

情報セキュリティ基本方針

当社は、医療機器の販売・修理等の事業により、医療機関等のお客様を通して地域医療の発展に貢献すべく事業活動を遂行しております。事業活動において利用する情報資産の適正な運用・管理について、お客様の信頼に応えることを目的に、情報セキュリティ基本方針を以下に定めます。

1. 対象範囲

情報セキュリティ基本方針が対象とする対象者及び対象物は以下のとおりである。

(1) 対象者

当社の業務に従事している役員、社員（正社員、契約社員、パート社員、アルバイト社員、派遣社員等）を対象とする。（以下「社員等」という。）

(2) 対象物

当社が保有する全ての情報資産である。

- ①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ②ネットワーク及び情報システムで取り扱う情報（情報を印刷した文書を含む。）。

2. 社員等の遵守義務

社員等は、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本基本方針及び対策基準等を遵守するものとする。

3. 組織・体制

当社は、情報セキュリティ対策を推進するため、情報セキュリティ責任者等を定め、全社的な組織体制を確立する。

4. 情報資産の分類と管理

当社は、情報資産を個々の情報の機密性、完全性及び可用性を踏まえ、その重要性に応じて分類し、情報資産の管理責任及び利用責任について明確にする。

また、情報資産の重要性に応じたセキュリティ管理対策を行う。

5. 情報セキュリティ対策

当社の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。これらの対策は、対策基準等に定め運用に当たる。

(1) 物理的セキュリティ対策

情報資産を損傷・妨害及び盗難等から保護するための物理的な対策及び情報システムの電源及び配線等の防護のための必要な措置を行う。

(2) 人的セキュリティ対策

組織・体制で定める責任者や担当者及び利用者としての役割及び責任を明確にし、

全ての対象者に対して、情報セキュリティの内容を周知徹底させるために必要な対策を行う。

(3) 技術的セキュリティ対策

情報システム及びネットワークについて、セキュリティ機器やセキュリティソフトの導入、各種設定による情報セキュリティ対策を行うとともに、新たな脅威の出現に対応するために、セキュリティパッチの適用や、機器の更新等の対応を行う。

また、情報資産の重要性に応じたアクセス制御に関する情報セキュリティ対策、ログの保管や定期的な情報のバックアップにより、情報セキュリティ対策を行う。

(4) 運用対策

情報セキュリティに関する事案の検知や情報セキュリティ対策の遵守状況を確認するために、情報システムの監視を行うなど、運用面での対策及び手順を定め実施する。

また、情報資産への侵害あるいは外部の情報資産に対する侵害が発生した際の対応手順を定める。

6. 情報セキュリティ監査及び評価・見直しの実施

(1) 監査

当社は、各部門が情報セキュリティ対策基準等に定めた運用を実施しているかを検証するために、計画的に監査を実施する。

(2) 評価及び見直し

当社は、情報セキュリティ監査の結果について評価を実施する。

また、情報セキュリティを取り巻く状況の変化に鑑み、情報セキュリティ対策基準等に定める事項の見直しを実施する。

7. 教育・研修

当社は、情報資産を利用する者に対し、必要な情報セキュリティに関する教育・研修を実施する。

8. 法令遵守の義務

当社は、情報資産を利用するにあたり、情報セキュリティ関連法令等を遵守する。

制定 令和5年4月1日

クロスウィルメディカル株式会社

代表取締役社長 阿部 篤仁