

## 情報セキュリティポリシー

### (目的)

第1条 このポリシーは一般財団法人札幌市職員福利厚生会（以下「本会」という。）における情報システムに関わり取得、利用、管理、保存されるすべての情報の取扱いに関し、本会の役員及び事務局職員（準職員及び臨時職員を含み、以下「職員等」という。）の責務及び情報を保護するための対策等の基本方針を定め、本会が保有する情報の適正な管理を図るとともに、本会会員が安心して本会の各制度やサービスを利用できるようにすることを目的とする。

### (用語の定義)

第2条 このポリシーで用いる用語の定義は、次の各号のとおりとする。

(1) 情報システム

電子計算機、ネットワーク、記憶媒体等により、処理を行う仕組みをいう。

(2) ネットワーク

電子計算機等を相互に接続するための通信回線及びその構成機器（ハードウェア及びソフトウェア）をいう。

(3) 情報資産

情報システムで取り扱うすべての電磁的データをいう。

(4) 情報セキュリティ

情報資産の機密の保持、正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(5) 情報セキュリティに対する脅威

情報セキュリティに対する脅威とは、情報セキュリティを脅かす好ましからぬ事態及び事故をいう。

### (ポリシーの位置付け)

第3条 このポリシーは、本会の情報セキュリティ管理の最上位の位置付けとする。

### (職員等の責務)

第4条 このポリシーは、職員等に適用し、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、業務の遂行に当たってこのポリシーを遵守する義務を負うものとする。

### (情報セキュリティの組織及び体制)

第5条 本会の情報セキュリティに関するすべての責任及び最終決定権限を有し、情報セキュリティに関する事項を総括し、指示・指導を行うために最高情報セキュリティ責任者を置き、理事長をもって充てる。

2 理事長は、情報セキュリティ対策を推進し、管理するための組織・体制を確立し、その役割、責任等を定めるものとする。

3 理事長は、情報資産を取り扱う委託事業者等に対しても、契約を通じて、又は別途取り決めを行うことにより、このポリシーを遵守させるための措置を講じなければならない。

(情報資産の分類)

第6条 理事長は、情報資産をその内容に応じて分類し、その重要性に応じた情報セキュリティ対策を行うものとする。

(情報セキュリティに対する脅威)

第7条 特に認識すべき情報セキュリティに対する脅威は、次のとおりである。

(1) 意図的（計画的）な人為的脅威

故意の不正アクセス又は不正操作による機器又は情報資産の破壊、盗難、改ざん、消去等。

(2) 偶発的な人為的脅威

誤操作等によって起きる情報資産の破壊、漏えい、消去等及び搬送中の事故等による情報資産の盗難、漏えい等。

(3) 環境的脅威

地震、落雷、火災、水害、停電等の災害又は事故による情報資産の破壊、消失、サービス又は業務の停止等。

(情報セキュリティ対策)

第8条 理事長は、情報セキュリティに対する脅威から本会の情報資産を保護するため、次の対策を講ずるものとする。

(1) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、十分な教育及び啓発を図るとともに、情報資産を取り扱う者の守るべき行動基準及び判断基準を定める。

(2) 物理的セキュリティ対策

不正侵入又は盗難から情報資産を保護するために、管理区域の設置等情報資産への物理的なアクセスを制御するための対策を講ずる。

(3) 技術面及び運用面におけるセキュリティ対策

情報資産を外部又は内部からの不正アクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策及び委託等による情報システム開発・運用保守の基準、このポリシー遵守状況の確認等の運用面の対策を講ずる。

(4) 危機管理対策

緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

(情報セキュリティ対策基準の策定)

第9条 理事長は、このポリシーに定める情報セキュリティ対策を実施するための基準を別途策定するものとする。

(情報セキュリティに関する違反への対応)

第10条 このポリシー及び実施手順に違反した職員等は、その重大性、発生した事案の状況等に応じて懲戒処分の対象となることがある。

(ポリシーの改廃)

第11条 このポリシーの改正又は廃止は、理事会の議決により行う。

附 則

このポリシーは、平成26年4月1日から適用する。