岩手中部水道企業団情報セキュリティ基本方針

（目的）

第１　この基本方針は、企業団が保有する情報資産の機密性、完全性及び可用性を維持し、地域住民に信頼される安定した水道事業を行うために、企業団の情報セキュリティ対策について基本的な事項を定めることを目的とする。

（定義）

第２　この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 情報

書類又は電磁的記録媒体に記録された、ある特定の目的について適切な判断をするため、または行動の意思決定をするために役立つ資料や知識をいう。

(2) 情報システム

電子機器及び電磁的記録媒体並びに電子機器周辺機器で構成された、情報を処理するためまたは水道施設を制御及び管理するための仕組みをいう。

(3) ネットワーク

情報システムを利用し情報を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(4) 情報資産

情報及び情報システム、システム開発、運用及び保守のための資料等情報を管理する仕組みの総称をいう。

(5) 情報セキュリティ

企業団が保有する全ての情報資産について、機密性、完全性、可用性を維持することをいう。

(6) 職員等

企業団の情報資産を業務上取り扱う全ての職員（非常勤及び会計年度任用職員を含む）をいう。

(7) 情報セキュリティポリシー

本基本方針及び岩手中部水道企業団情報セキュリティ対策基準をいう。

(8) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(9) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(10) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(11) 情報セキュリティインシデント

情報セキュリティに関する障害・事故及びシステム上の欠陥をいい、企業団が保有する情報資産の機密性、完全性又は可用性を侵害する事象及びそのおそれのある事象を含む。

（対象とする脅威）

第３　情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等。

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等。

(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等。

(4) 大規模・広範囲にわたる疫病による要員不足に伴うシステム運用の機能不全等。

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等。

（適用範囲）

第４　行政機関と情報資産の適用範囲は以下のとおりとする。

(1) 行政機関の範囲

本基本方針が適用される行政機関は、内部部局、議会、監査委員とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（情報を印刷した文書を含む）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

（職員等の遵守義務）

第５　職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

（情報セキュリティ対策）

第６　企業団の情報資産を保護するため、次に掲げる情報セキュリティ対策を講ずるものとする。

(1) 組織体制

企業団の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

企業団の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 物理的セキュリティ対策

情報資産への損傷、妨害等から保護するため、企業団サーバへの接触、パソコンの管理、停電対策等物理的セキュリティ対策を行うものとする。

(4) 技術的セキュリティ対策

情報資産を不正アクセス等から適切に保護するため、重要な情報システムへのアクセス権限の管理、不正プログラムに対する対策等技術的セキュリティ対策を行うものとする。

(5) 人的セキュリティ対策

不正行為、操作ミス、紛失、盗難等の人為的要因による情報資産の喪失を防止するため、職員等が遵守すべき事項を定めるとともに、職員等に対する情報セキュリティ研修、情報システムの運用等外部委託先に対する指導、監査等の人的セキュリティ対策を行うものとする。

(6) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時の対応を講ずる。

(7) 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、必要な管理体制を整備し、セキュリティ対策を講じる。

ソーシャルメディアサービスを利用する場合には、必要に応じてソーシャルメディアサービスの運用手順を定め、発信できる情報については対策基準に基づいて取り扱わなくてはならない。

（情報セキュリティ監査及び自己点検の実施）

第７　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し）

第８　情報セキュリティ監査及び自己点検を評価した結果、情報セキュリティポリシーの見直しが必要になった場合及び情報システム等の変更、新たな脅威等情報セキュリティを取り巻く状況が変化した場合には、情報セキュリティポリシーを適宜見直すものとする。

（情報セキュリティ対策基準の策定）

第９　第６、第７及び第８に規定する情報セキュリティ対策の具体的な遵守事項及び判断基準を統一的に定めるため、情報セキュリティ対策基準を策定するものとする。

（情報セキュリティ実施手順の策定）

第 10　情報セキュリティ対策基準に基づく情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を別に定める。なお、情報セキュリティ実施手順は、公にすることにより行政運営に重大な支障を及ぼすおそれがあることより非公開とする。

附則

この基本方針は、平成 27 年４月１日から施行する。

附則

この基本方針は、令和８年４月１日から施行する。