豊中市伊丹市クリーンランド
情報セキュリティ基本方針

（平成２０年９月１日　策 定）
（平成２６年３月１日　改 定）
（平成２７年４月１日　改 定）
（令和　６年２月１日　改 定）

1　目的

本基本方針は、情報セキュリティに関する基本的な事項について定めることにより、豊中市伊丹市クリーンランド（以下「クリーンランド」という。）の保有する情報資産を適正かつ円滑に管理し、及び運用することに関し必要な事項を定めることを目的とする。

2　定義

（1）情報資産

職員が業務上用いる情報及び当該情報を利用するための機器等をいう。

（2）機密性

情報資産の利用を許可された者に限り，当該情報資産を利用できる状態を確保することをいう。

（3）完全性

情報資産が破壊され，改ざんされ，又は滅失されていない状態を確保することをいう。

（4）可用性

情報資産の利用を許可された者が，必要なときに中断されることなく，情報資産を利用できる状態を確保することをいう。

（5）情報セキュリティ

情報資産の機密性，完全性及び可用性の維持をいう。

（6）ネットワーク

電子計算機を相互に接続するための通信網及びその接続機器をいう。

（7）電磁的記録媒体

職員が業務上用いる情報が記録された磁気テープ，磁気ディスク，光ディスク，光磁気ディスク，フラッシュメモリその他これらに類するものをいう。

（8）情報システム

電子計算機，ネットワーク及び電磁的記録媒体で構成されるものであって，これらの全部又は一部で情報処理を行う仕組みをいう。

3　職員の遵守義務

職員は，情報セキュリティの重要性を認識し，業務の遂行に当たっては，情報セキュリティポリシー（この基本方針及び９に規定する対策基準をいう。以下同じ。）を遵守しなければならない。

4　組織体制

（1）豊中市伊丹市クリーンランド管理者（以下「管理者」という。）は，情報資産について，情報セキュリティ対策(情報セキュリティに関する対策をいう。以下同じ。)を推進するため，情報セキュリティ統括責任者を置くほか，クリーンランド全体の組織体制を設けるものとする。

（2）情報セキュリティ統括責任者は，事務局長をもって充て，情報セキュリティ対策を統括するものとする。

（３）管理者は，情報セキュリティ対策に関する重要事項の調査審議等を行うため，情報セキュリティ統括責任者を議長とするセキュリティ会議を設置するものとする。

５　情報資産の分類及び管理

管理者は，情報資産を情報セキュリティの観点から重要度に応じて分類するとともに，当該分類に応じて管理するものとする。

６　情報セキュリティ対策

管理者は，情報資産に対する脅威の発生を想定し，及び防止するため，次に掲げる情報セキュリティ対策を行うものとする。

（１）重要な情報資産を保管する区域の入退室管理，電子計算機の適正な設置その他の物理的な対策

（２）職員に対する教育及び啓発の実施，緊急時の連絡体制の構築その他の人的な対策

（３）不正アクセスの防止，情報システムの開発及び保守に係る適正な管理その他の技術的な対策

７　情報セキュリティ監査及び自己点検の実施

管理者は，情報セキュリティポリシーの遵守状況を検証するため，情報セキュリティ監査(情報セキュリティに関する監査をいう。以下同じ。)及び自己点検を実施するものとする。

８　情報セキュリティポリシーの見直し

管理者は，情報セキュリティ監査及び自己点検の結果又は情報セキュリティに関する状況の変化に応じ，情報セキュリティポリシーを見直すものとする。

９　情報セキュリティに関する対策基準の策定

管理者は，情報セキュリティに関する具体的な遵守事項等を定めた対策基準を策定するものとする。

１０　情報セキュリティに関する実施手順の策定

管理者は，９の対策基準に基づき，情報セキュリティに関する実施手順を策定するものとする。

１１　その他

この基本方針に定めるもののほか，情報セキュリティに関して必要な事項は，別に定める。