城南衛生管理組合情報セキュリティ基本方針

1　目的

本基本方針は、本組合が保有する情報資産の維持及び管理のため、本組合が実施する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。

2　定義

(1) 情報資産

業務上作成し、又は受領した電子データ及びその内容をいう。

(2) 情報機器

業務用パソコン、サーバ、ポータブル記憶装置その他の情報資産を保存し、又は操作するための機器及びルータ、LAN ケーブルその他のネットワーク機器をいう。

(3) 情報システム

情報機器及び情報機器を操作するためのソフトウェア等で構成され、情報処理を行う仕組みをいう。

(4) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

3　対象とする脅威

本方針では、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。

- 不正アクセスやウィルスなどによる外部攻撃又は内部不正等による情報資産の漏えい、改ざん又は消失
- 情報機器の盗難、流出又は紛失による情報資産の漏えい又は消失
- 情報機器の故障又は災害等による損傷などによる情報資産の消失及び情報システムの機能不全や業務への影響
- 情報機器又は情報システムを操作するソフトウェアの誤操作等による情報資産の漏えい又は消失
- 情報資産を取り扱う委託業務や外部サービスの利用における委託先やサービス提供者の不備による情報資産の漏えい又は消失

4　適用範囲

本基本方針が適用される行政機関は、内部部局、議会、公平委員会及び監査委員とする。

5　職員等の遵守義務

職員、臨時・非常勤職員等（以下「職員等」という。）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。

6　情報セキュリティ対策

上記３　の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1）組織体制

本組合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）物理的セキュリティ

情報機器及びその設置場所の管理について、物理的な対策を講じる。

（3）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（4）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（5）業務委託と外部サービスの利用

業務委託や外部サービスの利用において情報資産又は情報システムを取り扱う場合には、情報セキュリティに関する観点から必要な要件を定め、これを満たす業者やサービスを利用するとともに、必要に応じてこれを遵守させる措置を講じる。

（6）運用

職員等の情報セキュリティポリシーの遵守状況や情報システムの状態につ

いて確認する体制を構築し、問題が発覚した場合は速やかに必要な措置を講じる。

7　情報セキュリティポリシーの見直し

情報セキュリティに係る内外の環境の変化に対応するため、また、情報セキュリティポリシーの不備によるリスクを排除するため、情報セキュリティに関する情報を収集し、情報システムの運用状況を確認し、必要に応じて情報セキュリティポリシーを見直す。

8　情報セキュリティ対策基準の策定

上記6　及び7　に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

9　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、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策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本組合の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

策定

令和8年4月1日