情報セキュリティ基本方針

株式会社 KortValuta（以下「当社」という）は、カード運営事業を通じてお客様に価値あるサービスを提供していくために情報セキュリティに取り組むことはきわめて重要な責務であると認識しております。
この考えのもと、事業活動のために保有または利用する情報資産を盗難、改ざん、破壊、漏えい、不正アクセス行為等の脅威から保護し、適切に管理・運用を行うための指針として、情報セキュリティ基本方針（以下「本基本方針」という）を定めました。
当社は、本基本方針に従い情報セキュリティを構築、運営し、必要な保護と適切な安全対策を講じるとともに、役員、社員、契約社員、派遣社員および協力会社社員(以下「従業員」という)が倫理観をもって業務に携わることをここに宣言いたします。

1. 情報セキュリティポリシーの策定
   当社経営陣の意向表明に従い情報セキュリティポリシーを策定し、従業員へ周知徹底する。従業員は、この情報セキュリティポリシーを遵守して情報セキュリティ対策を遂行する。

2. 情報セキュリティ管理体制の確立
   ・情報セキュリティに関して、全般的な責任を持つ情報セキュリティ管理責任者（以下管理責任者という）を設置する。管理責任者は、セキュリティ事件・事故に対応することを含め、情報セキュリティの構築・運営に関して組織を指導し、管理する責任を持つ。
   ・全社レベルの情報セキュリティの状況を正確に把握し、必要な対策を迅速に実施できるようにするため、情報セキュリティ委員会を設置する。

3. 見直
   経営環境の変化、社会環境や法規制の変化、情報関連技術の最新動向、および新たに発見されたリスクに照らし合わせて、本基本方針の適宜見直しを行い、継続的な改善を行う。

4. 情報システム・セキュリティ対策の実施
   当社情報システム資産を保護するために、リスク分析を実施し不正アクセス対策、ウイルス対策、漏洩対策、信頼性対策など情報システムに対するセキュリティ対策を実施する。

5. 業務委託に関するセキュリティ対策
   当社業務の外部委託について、会社機密情報および個人情報の保護の観点から、委託先の適格性の審査、契約書の内容に関する見直し、改善を図る。

6. 法的および契約上の要求事項への適合
   当社情報セキュリティに関連する法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるために、これらの要求事項を明確にして、適合するための対策を策定し実施する。また、これらに違反した場合には就業規則等に照らし合わせて然るべき処分を行う。

7. 情報セキュリティに関する教育・訓練及び周知・徹底

   従業員に対し、定期的な情報セキュリティに関する教育・訓練を行い、情報セキュリティの重要性、適切な取り扱いおよび管理に関し周知・徹底を図る。

8. セキュリティ事故予防と事故発生時の対応

   当社はセキュリティ事故の防止に努めるとともに、万一情報セキュリティに関連する事故が発生した場合は、あらかじめ定められた手続きに則り速やかに管理責任者にその内容を報告し、管理責任者は直ちに関係者に報告すると共に、必要に応じて緊急措置を講じることとする。これら情報セキュリティ事故については、その事故原因を分析し再発防止策を講じる。

9. 事業継続管理

   偶発的に発生する災害・故障・過失及び意図的に発生する情報資産の悪用などによる事業の中断を可能な限り抑え、事業の継続を確保する。

10. クレジットカード情報の取扱について

    当社は、クレジットカード情報を保管、処理、伝送する業務の範囲において、クレジットカード情報を保護するために定められた基準である PCI DSS (Payment Card Industry Data Security Standard) の要件に準拠する。

    - PCI DSS に準拠したポリシーと手順を整備する。
    - PCI DSS に準拠するための体制を整備し、すべての担当者の役割と責任を明確にする。
    - 経営者を含む全ての従業員は上記に定めたポリシーと手順を遵守する義務を負う。
    - PCI DSS に準拠するための活動は、適宜経営陣による見直しを行い、改善を図る。

制定：2019 年 7 月 29 日
改訂: 2020 年 12 月 10 日
株式会社　KortValuta
代表取締役　柴田　秀樹