

情報システムに関するセキュリティ基本方針

令和4年4月1日

1. 目的

別府市医師会立別府青山看護学校(以下「本校」という。)の情報システムが取り扱う情報には、別府市医師会職員及び学生の個人情報や運営上重要な情報が多数含まれている。これらの情報資産を人的脅威や災害、事故等様々な脅威から防御することは、プライバシーの保護、質の高い教育研究活動及び看護学校の運営を確保するために必要不可欠である。

このため、本校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ことを目的として、情報セキュリティ基本方針を定める。

2. 適用者

情報資産を取り扱う医師会職員、学生その他本校の許可を受け情報資産を取り扱う者(以下総称して「利用者」という。)

3. 用語の定義

(1) 情報資産

情報及び情報システムをいう。

(2) 情報システム

ネットワーク、ハードウェア、ソフトウェアおよび記録媒体で構成され、処理を行う仕組みをいう。

(3) 情報

別府市医師会、本校が管理する情報をいう。

(4) 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及びその構成機器をいう。

(5) 情報セキュリティ

情報資産の機密性、完全性および可用性を維持することをいう。

(6) 機密性

情報にアクセスすることが認められたものだけがアクセスできることを確実にすることをいう。

(7) 完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

(8) 可用性

情報にアクセスできることを認められた者だけが、必要な時に中断されることなく、情報にアクセスできる状態を確保することをいう。

4. 利用者の責務

利用者は、情報セキュリティの重要性を常に意識して行動するとともに、情報セキュリティ実施手順を遵守しなければならない。

5. 情報資産の分類及び管理

情報の機密性、完全性および可用性を踏まえた情報資産の分類を行い、その重要性に応じて適切な管理を行うものとする。

6. 情報セキュリティ管理体制

基本方針に基づき情報セキュリティの確保・維持を担保するため、最高情報統括責任者、情報セキュリティ責任者及び管理者を置く。

- 一 最高情報統括責任者(副学校長)
- 二 情報セキュリティ責任者(教務主任)
- 三 情報セキュリティ管理者(司書)

7. 情報セキュリティ対策

本校は情報資産を、故意(盗聴、不正アクセス、改ざん、破壊、窃盗等)、過失(入力ミス、操作ミスなど)、災害(火災、地震など)、故障などによる損傷などの脅威から守るため、次の情報セキュリティ対策を講ずる。

(1) 人的セキュリティ

情報セキュリティに関する権限や責任及び遵守すべき事項を定め、利用者に対する周知及び徹底を図るとともに、十分な教育及び啓発を行うために必要な対策

(2) 物理的セキュリティ対策

情報システムの場所及び情報の保管場所などへの不正な立ち入りならびに情報資産への加害及び利用者の妨害などから保護するための物理的な対策

(3) 技術的セキュリティ対策

情報資産を不正アクセスなどから保護するため、情報資産へのアクセス防御、ネットワーク管理等の技術的対策

(4) 運用などにおける対策

情報システムの監視および情報セキュリティ対策の遵守状況の確認などの運用面の対策

(5) 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が可能となるような危機管理対策

8. 情報セキュリティに関する違反への対応

本校は、基本方針、対策基準および実施手順に違反したものについては、その重大性、発生した事案の状況などに応じて懲戒処分の対象とする。

9. 情報セキュリティ監査の実施

本校は、基本方針、対策基準及び実施手順が遵守されていることを検証するため、必要に応じて自己点検、情報セキュリティ監査を実施するものとする。

10. 評価および見直し

本校は、情報セキュリティ監査の結果等にもとづき、基本方針、対策基準、実施手順に定める事項および情報セキュリティ対策についての評価を、倫理委員会をとおして定期的の実施するとともに、情報セキュリティを取り巻く状況の変化などに対応して、基本方針、対策基準、実施手順及び情報セキュリティ対策の見直しを実施するものとする。

- (1) 情報セキュリティに関する倫理委員会は、年に2回開催する(定期)。
- (2) 情報セキュリティ対策についての評価は、別に定める基準をもとに実施する。