北河内４市リサイクル施設組合情報セキュリティ基本方針

１　目的

この基本方針（以下「方針」という。）は、本組合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、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

この方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

⑴　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。

⑵　電磁的記録媒体

ハードディスク、ＵＳＢメモリ、ＣＤ－ＲＯＭ、磁気テープ等、情報システムで電子データを記録するための媒体をいう。

⑶　情報システム

コンピュータ、ネットワーク、電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。

⑷　情報資産

情報システム及びネットワークにより処理、保管、通信又は送付されるすべての行政情報（電子データ、紙等の有体物に出力された情報を含む。以下同じ。）をいう。

⑸　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。

⑹　情報セキュリティポリシー

本方針及び本方針に基づき定める基準等をいう。

⑺　機密性

情報資産にアクセスすることを許可された者だけが、情報資産にアクセスできる状態を確保することをいう。

⑻　完全性

情報資産が破壊、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。

⑼　可用性

情報資産にアクセスすることを許可された者が、必要なときに中断されることなく、情報資産にアクセスできる状態を確保することをいう。

⑽　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

⑾　情報セキュリティインシデント

障害、事故及びシステムの欠陥等で情報セキュリティが脅かされる状態及び事象をいう。

⑿　管理区域

ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋をいう。

⒀　クラウドサービス

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスをいう。

３　対象とする脅威

情報資産に対する脅威として、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施する。

⑴　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

⑵　情報資産の無断及び目的以外の用途及び場所への持ち出し、無許可ソフトウェアの使用等の規定違反、紛失・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、データの残存等の非意図的要因による情報資産の漏えい・破壊・消去等

⑶　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

⑷　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

⑸　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

4　適用範囲

この方針の適用範囲は、次の各号に掲げるところとする。

⑴　組織の範囲

事務局

⑵　情報資産の範囲

この方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（印刷した文書も含む。）

ウ　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

5　職員等の遵守義務

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。

6　情報セキュリティ対策

上記「3　対象とする脅威」の脅威から情報資産を保護するために、情報セキュリティ対策として、次の各号に掲げる対策を講じる。

⑴　組織体制

本組合の情報資産について、別に定めるところにより情報セキュリティ対策を推進する組織体制を確立する。

⑵　情報資産の分類及び管理

本組合の保有する情報資産について、別に定めるところにより機密性、完全性及び可用性に応じて分類を行い、その重要性に応じ、情報セキュリティ対策を実施する。

⑶　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

⑷　物理的セキュリティ対策

サーバ、パソコン、通信回線及びそれらを設置している施設等への不正な立入り、情報資産の損傷、妨害等から保護するため、別に定める物理的な対策を講じる。

⑸　人的セキュリティ対策

情報セキュリティに関する権限及び責任並びに記録媒体又は外部記録媒体の適切な取扱方法その他の遵守事項を定め、職員に情報セキュリティポリシーを周知徹底するための教育及び訓練を実施する等の別に定める人的な対策を講じる。

⑹　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保護するため、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別に定める技術的対策を講じる。

⑺　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等別に定める対策を講じる。

⑻　緊急時におけるセキュリティ対策

緊急事態が発生した場合に、迅速かつ適切な対応を可能とするための緊急時連絡体制の整備等別に定める対策を講じる。

⑼　業務委託及びクラウドサービスの利用

ア　業務委託する場合には、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。

イ　クラウドサービスを利用する場合には、利用に係る規定を整備し、対策を講じる。

ウ　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

7　情報セキュリティ監査及び自己点検の実施

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し、必要に応じて運用改善を行い、情報セキュリティの向上を図る。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策の整備

上記「6 情報セキュリティ対策」、「7 情報セキュリティ監査及び自己点検の実施」、「8 情報セキュリティポリシーの見直し」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別に定める。なお、公にすることにより、本組合の行政運営に支障を及ぼすおそれがあることから非公開とする。

10　委任

この方針の施行について必要な事項は、事務局長が定める。

附　則

この方針は、令和８年４月１日から施行する。