情報セキュリティ基本方針

1．目的

当社は、お客様企業の情報システムの安定稼働と情報資産を守り、情報管理社会の安定・発展に貢献する企業としてお客様やパートナー様から情報セキュリティに関して高い水準を要求されております。

情報セキュリティに関連する事故や犯罪が多発する中、当社のサービスをお客様企業に安心してご利用いただくために、ISO27001 に準拠した情報セキュリティ対策を策定し、継続的に改善を行っていきます。

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）またはプロセスに対して、情報を使用不可または非公開する特性（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：エクストリーク株式会社

(2) 拠　点：本社：東京都港区芝 4-9-4　芝浜ビル　　本社別館：東京都港区芝 1-4-4　芝桝田ビル

北海道事業所：札幌市中央区北 3 条西 2-2-1　日通札幌ビル　　関西事業所：大阪市淀川区宮原 5-1-3　NLC 新大阪アースビル

(3)業　務：システムインテグレーション

IT エンジニアアウトソーシングサービス

IT ファシリティエンジニアリングサービス（ITFE）

-構内情報インフラサービス

-IT リロケーションサービス

-ファシリティソリューションサービス

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に実施すること。

(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．継続的改善

経営者は、常に変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、当社のＩＳＭＳを継続的に改善します。また、

本方針と整合性のある情報セキュリティ目的・目標を確立し、達成状況を評価します。

改訂：令和　2 年　7 月　29 日

エクストリーク株式会社

代表取締役社長　　村瀬　耕太郎