八戸圏域水道企業団情報セキュリティ基本方針

（目的）
第１条　八戸圏域水道企業団情報セキュリティ基本方針は、八戸圏域水道企業団（以下「企業団」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、企業団が実施する情報セキュリティ対策の基本的な事項を定めることを目的とする。

（定義）
第２条　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)ネットワーク
　コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。
(2)情報システム
　コンピュータ、ネットワーク、記録媒体等で構成され、情報処理を行う仕組みをいう。
(3)情報資産　次に掲げるものをいう。
　ア　情報システム並びに情報システムに関する設備及び電磁的記録媒体
　イ　情報システムで取り扱う情報（これを印刷した文書を含む。）
　ウ　情報システムの仕様書、ネットワーク図その他のシステム関連文書
(4)情報セキュリティ
　情報資産の機密性、完全性及び可用性を維持することをいう。
(5)情報セキュリティポリシー
　この情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。
(6)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。
(7)完全性
　情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。
(8)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。

（情報セキュリティポリシーの位置付け）
第３条　情報セキュリティポリシーは、企業団の情報資産に関する情報セキュリティ対策について、総合的かつ体系的にまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

（情報セキュリティポリシーの対象範囲）
第４条　情報セキュリティポリシーの対象範囲は、企業団における情報資産並びに情報資産の取扱いを伴う業務に携わる全ての職員及び情報資産の取扱いを伴う業務を受託したもの（以下「職員等」という。）とする。

（職員等の義務）
第５条　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つとともに、当該業務の遂行に当たっては情報セキュリティポリシーを遵守するものとする。

（情報セキュリティ管理体制）
第６条　最高情報セキュリティ責任者は、副企業長とする。
2　最高情報セキュリティ責任者は、企業団における全ての情報資産の管理並びに情報セキュリティ対策に関する最終決定権限及び責任を有する。
3　情報セキュリティ対策の実施及び推進並びに実効性の確保を図るため、情報セキュリティ委員

会（以下「委員会」という。）を設置する。
4　委員会の組織その他情報セキュリティ管理体制に関し必要な事項は、最高情報セキュリティ責任者が定めるものとする。

（情報システムに係る情報資産に対する脅威）
第7条　職員等は、情報システムに係る情報資産に対する次に掲げる脅威については、発生した場合の影響の大きさ等を考慮し、その危険性を特に認識するものとする。
(1)意図的要因
　不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス攻撃、サービス不能攻撃、情報漏えい、重要情報の搾取、内部不正等
(2)非意図的要因
　開発・設計の不備、操作・設定ミス、プログラム上の欠陥、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障、職員等が指定外の機器等を接続することにより発生するデータの漏えい等
(3)災害・事故
　地震、落雷、火災、水害等の災害又は事故による電力設備の損壊、通信設備の損壊、機器の損壊等
(4)疾病
　大規模・広範囲にわたる疾病による要員不足に伴う情報システムの運用に係る機能不全等
(5)他分野の障害からの波及
　電力供給の途絶、通信の途絶等の障害からの波及等

（情報セキュリティ対策）
第8条　前条各号に掲げる脅威その他の情報資産に対する脅威から情報資産を保護するため、次に掲げるセキュリティ対策の種別に応じ、当該各号に定める措置を講じるものとする。
(1)人的セキュリティ対策
　情報セキュリティ対策に関する職員等の権限や責任を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な研修・啓発を行う。
(2)物理的セキュリティ対策
　情報システムを設置する場所への不正な立入りの防止等、情報資産への損傷・妨害等から保護するための物理的な対策を講じる。
(3)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、アクセスの制御、ネットワーク監視及びコンピュータウィルス対策等を実施する。
(4)運用
　情報セキュリティポリシーの実効性を確保するため、その順守状況の確認等の運用面の対策を講ずる。また、障害が発生した際の迅速な対応を可能とするため、障害時の対応を講ずる。

（情報セキュリティ対策基準）
第9条　最高情報セキュリティ責任者は、前条の対策を講ずるに当たって、遵守すべき事項及び判断等の基準を統一的に定めるため、必要となる基本的な要件を明記した情報セキュリティ対策基準を定めるものとする。

（評価及び見直し）
第10条　情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するため、必要に応じて情報セキュリティポリシーの見直しを行うものとする。

附　則
この基本方針は、平成27年7月27日から施行する。