

情報セキュリティ基本方針

1. 目的

本基本方針は、お客様の信頼に応えるために情報資産を適切に取り扱い、故意、過失、災害による破壊、漏洩、改ざん、喪失などから情報資産を保護することを目的として策定されたものである。

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: 許可されていない個人、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。(情報を漏えいや不正アクセスから保護すること。)
- (2) 完全性: 資産の正確さ及び完全さを保護する特性(情報の改ざんや間違いから保護すること。)
- (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。(情報の紛失・破損やシステムの停止などから保護すること。)

3. 適用範囲

組織	株式会社ラディアント・ソリューションズ
施設	本社
業務	技術者派遣管理、IT インフラ構築及びシステム開発
資産	上記業務、サービスにかかわる書類、データ、情報システム
ネットワーク	本社ネットワーク

4. 実施事項

- (1) 適用範囲の全ての情報資産を脅威(漏えい、不正アクセス、改ざん、紛失・破損)から保護するための情報セキュリティマネジメントシステムを確立、導入、運用、監視、見直し、維持及び改善するものとする。
- (2) 情報資産の取り扱いは、関係法令及び契約上の要求事項を遵守するものとする。

(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ものとする。

(4) 情報セキュリティの教育・訓練を適用範囲すべての社員に対して定期的実施するものとする。

5. 責任と義務及び罰則

(1) 情報セキュリティの責任は、代表取締役が負う。そのために代表取締役は、適用範囲のスタッフが必要とする資源を提供するものとする。

(2) 適用範囲のスタッフは、お客さま情報を守る義務があるものとする。

(3) 適用範囲のスタッフは、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ものとする。

(4) 適用範囲のスタッフは、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ものとする。

(5) 適用範囲のスタッフが、お客さま情報に限らず取り扱う情報資産の保護を危うくする行為を行った場合は、社員就業規則に従い処分を行なうものとする。

6. 実施事項

情報セキュリティマネジメントシステムの見直しは、環境変化に合わせるため定期的実施するものとする。

7. 認証情報

取得認証規格 ISO/IEC 27001:2013 JIS Q 27001:2014

認定機関 ANAB(米国適合性認定機関)
JIPDEC(日本情報経済社会推進協会)

認証登録番号 IS587916

発効日 2015年9月23日

審査登録機関 BSI グループジャパン株式会社

2019年1月1日制定

株式会社ラディアントソリューションズ