学校法人　聖心女子学院
情報セキュリティポリシー（基本方針及び対策基準）

趣旨

高度情報化社会において、学校法人聖心女子学院（以下「本法人」という。）が建学の精神を継承・発展させ、教育・研究機関としての社会的責任を果たすためには、情報基盤の整備に加え情報資産を重要な資産として保護・管理することが必要である。このため、本法人は、情報を扱う際の情報セキュリティの確保を図り、情報資産に対する適切な安全対策を実施するために情報セキュリティポリシー（以下「ポリシー」という。）を定め、ポリシーに基づき取り組みを展開していくこととする。

Ⅰ．総則

１．ポリシーの構成

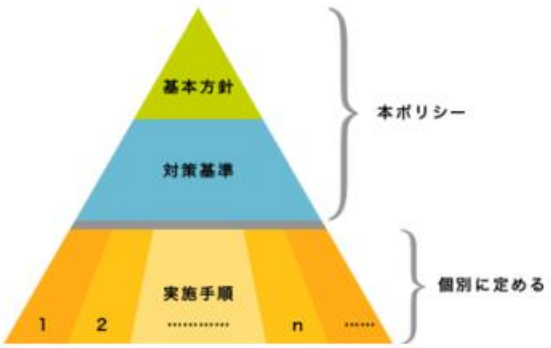
ポリシーは、以下の３つの階層により構成するものとし、学校法人聖心女子学院情報セキュリティポリシー（基本方針及び対策基準）（以下「本ポリシー」という。）では（１）及び（２）を定めるものとする。

（１）情報セキュリティポリシー基本方針（以下「基本方針」という。）
　本法人が情報セキュリティに取り組む上での基本となる方向性を定め、ポリシーの対象者にとっての基本的な考え方や役割と責任を明確にする。

（２）情報セキュリティポリシー対策基準（以下「対策基準」という。）
　基本方針に基づき、本法人が組織的に情報セキュリティ対策を行うための具体的な施策と達成すべき基準を定める。

（３）情報セキュリティ実施要領（以下「実施要領」という。）
　情報資産の重要度に応じて、情報セキュリティ対策を実施していくための具体的な手順を定める。本法人の設置する学校、法人本部、研究所、センター及び農園（以下「設置校等」という。）は、設置校等ごとの情報資産の管理に係る実施要領を定める。

（１）～（３）に示す階層構造を下図に示す。



２．適用範囲

ポリシーの適用範囲は、設置校等のすべての情報資産とそれに関わる情報システムとする（本法人の情報資産に一時的にアクセスするための情報システムを含む。）。

３．対象者と責務

ポリシーを遵守すべき対象者（以下「対象者」という。）は、以下の者とする。対象者は、加えて、関係諸規則諸規程、関係ガイドライン及び関係法令等を遵守しなければならない。

（１）本法人及び設置校等が雇用する教職員（専任・嘱託・非常勤を含む。）並びに役員等（理事・監事・評議員を含む。）

（２）契約に基づき本法人及び設置校等の業務に携わる者（業務委託者、派遣職員を含む。）

なお、設置校等が提供する情報サービスを利用する児童、生徒、学生、保護者、卒業生並びに講習会・イベントの受講者・参加者等については、情報セキュリティに関する規約を該当する設置校等が別に定める。

Ⅱ．基本方針

以下の７項目を基本方針とする。

（１）情報セキュリティの目的と目標を以下の通り定め、組織的に取り組む。

　１）情報資産の保護・管理

　２）本法人の情報セキュリティに対する侵害の阻止

　３）本法人内外の情報セキュリティを損ねる加害行為の抑止

　４）情報セキュリティの評価と改善

（２）ポリシーを遵守すべき対象者の役割と責任を明確にして取り組む。

（３）情報セキュリティのリスクを評価し、適切な対策を講じる。

（４）情報セキュリティに関する教育及び啓発を実施し、情報リテラシーをもって業務を遂行できるようにする。

Ⅲ．対策基準

１．組織体制

（１）情報セキュリティ最高責任者

情報セキュリティ最高責任者は理事長をもって充て、本法人における情報セキュリティに関する全ての責任を負うものとする。

（２）情報セキュリティ統括責任者

情報セキュリティ統括責任者は常務理事をもって充て、情報セキュリティ最高責任者の命を受

け、本法人の統括責任を負うものとする。
（3）情報セキュリティ管理責任者
情報セキュリティ管理責任者は設置校等の長をもって充て、設置校等の情報セキュリティに関する責任を負い、情報システムが安全かつ円滑に運用されるよう情報セキュリティの保持と強化を統括する。また、システム管理者を指名し、システム管理を実施する。
（4）情報セキュリティ委員会
情報セキュリティに関する重要な事項を審議する機関として、情報セキュリティ委員会（以下「委員会」という。）を設置し、必要に応じて委員会を開催するものとする。委員会については、別に定める。

2．情報資産の分類と管理

情報セキュリティ管理責任者は、（1）機密性　（2）完全性　（3）可用性による情報資産の分類を行い、重要度に応じた情報セキュリティ対策を講じて情報資産を管理する。

3．物理的セキュリティ

情報セキュリティ管理責任者は、情報資産の保管場所や情報システムの設置場所等について、物理的な侵害対策を講じる。

4．人的セキュリティ

情報セキュリティ管理責任者は、ポリシーに基づき、対象者が遵守すべき事項を定め、周知徹底を図る。情報セキュリティ管理責任者は教職員向けの研修や、児童、生徒及び学生向けのオリエンテーション等を実施する。

5．技術的セキュリティ

情報セキュリティ管理責任者は、情報システムの保守、導入等において、技術的な侵害対策を講じる。

6．情報セキュリティインシデント対応

情報セキュリティインシデントを発見した者は、速やかに情報セキュリティ管理責任者に届け出なければならない。
情報セキュリティ管理責任者は、届け出のあった情報セキュリティインシデントについて調査、対応、対策等を講じ、別に定める書式により、情報セキュリティ統括責任者に報告する。
情報セキュリティ統括責任者は、情報セキュリティ最高責任者に対し、適時、報告する。

7．評価と改善

情報セキュリティ最高責任者は、定期的に情報セキュリティの点検・評価を行い、情報セキュリティ委員会に報告するとともに、ポリシー等の見直しに活用する。

8．懲戒

ポリシーを順守すべき対象者が、故意又は過失によりポリシーに違反したときは、規則等に基づき措置されることがある。

Ⅳ．その他

本ポリシーに定めるもののほか、情報セキュリティに関し必要な事項は、別に定める。
また、本ポリシーの改廃等は、理事会において決定するものとし、本ポリシーの改廃等に関する事務は、本法人本部事務局が所管する。

附 則
本ポリシーは、2023 年 4 月 1 日から施行する。

付録　用語の定義

ポリシーにおいて使用する用語の定義は、以下のとおりとする。

（1）情報

本法人の教育・研究・管理運営に関わる者が作成し、又は収集及び取得した内容が記録された電磁的媒体、紙媒体及びそれに準ずる媒体をいう。

（2）情報資産

情報システムに記録された情報及び情報システムに関係がある書面に記載された情報であり、電磁的に記録された情報全てを含む。書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。

（3）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。

1）機密性とは、権限のある者にのみ情報資産が利用可能であることをいう。

2）完全性とは、情報資産が破壊、改ざん又は消去されていない状態をいう。

3）可用性とは、権限のある者が、必要なときは常に情報資産を利用できることをいう。

（4）情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって情報処理を行う仕組みをいう。本法人の情報システムは、本法人により所有又は管理されているもの及び本法人との契約あるいは他の協定に従って提供されるものをいい、本法人の情報ネットワークに接続される機器を含む。

（5）記録媒体

電磁的又は光学的に情報を記録した媒体あるいは情報をプリントアウトした紙媒体等をいう。

（6）情報セキュリティインシデント

不正アクセス、情報漏えい、データの改ざん、ウィルス感染等により、情報セキュリティに脅威が発生している又は発生するおそれがある事象をいう。