茨城県看護教育財団情報セキュリティポリシー基本方針

1　目的

本基本方針は、公益財団法人茨城県看護教育財団（以下「財団」という。）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、財団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

コンピュータ、ネットワーク、情報システム及びこれらの仕様書、関連文書並びに職員が業務上知り得た個人情報等をいう。

(2)　コンピュータ

電子計算機及びパーソナルコンピュータ（以下「パソコン」という。）をいう。

(3)　ネットワーク

コンピュータを相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(4)　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(5)　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(6)　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。

(7)　機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

(8)　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。

(9)　可用性

情報資産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、情報資産にアクセスできる状態を確保することをいう。

３　対象とする脅威

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。

(1)　サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、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・消去、重要情報の詐取、内部不正等

(2)　情報資産の無断持ち出、無許可ソフトウェアの使用等の規定違反、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、外部委託管理の不備、マネジメントの欠陥、機器故障等非意図的要因による情報資産の漏えい・破壊・消去等

(3)　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

４　適用範囲

本基本方針が対象とする情報資産は、２定義(１)の情報資産の範囲内とする。

５　職員等の遵守義務

職員、非常勤職員及び臨時職員（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

財団の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2)　セキュリティ対策基準の構成

財団の保有する情報資産を機密性、完全性及び可用性に応じて構成し、当該構成に基づき情報セキュリティ対策を行う。

(3)　物理的セキュリティ

サーバ等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4)　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、十分な啓発を行うなどの人的な対策を講じる。

(5)　技術的セキュリティ

コンピュータ及びネットワークの管理、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。

7　情報セキュリティ自己点検の実施

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自己点検を実施する。

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基準の策定

上記６、７及び８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。

10　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財団の事業運営に重大な支障を及ぼすおそれがあることから非開示とする。