情報セキュリティに関するガイドライン

第１条（目的）

このガイドラインは，医療法人恵生会（以下，会）の社会的信頼を維持し，健全な運営を継続するために定める.

第２条（ガイドラインの対象）

このガイドラインは，会が保有する情報を対象とする.

第３条（用語の定義）

このガイドラインにおいて，次の各号に掲げる用語の意義は，当該各号に定めるところによる.

1　情報システム

コンピュータ，情報ネットワーク及び記録媒体等で構成され，業務に必要な情報の収集・蓄積・処理・伝達・利用を行う仕組みをいう.

2　情報セキュリティ

情報の機密性・完全性・可用性を維持すること.

3　情報セキュリティ対策に関わる責任者

統括的責任と権限を有する者をいい，理事長もしくは理事長が任命した者が担当する.

4　情報セキュリティ対策に関わる担当者

各所属長が情報セキュリティ対策に関わる責任者の指示のもと，この任にあたる者とする.

5　従業者

医療資格者のみならず，会の指揮命令を受けて業務に従事する者すべてをいう．また，雇用関係のある者のみならず，理事，派遣労働者等も含む.

6　会の情報セキュリティ監査機関

会から選任され、理事長の諮問としながらも公平かつ客観的な立場にあり、監査の実施及び報告を行う権限を有する機関であり、情報委員会が担当する.

7　物理的セキュリティ

重要な情報を保管したり扱ったりする場所の入退管理や施錠管理及び使用するコンピュータや周辺機器に対するセキュリティ.

第４条（従業者の義務）

1　従業者は，採用時より機密保持義務も含む守秘義務に関する契約書や誓約書を交わし，退職後も遵守しなければならない.

2　従業者は，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に関するガイドラインを遵守しなければならない.

第５条（情報セキュリティに対する組織的取り組み）

平常時から，事故が起こったことを想定し対策を検討しておく.

1　情報システムに関するセキュリティ対策

(１)インターネットにより外部から内部にアクセスされないよう，また内部のデータが外部に漏れないよう手段を講じる．外部へも不要なアクセスはしない.

(２)私用コンピュータ等への情報の移植は基本的には行わない．必要により行った場合はできるだけ早く消去する.

(３)重要情報は原則として会の外に持ち出さないようにする．必要が生じた時は書面（情発-1）により管理者もしくは所属長の許可を得る.

(４)第三者に不用意に使用されないよう，コンピュータ等にはパスワードを設定する．また共通で重要な情報にはアクセスを制限するため，使用者ごとの ID を設定する.

(５)業務に必要なソフトのダウンロードは所属長の許可を得る.

2　物理的セキュリティ対策

(１)重要な情報を保管したり扱ったりする場所の入退室管理と施錠管理を行う.

(２)コンピュータや配線は地震等の自然災害や，ケーブルの引っ掛け等の人的災害が起こらないように配置，設置する.

(３)部署ごとに重要な情報を区分し，データやシステムの保全のためバックアップデータなど複製をあらかじめ作成し，たとえ問題が起きてもデータを復旧できるよう備えておく.

(４)重要な情報は整理整頓し盗難防止に努める．不要になった情報は速やかに消去ソフトや溶解処理，シュレッダなどで確実に消去する.

第６条（情報セキュリティ事故後の対応及び対策）

1　事故後の手順

(１)情報セキュリティに関する事件や事故等が発生したら速やかに上司に報告し，以降の指示を受ける．会が平常の勤務体制であれば所属長に報告し，休日体制であれば看護当直に報告する．またその経過を時間とともに記録する.

(２)最終報告を受けた情報セキュリティ対策に関わる責任者が速やかに対応方針を決定する．対応方針には，被害状況の把握，被害の拡大防止と復旧のための措置，関係者への報告・謝罪，ホームページへの公開等，あらゆることを検討する.

2　再発防止対策

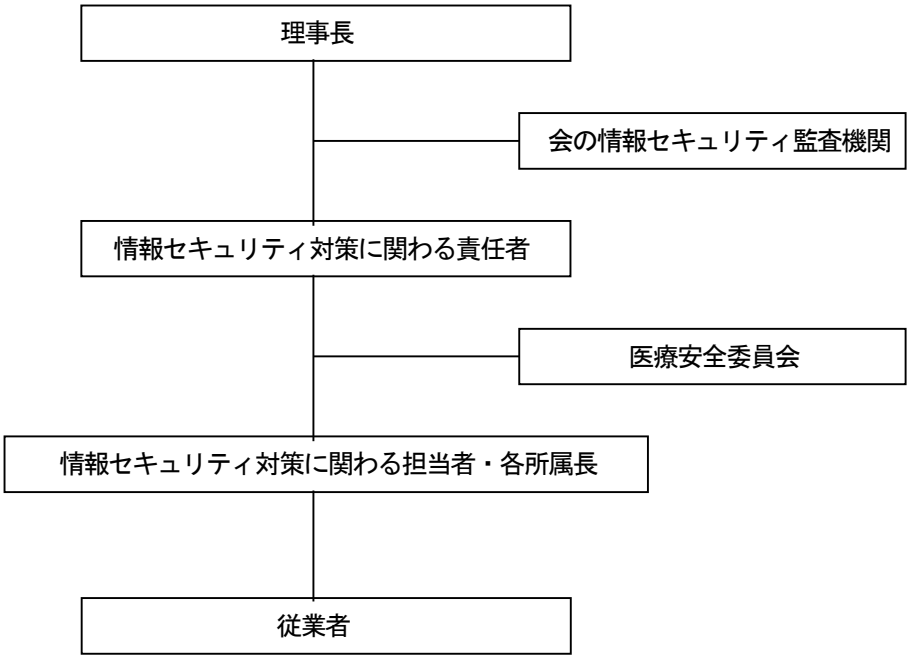
事故の分析と対策として，優先順序を決めて，原因の究明，脆弱システムの改善を可及的速やかに行う.

第７条（会の情報セキュリティに関するガイドラインの見直し）

会の情報セキュリティに関するガイドラインは，情報システムの変更，新たな脅威など情報セキュリティを取り巻く状況の変化に対応し，情報セキュリティ対策に関わる責任者の指示により検証し見直す.

第８条（管理組織・体制）

会の情報セキュリティに関する組織体制を以下に図示する



第９条（罰則）

理事長は本ガイドラインに違反した職員等に対し，就業規程に基づいた懲戒を行うことがある.