

長野県上伊那広域水道用水企業団情報セキュリティ基本方針

(目的)

第1条 この訓令は、長野県上伊那広域水道用水企業団（以下「企業団」という。）が管理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、情報セキュリティ対策について基本的な事項を定めるものとする。

(定義)

第2条 この訓令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 コンピュータ等で構成され、情報処理を行う仕組みをいう。
- (3)システム関連文書 情報システムの仕様書及びネットワーク図等をいう。
- (4)情報 ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）並びにシステム関連文書をいう。
- (5)情報資産 情報並びにネットワーク、情報システム、これらに関する設備及び電磁的記録媒体をいう。
- (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、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。
- (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。
- (9)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。
- (10)職員等 地方公務員法（昭和25年法律第261号）に規定された特別職及び一般職に属する地方公務員のうち、企業団に勤務する者をいう。
- (11)外部委託事業者 契約等に基づき企業団の管理する情報資産の取扱いを含む業務等に従事する者（再委託等により当該業務等に従事する者を含む。）をいう。
- (12)部外者 職員等及び外部委託事業者以外の者で、企業団の管理する情報資産に接することが認められていないものをいう。
- (13)不正アクセス 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）第3条第2項に規定する不正アクセス行為その他の不正な手段により行うアクセス（権限外のアクセスを含む。）をいう。

(情報セキュリティポリシー)

第3条 情報セキュリティポリシーは、この訓令及び第9条に定める情報セキュリティ対策基準により構成され、情報セキュリティ対策の頂点に位置するものとする。

(情報セキュリティポリシーの適用範囲)

第4条 情報セキュリティポリシーの適用範囲は、次の各号に定めるところによる。

- (1) 情報資産の範囲 企業団が管理するすべての情報資産とする。
- (2) 対象者の範囲 前号に定める情報資産に接するすべての職員等及び外部委託事業者とする。

(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ち、関係法令、情報セキュリティポリシーを遵守しなければならない。

- 2 職員等は、外部委託事業者において必要な情報セキュリティ対策が確保されることを、確実にしなければならない。

(組織体制)

第6条 情報セキュリティ対策のための組織体制を整備する。

(情報資産の分類)

第7条 情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行うものとする。

(情報資産への脅威)

第8条 情報資産に対する脅威として、次のものを想定する。

- (1) 部外者の侵入、不正アクセス、ウイルス攻撃及びサービス不能攻撃等の意図的な要因による情報資産の漏えい、破壊、改ざん及び消去等
- (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、プログラム上の欠陥、誤操作、故障等の非意図的な要因による情報資産の漏えい、破壊及び消去等
- (3) 地震、落雷及び火災等の災害、事故並びに故障によるサービス及び業務の停止等

(情報セキュリティ対策)

第9条 情報資産を前条の脅威から保護するために、次の情報セキュリティ対策を講じるものとする。

- (1) 物理的セキュリティ対策 情報資産を保護するための物理的な対策

(2)人的セキュリティ対策 職員等及び外部委託事業者が遵守すべき人的な対策

(3)その他のセキュリティ対策 情報資産に対するアクセス制御等の技術的な対策、運用面における必要な対策、並びに情報資産への侵害が発生した場合等に、迅速かつ適切に対応するための緊急時における対策

(情報セキュリティ対策基準)

第10条 前条の情報セキュリティ対策を講じるに当たって、職員等が遵守すべき行為及び判断等の統一的な基準として、情報セキュリティ対策基準を策定するものとする。

(監査・自己点検の実施)

第11条 セキュリティ対策の実施状況を定期的に監査し、その結果に基づき問題を改善し、組織内のセキュリティ体制を強化する。

(情報セキュリティポリシーの見直し)

第12条 情報セキュリティに関する状況の変化に対応するため、随時、情報セキュリティポリシーを見直すものとする。