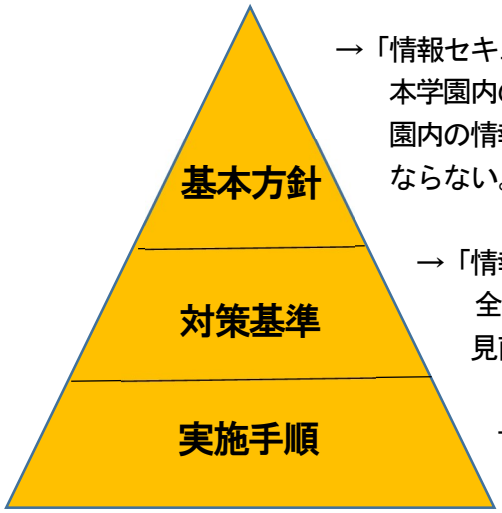
＜情報セキュリティポリシー全体の構成＞



→「情報セキュリティポリシー」の最上位に位置する文書。
本学園内の情報セキュリティの『憲法』に相当する文書で、本学園内の情報に関わる全員が、この方針に基づいて行動しなければならない。

→「情報セキュリティ基本方針」の下層に位置する文書。
全員が遵守すべき具体的事項（体制、運用、管理、評価、見直し等）をすべて記述する。

→「情報セキュリティ対策基準」の下層に位置する文書。
対策基準のうち「対象者ごと」や「機器ごと」といったその担当で必要なものにカスタマイズしたもの。

↑

関連法規（刑法、不正アクセス防止法、個人情報保護法、著作権法等）と照らして違反のないものとする。

第１章　情報セキュリティ基本方針

１　目的

本学園の情報システム等が取り扱う情報には、学生・保護者・教職員等の個人情報のみならず、試験・受験等の重要な情報など、外部に漏えい等した場合に重大な結果を招く情報も含まれている。

したがって、これらの情報及び情報を取り扱う情報システム等を様々な脅威から防御することは、学生・保護者・教職員のプライバシー、本学園の情報資産等を守るためにも、また、本学園業務の安定的な運営のためにも必要不可欠であり、対外的な信頼の維持向上に寄与するものである。

本基本方針は、本学園が所管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、本学園が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　「情報セキュリティポリシー」の適用範囲

「情報セキュリティポリシー」の適用範囲は、本学園の情報資産に関連する人的・物理的リソースを含むものとする。

３　「情報セキュリティポリシー」の適用者

「情報セキュリティポリシー」の適用者は、学校長以下、教職員、学生を含めた本学園の情報資産を利用するすべての者である。

①学校長の責務

学校長は、「情報セキュリティポリシー」への支持・支援を表明し、率先し情報セキュリティマネジメントを推進しなければならない。

②教職員の責務

教職員には本学園の情報資産の使用を認めるが、それは円滑な校務遂行の手段としての使用を認めることであり、私的利用を許可するものではない。本学園の情報資産を扱う上で、「情報セキュリティポリシー」に同意し、遵守しなければならない。また、これに違反した者は、その結果について責任を負わなければならない。

③学生に対する対応

授業または教育目的で、情報資産の使用を学生に認める場合、その行為に先立って遵守すべきセキュリティ事項を明記し、学生に伝えておかなければならない。

学生への指示及び管理は、教職員の権限の範囲とし、その責務を怠った場合は然るべき責任を負わなければならない。

４　「情報セキュリティポリシー」の公開範囲

情報セキュリティ基本方針　　→一般に公開する。
情報セキュリティ対策基準　　→教職員の限りとする。
情報セキュリティ実施手順　　→該当する業務を行う者の限りとする。

５　情報セキュリティ管理体制

本学園内の情報資産管理の方法に関して、環境変化に対応し継続的変化・改善を行い、かつリスク発生時の迅速な対応を行うための体制を確立する。

６　情報資産の分類

情報資産は管理の効果を高めるために、その機密性、完全性及び可用性により分類し、それぞれに応じた情報セキュリティ対策を行う。

７　情報資産リスク分析

本学園内の情報資産に関して、特に認識すべきリスクは以下の 10 種類である。

①外部からの、故意の不正アクセスによる情報資産の盗聴、持ち出し、改ざん、消去、損壊
②内部からの、故意または意図しない操作等での不正アクセスによる、情報資産の盗聴、持ち出し、改ざん、消去、損壊
③ウィルスによるデータ、システムの破壊。あるいはウィルスの送信者（加害者）となること
④他の組織への、不正アクセスの踏み台となること
⑤地震、火災、落雷などによるシステムの故障および停止
⑥機器、媒体そのものの盗難

上記以外に特に学生に関するリスクとしては以下の通りである。

⑦学生の個人情報流出
⑧学生の著作物への著作権侵害
⑨外部の有害情報に学生が触れること
⑩学生による、ネットワーク上における故意または無意識での誹謗中傷行為

８　情報セキュリティ対策

情報資産の保護をより確実にするために、以下の情報セキュリティ対策を講じる。

①物理的対策

情報システムを設置する施設など、情報資産を保護するために物理的な対策を講じる。

②人的対策

情報セキュリティに関する権限や責任を明確にし、全教職員にセキュリティポリシーの内容を周知させるための教育や啓蒙などの対策を講じる。

③技術的対策

情報資産を保護するために、アクセス制御、ネットワーク管理など、主に技術的な面での対策を講じる。また、緊急事態が発生した場合の対応策など、機器管理対策を講じる。

④運用における対策

情報システム監視、情報セキュリティポリシーの厳守状況の確認、委託を行う際の情報セキュリティ確保等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とする危機管理の対策を講じる。

９　情報セキュリティ対策基準の策定

本学園内の情報資産を保護するために遵守すべき行為や判断基準の統一化などに関して、基本的な要件を明記した情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して、情報セキュリティ対策を実施するために、個々の情報資産に関して、個別の実施手順を策定する。

11　情報セキュリティ監査の実施

情報セキュリティポリシーが遵守されていることを検証するために、定期的に監査を実施する。

12　評価および見直しの実施

情報セキュリティ監査の実施結果および世の中の環境変化への対応や、本学園内での改善活動の結果を反映させるために、情報セキュリティポリシーに定める事項の見直しを実行する。