
- クラウドサービス利用時のセキュリティ要件を定め、適切なベンダー管理を実施

7. 教育および啓発

- 従業員・関係者に対し、年 1 回以上のセキュリティトレーニングを義務化
- フィッシング詐欺、ソーシャルエンジニアリング対策の意識向上施策を実施
- 新入社員研修に情報セキュリティ教育を組み込む

8. セキュリティインシデント対応

- CSIRT（Computer Security Incident Response Team）を設置し、セキュリティインシデントへの迅速な対応を実施
- インシデント対応計画（IRP: Incident Response Plan）を策定し、事前対応・検知・対応・復旧・再発防止策を確立
- ログ監視・侵入検知システム（IDS/IPS）を導入し、常時監視体制を構築

9. 事業継続管理（BCM）

- 事業継続計画（BCP: Business Continuity Plan）および災害復旧計画（DRP: Disaster Recovery Plan）を策定
- システムの可用性を確保するため、定期的なバックアップおよび復旧テストを実施
- サプライチェーンリスクを考慮し、取引先のセキュリティ評価を実施

10. 法令および規範の遵守

- ISMS（ISO/IEC 27001）、NIST CSF、CIS Controls などの国際基準を参考にセキュリティ対策を強化
- 各国のプライバシー法規制（GDPR、CCPA、日本の個人情報保護法）を遵守
- 取引先との契約において、情報セキュリティ要件を含める

11. 継続的な改善

- 年 1 回以上の内部監査および第三者監査を実施し、運用状況を評価
- セキュリティ脅威の変化に対応するため、脆弱性管理プロセスを導入
- PDCA（Plan-Do-Check-Act）サイクルを適用し、情報セキュリティの継続的な改善を実施

12. 問い合わせ先

本ポリシーに関するお問い合わせは、以下の窓口までご連絡ください。

【問い合わせ窓口】
会社名： AMAZY INC.（アメイジィ株式会社）
住所： 東京都渋谷区道玄坂 1-12-1 渋谷マークシティ