

情報セキュリティ基本方針

1. 目的

当社が事業を行う上でお客様からお預かりする個人情報及び契約・仕様情報等の機密情報の保護はもとより、これらの情報を保管、利用等する上で必要な資産の保護・管理及びセキュリティ環境の強化を図ることにより、セキュリティに関する事件・事故を未然に防止します。また、サービスを提供していく中で、関係する法令・規制・規則及びお客様との契約要求事項を遵守することにより、お客様から存在感のある「信頼される企業」として、将来にわたり成長・発展し続けることを目的とし、行動します。

2. 情報セキュリティの定義

情報セキュリティとは、機密性、完全性及び可用性を確保し維持することをいう。

- (1) 機密性：許可されない個人、エンティティ（団体等）又はプロセスに対して、情報を使用不可又は非公開にする特性（アクセスを許可された者だけが、情報にアクセスできること。）
- (2) 完全性：資産の正確さ及び完全さを保護する特性
（情報は正確であり、情報の処理方法が統一化されていること。）
- (3) 可用性：認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性（アクセスを許可された者が、必要なとき必要な情報にアクセスできること。）

3. 適用範囲

情報セキュリティマネジメントの適用範囲は、当社の全組織及び全業務とする。

- (1) 組織：株式会社 Avirity Information
- (2) 拠点：東京都渋谷区広尾1丁目9-18 雨宮ビル2F
- (3) 業務：ホームページ制作及び保守管理、コンピュータ並びに携帯電話のシステム及びプログラムの企画、開発、販売、提供及びコンサルティング、労働者派遣事業法に基づく特定労働者派遣事業、前各号に附随する一切の業務

4. 実施事項

- (1) 情報セキュリティの基本的な維持事項である「機密性」、「完全性」及び「可用性」を確保し維持すること。
- (2) 社内規則、規制及び法律の要求事項に対して違反しないこと。
- (3) 重大な障害または災害から事業活動が中断しないように、予防及び回復手順を策定し、定期的な見直しをすること。
- (4) 情報セキュリティの教育・訓練を適用範囲全ての社員等に対して定期的実施すること。
- (5) 情報セキュリティの事件事故及び疑いある弱点のすべてが報告され、調査されること。
- (6) 情報セキュリティの違反及び、疑いある違反のすべてが報告され、調査されること。

5. 責任と義務及び罰則

- (1) 情報セキュリティの責任は、代表取締役社長が負う。そのために代表取締役社長は、全ての社員等が必要とする資源を提供する。
- (2) 全ての社員等は、情報を守る義務がある。
- (3) 全ての社員等は、本基本方針を維持するため策定された手順に従わなければならない。
- (4) 全ての社員等は、情報セキュリティに対する事故及び弱点を報告する責任を有する。
- (5) 全ての社員等は、当社が取り扱う情報資産の保護を危うくする行為を行なった場合は、懲戒処分及び法的処分の対象となる。

6. 定期的見直し

経営者は、常に化するリスクに対して効率的にマネジメントを行なうため、情報セキュリティマネジメントシステムの見直しを毎年6月に行う。また、本方針と整合性のある情報セキュリティ目標を確立し達成状況を評価します。

制定：2012年10月02日

改訂：2020年11月18日

代表取締役社長 奥野 友美