情報セキュリティポリシー

保健医療・福祉施設あしかがの森（以下「当施設」といいます。）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、当施設が実施する情報セキュリティについて基本的な事項を定めています。

１．定義

① 情報資産とは、当施設にとって価値を持つ情報及びその情報を利用可能とする手段（ハードウェア、ソフトウェア、サービス等）をいいます。

② ネットワークとは、コンピュータ等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）をいいます。

③ 情報システムとは、コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みのことであり、当施設の所有であるかを問わず、当施設の業務に使用するものすべてをいいます。

④ 情報セキュリティとは、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います。

⑤ 情報セキュリティポリシー（以下「本ポリシー」という。）とは、情報セキュリティ基本方針及び情報セキュリティ対策基準をいいます。

⑥ 機密性とは、情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいいます。

⑦ 完全性とは、情報が破壊、改ざん又は消去されていない状態を確保することをいいます。

⑧ 可用性とは、情報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、情報にアクセ スできる状態を確保することをいいます。

⑨ 職員とは、当施設の職員（常勤、非常勤を問わない。）をいいます。

２．脅威

情報資産に対する脅威には、次の各号として対策を実施するものとします。

一 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入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

二 情報資産の無断持ち出し、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、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

三 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

四　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
五　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

3. 遵守事項

① 職員は、情報セキュリティの重要性を十分に理解し、業務の遂行に当たって情報セキュリティポリシーを遵守します。
② 当施設の情報資産を使用し業務を行っている取引先及び業務委託先並びにその従業員が本ポリシーを遵守することとなるように、契約の際十分に留意します。

4. 情報セキュリティ基本方針

① 脅威から情報資産を保護するための対策や監査など情報セキュリティに関する重要な事項は、情報資産の機密性、完全性及び可用性に応じて、幹部会議で審議決定するものとします。
② 職員が本ポリシーを遵守するように、職員に対する教育及び啓発を行う等の人的なセキュリティ対策を講じます。
③ 情報資産の機密性、完全性及び可用性を確保する対策を講じます。
④ サーバ、情報システム室、通信回線及びパソコン等のハードウェアの管理について、可能な範囲で物理的セキュリティ対策を講じます。
⑤ コンピュータ等の管理、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セキュリティ対策を講じます。
⑥ 外部委託を行う際のセキュリティ確保等、本運用面の対策を講じます。
⑦ 情報資産に対するセキュリティ侵害（そのおそれのある場合を含む。以下、同じ。）が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定します。

5. 監査と見直し

情報セキュリティの自己点検及び監査を実施し、運用改善を図り、必要に応じて本ポリシーの見直しを行います。

6. 情報セキュリティ対策基準

① 情報セキュリティを統括する最高責任者である情報セキュリティ統括責任者は、所長とします。
② 情報セキュリティ統括責任者は、情報セキュリティに関する障害・事故及びシステム上の　欠陥（以下、「情報セキュリティインシデント」 という。）に対処するため関係者と協議の上対応を指示するとともに、当施設最高議決機関である幹部会議に報告します。
③ 情報セキュリティ統括責任者を補佐する情報セキュリティ副統括責任者は、院長とします。
④ 各部署内で取扱われる情報資産を保護するための責任者である情報セキュリティ管理者は、総務部長、診療部長、看護部長、センター長とし、各部署における次の各号

の業務を担います。

一　情報セキュリティ対策の運用及び管理等

二　本ポリシーの遵守に関する職員の教育、訓練、助言及び指示

三　情報セキュリティインシデント発生時の情報収集、管理及び対応

⑤　情報システムネットワーク管理者は、経理課長とし、情報システムネットワークの情報セキュリティを保護します。

⑥　情報セキュリティ事務局は、経理課とします。

⑦　情報セキュリティの監査は、庶務課で行います。

7. 情報資産の分類

情報資産を、機密性、完全性及び可用性により、次のとおり分類し、取扱いを定めます。

	種別	分類	取扱制限
機密性	Ⅰ種	・個人情報 ・事業上の秘密情報	・当施設の端末以外での作業の禁止 ・当施設の端末への PW 設定 ・電磁的記録媒体の施錠可能な場所での保管
	Ⅱ種	上記Ⅰ種以外	・所定の場所に保管
完全性	Ⅰ種	・個人情報 ・改竄又は破損により、患者等の権利が侵害される、又は業務遂行に支障を及ぼすおそれがあるもの	・情報資産のバックアップ ・当施設の端末への PW 設定 ・電磁的記録媒体の施錠可能な場所での保管
	Ⅱ種	上記Ⅰ種以外	・所定の場所に保管
可用性	Ⅰ種	・滅失又は紛失により、患者等の権利が侵害される、又は業務遂行に支障を及ぼすおそれがあるもの	・情報資産のバックアップ ・電磁的記録媒体の施錠可能な場所での保管
	Ⅱ種	上記Ⅰ種以外	・所定の場所に保管

8. 情報資産の管理

情報は、当施設の端末又は共有ファイルに保存します。必要あるときは、法令及び当施設の所定の手続きを経て、外部記録媒体に情報を保存することもあります。

9. 情報資産の取得

情報セキュリティに支障が生じる可能性のある情報資産を取得するときは、あらかじめ情報セキュリティ統括責任者と協議します。

10. 目的外使用の禁止

業務以外の目的に情報資産を利用しません。

11. 情報資産の送信・提供

電子メール等により情報資産を送信・提供するときは、必要に応じて暗号化、パスワード設定、契約の締結等を行います。

12. 情報資産の廃棄

情報を記録している電磁的記録媒体を廃棄するときは、情報を復元できないように処理して廃棄します。

13. 人的セキュリティ対策

全職員を対象とした情報セキュリティ研修を年1回実施し、本ポリシーの徹底を図ります。

14. 物理的セキュリティ対策

① サーバ等の機器を設置する場合、災害の影響を最小限となる場所とし、容易に取り外せないよう固定する等、必要な措置を講じます。

② サーバ等の機器の電源について、停電等 による電源供給の停止に備え、自家発電設備を備えています。

③ サーバ室には施錠管理を行い、許可されていない立入りを防止しています。

15. 技術的セキュリティ対策

複雑化・巧妙化しているサイバー攻撃の脅威により、当施設の業務に重大な影響をあたえるリスクが想定されるため、機密性、可用性、完全性の確保に十分配慮し攻撃に強い情報システムにしています。

16. セキュリティ侵害

セキュリティ侵害の発生の報告を受けた情報セキュリティ管理者は、ただちに情報セキュリティ統括管理者と法人本部に報告し、公表するとともに、法人本部の指示のもとセキュリティ侵害に対処します。