情報セキュリティ基本規程

学校法人　順正学園

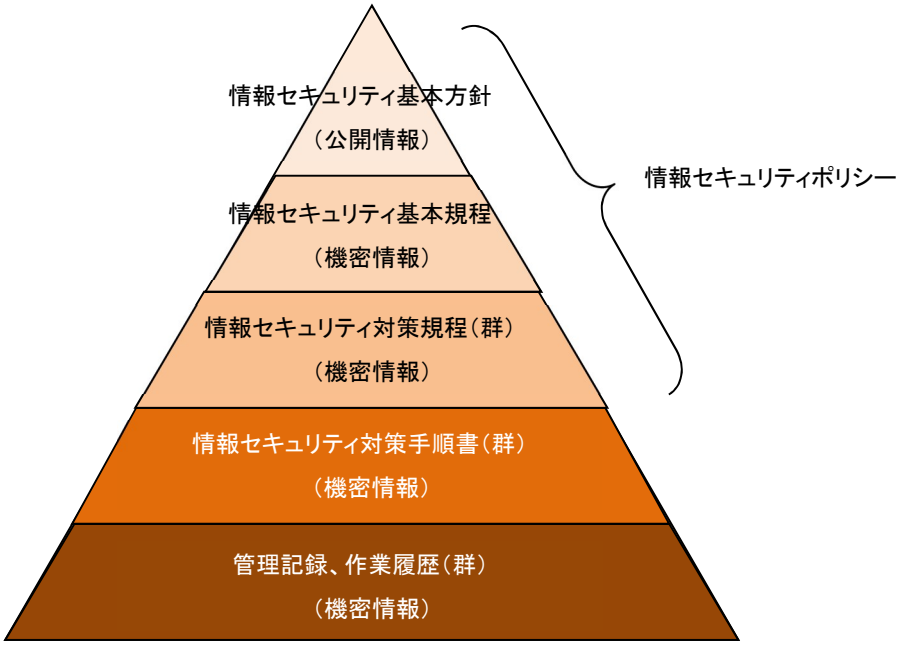
第１章　総則

（目的）

第１条　本規程は、学校法人　順正学園（以下「本学園」という。）における情報資産の運用及び管理について必要な事項を定め、本学園の保有する情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

（情報セキュリティポリシーの定義）

第２条　『情報セキュリティポリシー』は、以下の「情報セキュリティ基本方針」を含む３つの階層に分けて策定・管理される文書とする。「情報セキュリティ基本方針」は、本学園の情報セキュリティに対する基本的な考え方を表した文章である。



（情報セキュリティ基本規程）

第３条　情報セキュリティ基本規程（以下、「基本規程」とする）は、本学園のセキュリティマネジメントにおける基本的な方針を記述したものである。この文書に基づいて下層の文書を策定する。

（情報セキュリティ対策規程）

第４条　情報セキュリティ対策規程（以下、「対策規程」とする）は、基本規程の下層に位置する文書である。この文書は、基本規程での宣言を受け、項目ごとに遵守すべき事項を網羅的に記述する。

（情報セキュリティ対策手順書）

第５条　情報セキュリティ対策手順書（以下、「対策手順書」とする）は、対策規程の下層に位置する文書である。この文書は、対策規程で記述された文書をより具体的に、配布するべき対象者

ごとに内容をカスタマイズして記述する。対策手順書の確実な運用もしくは監査を行うため、管理記録や作業履歴を作成し、保管する。

（文書の開示）
第６条　情報セキュリティ基本方針は、一般に公開する。
２　基本規程は、必要な部分のみを一般に公開する。全文については、教職員すべてに公開とし、一般には公表しない機密情報として取り扱わなければならない。
３　対策規程は、情報セキュリティ委員会メンバーと担当部署の者に公開とする。
４　対策手順書は、該当する職務を行う者に公開とする。
５　公開しなければ職務を遂行できない場合には、機密保持契約の締結等により、公開を認める場合がある。

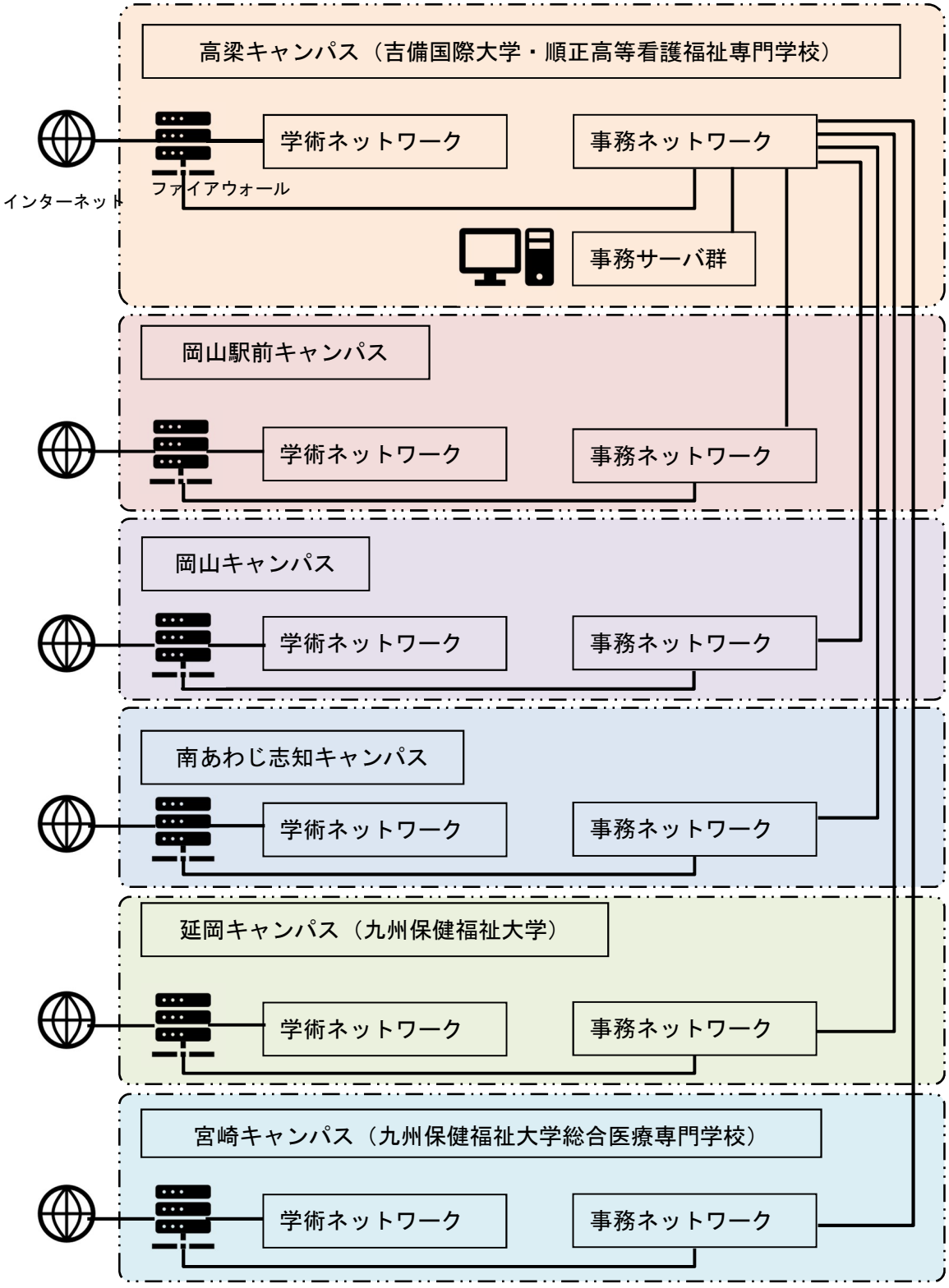
（既存の規程との関連）
第７条　基本規程は、本学園の他の規程（人事規程、就業規則等）と同等の位置づけの文書とする。よって、この文書の改廃は所定の規程に準じて行うものとする。
２　『情報セキュリティポリシー』は、情報資産に関連する本学園の他の規程等と照らして、相互に矛盾が生じないようにしなければならない。

（その他関連法規）
第８条　『情報セキュリティポリシー』は、関連法規と照らして違反することの無いようにしなければならない。また、必要に応じて関連規格に遵守した管理策を導入しなければならない。
関連法規・関連規格としては、例として以下のものが挙げられる。
国際規格
・ISO/IEC 27000 シリーズ
国内規格
・JIS Q 15001
国内法規
・刑法
・不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）
・建築基準法/同施行令
・消防法/同施行令/同施行規則
・不正競争防止法
・著作権法・個人情報の保護に関する法律（個人情報保護法）
・行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（番号法）
・外国為替及び外国貿易法（外為法）および輸出貿易管理令
・労働契約法
・労働基準法
・会社法
・金融商品取引法
・刑事訴訟法

（適用範囲）

第９条　『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・環境的リソースを含むものとする。

本学園の所有する情報システムの概要は、以下の図のとおりとする。



２　本学園が所有する情報システムではないが、契約等により本学園の情報を運用・管理しているサービス等で取り扱う情報に関しては、『情報セキュリティポリシー』の適用範囲とする。

（適用者）
第１０条　『情報セキュリティポリシー』の適用者は、本学園の経営に関わる者、教職員および契約社員、その他本学園の情報資産を利用するすべての者とする。

（定義）
第１１条　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。
(1)　情報システム
　情報処理及び情報ネットワークに係わるシステムで、次のものをいい、本学園情報ネットワークに接続する機器を含む。
　① 本学園により、所有又は管理されているもの
　② 本学園との契約あるいは他の協定に従って提供されるもの
(2)　情報
　情報には次のものを含む。
　①　情報システム内部に記録された情報
　②　情報システム外部の電磁的記録媒体に記録された情報
　③　情報システムに関係がある書面に記載された情報
(3)　情報資産
　情報システム並びに情報システム内部に記録された情報、情報システム外部の電磁的記録媒体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をいう。
(4)　事務情報
　事務情報とは情報のうち次のものをいう。
　①「法人文書の管理に関する規程」の対象となる法人文書
　②　①以外の法人文書で、部局長が指定した文書
(5)　事務情報システム
　事務情報を扱う情報システムをいう。
(6)　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。
　注）
　機密性は、情報にアクセスすることが認可された者だけがアクセスできることを確実にすること、として定義される。
　完全性は、情報及び処理方法の正確さ及び完全である状態を安全防護すること、として定義される。
　可用性は、許可されたユーザが、必要時に、必要な情報及び関連資産にアクセスできることを確実にすること、として定義される。
(7)　ポリシー
　本学園が定める「情報セキュリティ基本方針」「情報セキュリティ基本規程」及び「情報セキュリティ対策規程」をいう。

(8)　対策規程

本学園が定める「情報セキュリティ基本方針」「情報セキュリティ基本規程」に基づいて策定される規程及び、基準、計画をいう。

(9)　手順書

対策規程に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。

(10)　利用者

教職員等及び学生等で、本学園情報システムを利用する許可を受けて利用するものをいう。

(11)　教職員等

本学園を設置する法人の役員及び、本学園に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局総括責任者が認めた者をいう。

(12)　学生等

本学園通則に定める学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。

(13)　臨時利用者

教職員等及び学生等以外の者で、本学園情報システムを臨時に利用する許可を受けて利用するものをいう。

(14)　電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

(15)　情報セキュリティインシデント

情報セキュリティに関し、意図的または偶発的に生じる、本学園規程または法律に反する事故あるいは事件をいう。

(16)　CSIRT（シーサート）

本学園において発生した情報セキュリティインシデントに対処するため、本学園に設置された体制をいう。Computer Security Incident Response Team の略。

(17)　明示等

情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

(18)　リスクアセスメント

情報及び情報処理施設や設備に対する脅威と重要度を特定し、事故発生につながる脆弱性及び事故のおこりやすさを評価することをいう。

(19)　リスクマネジメント

リスクアセスメントにより、情報及び情報処理施設や設備に影響を及ぼす可能性がある情報セキュリティリスクを明確にし、許容コストに応じて情報セキュリティリスクを制御し、最小限に抑制するか、又は除去するプロセスを指す。

(20)　脅威

自然災害、機器障害、悪意のある行為等、損失を発生させる直接の要因をいう。

(21)　脆弱性

　ハードウェア・ソフトウェアの欠陥、定期点検の不備、要員教育の不備等、脅威を増加させる要因（脆さ、弱点）をいう。

第２章　情報セキュリティ委員会

（組織の目的）

第１２条　本学園の情報システムについて、教育・研究上必要な情報の円滑な伝達及び健全な運用を目的として、情報セキュリティ委員会を設ける。

（組織の概要）

第１３条　情報セキュリティ委員会は、本学園情報教育センターを中心に、本学園法人本部、総務部情報システム課により運営する。

２　組織に関する詳細は、別途『情報セキュリティ委員会組織規程』にて定める。

第３章　情報セキュリティマネジメント

（リスク分析）

第１４条　本学園の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

（情報セキュリティポリシーの策定）

第１５条　『情報セキュリティポリシー』の策定・評価・レビューは、情報セキュリティ委員会が行うこととする。

情報セキュリティ委員会では、基本規程および対策規程を策定することとする。

対策手順書に関しては、情報セキュリティ委員会より指名された各情報システムの担当者が策定し、運用しなければならない。

（対策の実施）

第１６条　本学園で策定した『情報セキュリティポリシー』に記述した対策は、計画的に実装しなければならない。情報システム課は、セキュリティ対策実装のための計画書を策定し、情報セキュリティ委員会の承認を得なければならない。

（教育・啓蒙）

第１７条　本学園は、情報資産を扱うすべての者に対し、意識向上と技術レベルの向上の両面から、積極的に啓蒙活動及び情報セキュリティ教育を行うこととする。

本学園の情報資産に関わるすべての者は、本学園が実施する情報セキュリティの教育を受けなければならない。同時に、本学園の情報資産に関わる者は、情報セキュリティに関する最新の情報について、自発的に情報セキュリティ委員に提言することが望ましい。

（情報セキュリティ侵害時の対応）

第１８条　本学園の情報セキュリティが侵害されたと思われる事象が判明した場合は、速やかに準備された対応方法に従って対応しなければならない。

（違反者の取り扱い）

第１９条　本学園は、『情報セキュリティポリシー』の違反者に対し、必要かつ適切な措置（教育・研修、処分等）をとるものとする。情報セキュリティ委員会は、『情報セキュリティポリシー』に違反した事項の重要度を評価し、被害の防止と拡大に資する適切かつ必要な措置をとることとする。

２　本学園の情報資産運用に係わる関連規定及び関連規則の違反者についても、『情報セキュリティポリシー』の違反者と同様に対処する。

３　意図的に情報セキュリティを侵害しようとした者や、情報セキュリティ侵害が発生した際に情報セキュリティ委員会等の指示に従わない者に対しては、厳格な措置をとる。

（評価と見直し）

第２０条　情報セキュリティ委員会は、定期的あるいは発見の可能性のあるときに情報セキュリティに対する脅威、脆弱性を洗い出し、その対策を検討し、必要があると認めた場合にはその見直しを行う。それらは、監査の結果、情報資産の利用者から届けられた情報、情報セキュリティの脆弱性に関する情報の収集等の活動から得られる情報をもとに行われる場合もある。

２　本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

附則　この規則は、令和 2 年 4 月１日から施行する。