学校法人尚絅学園 情報システム運用基本規程

（目的）

第１条　本規程は、学校法人尚絅学園（以下「本学園」という。）における情報システムの運用及び管理について必要な事項を定め、もって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。

（適用範囲）

第２条　本規程は、本学園情報システムを運用・管理する全ての者、並びに利用者及び臨時利用者（来学中に利用する訪問者や受託業務従事者などの臨時利用者を含む。）に適用する。

（定義）

第３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。なお、情報ネットワークに接続されている情報処理システムだけではなく、スタンドアロンの情報処理システムも含まれる。また、下記の二つの項目に該当しない機器、例えば私物 PC であっても本学園の情報ネットワークに接続する時は本規程の対象となる。

(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、ネットワークに接続している、いないに関わらず、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

(4)　情報システムの運用管理に関する資料（仕様、設計、運用、管理、操作方法などの資料）

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、情報システムに関係がある書面及び情報システムの運用管理に関する資料等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)　「学校法人尚絅学園文書取扱・管理規程」の対象となる文書

(2)　(1)以外の文書で、文書管理責任者が指定した文書

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。なお、事務情報システムには、事務局が運用責任を持つ情報システムばかりではなく、教員等が成績管理に使用するパソコン等も含まれる。

６　情報システムポリシー

本学園が定める「学校法人尚絅学園　情報システム運用基本方針（以下、「情報システム運用基本方針」という。）」及び「学校法人尚絅学園　情報システム運用基本規程（以下、「情報システム運用基本規程」という。）」をいう。

７　実施規程

情報システムポリシーに基づいて策定される規程及び基準、計画をいう。

8　手順

実施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。

9　利用者

教職員等及び学生等並びに臨時利用者で、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。

10　教職員等

法人の役員及び本学園が設置する学校等に勤務する常勤又は非常勤の教職員（派遣職員、パート職員、臨時職員等を含む）その他、総括文書管理責任者が認めた者をいう。

11　学生等

本学園が設置する大学及び短期大学部学生、中学校・高等学校生徒、聴講生、科目履修生、留学生等、その他、総括文書管理責任者が認めた者をいう。

12　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。なお、訪問者や受託業務従事者などの本学園構成員以外の者が本学園情報システムを臨時に利用する場合は、所定の手続きで身元を確認した上で、情報システムポリシー及び関連規程を遵守することを条件に利用を許可するものとする。

13　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。

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。

（注）電磁的記録として扱われる記録方式を用いる媒体の例：

メモリ、ハードディスク、CD、DVD、光磁気(MO)ディスク、磁気テープ、磁気カード、IC カード、二次元バーコード（QR コード等）

電磁的記録ではないものの例：

人の知覚による認識を目的としたコンピュータからの印刷出力、入力用に記入する伝票、フォーム等の帳票類、マイクロフィルム

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。

（注）情報セキュリティインシデントの例としては、地震・水害等の天災、火災、事故等によるネットワークを構成する機器や回線の物理的損壊や滅失によるネットワークの機能不全や障害、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等がある。また、その疑いがある場合及びそれに至る行為もこれに準じて扱う。

16　CSIRT（シーサート）（Computer Security Incident Response Team の略。）

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。

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。情報の格付については「学校法人尚絅学園　情報システム運用・管理規程」（以下、「情報システム運用・管理規程」という。）に定める。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。

（注）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をいう。

（全学情報システム総括責任者）

第４条　本学園情報システムの運用に責任を持つ者として、本学園に全学情報システム総括責任者を置き、学園事務局長をもって充てる。

２　全学情報システム総括責任者は、情報システムポリシー及びそれに基づく規程の決定や情報システム上での各種問題に対する処置を行う。

３　全学情報システム総括責任者は、全学の情報基盤として供される本学園情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

４　全学情報システム総括責任者は、全学向け教育及び全学情報システムを担当する部局情報システム技術担当者向け教育を統括する。

５　全学情報システム総括責任者に事故があるときは、全学情報システム総括責任者があらかじめ指名する者が、その職務を代行する。

６　全学情報システム総括責任者は、原則として、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして、理事長の承認を経て、置くことができる。

（情報システム委員会）

第５条　本学園情報システムの円滑な運用のために、本学園に情報システム委員会を置く。

２　情報システム委員会は以下を実施する。

(1)　情報システムポリシー及び全学向け教育の実施ガイドラインの改廃に関する事項

(2)　情報システムの運用と利用及び教育に係る規程及び手順の制定及び改廃に関する事項

(3)　情報システムの運用と利用に関する教育の年度講習計画の制定及び改廃並びにその計画の実施状況の把握に関する事項

(4)　情報システム運用リスク管理規程の制定及び改廃並びにその実施状況の把握に関する事項

(5)　情報システム非常時行動計画の制定及び改廃並びにその計画の実施状況の把握に関する事項

(6)　情報セキュリティインシデントの再発防止策の検討及び実施に関する事項

（情報システム委員会の構成員）

第６条　情報システム委員会は、委員長及び次の各号に掲げる委員をもって組織する。

１　全学情報システム実施責任者

２　各設置校情報システム総括責任者
３　ＣＳＩＲＴ責任者
４　その他全学情報システム総括責任者が必要と認める者

（情報システム委員会の委員長）
第７条　情報システム委員会の委員長は、全学情報システム総括責任者をもって充てる。
２　委員長は、会務を総理する。

（全学情報システム実施責任者）
第８条　本学園に全学情報システム実施責任者を置く。
２　全学情報システム実施責任者は、全学情報システム総括責任者の指示により、本学園情報システムの整備と運用に関し、情報システムポリシー及びそれに基づく規程並びに手順等の実施を行う。
３　全学情報システム実施責任者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用並びに利用及び情報システムのセキュリティに関する教育を企画し、情報システムポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。
４　全学情報システム実施責任者は、本学園の情報システムのセキュリティに関する連絡と通報において本学園情報システムを代表する。
５　全学情報システム実施責任者は、学園事務局総務部長をもって充てる。

（情報セキュリティ監査責任者）
第９条　情報システムポリシーに基づき、本学園情報システムの情報セキュリティ監査を実施するため、情報セキュリティ監査責任者を置く。
２　監査の独立性・実効性を確保するため、情報セキュリティ監査責任者は、内部監査室長をもって充て、監査に関する事務を統括する。

（管理運営部局）
第 10 条　情報システム委員会は、本学園情報システムの管理運営部局を定め、学園事務局総務部とする。

（管理運営部局が行う事務）
第 11 条　管理運営部局は、全学情報システム実施責任者の指示により、以下の各号に定める事務を行う。
１　情報システム委員会の運営に関する事務
２　本学園情報システムの運用と利用における情報システムポリシーの実施状況の取りまとめ
３　本学園情報システムの講習計画、リスク管理及び非常時行動計画等の実施状況の取り纏め
４　本学園情報システムのセキュリティに関する連絡と通報

（部局情報システム総括責任者）
第 12 条　各設置校及び大学図書館、中高図書室並びに各事務局・事務室等（以下、「部局」という。）に部局情報システム総括責任者を置き、以下の者をもって充てる。

(1) 大学においては、各学部長
(2) 短期大学部においては、各学科長
(3) 中学校・高等学校においては、教頭
(4) 附属こども園においては、副園長
(5) 大学図書館においては、図書館長
(6) 中高図書室においては、図書室長
(7) 大学事務局においては、大学事務局長
(8) 中・高事務室においては、中・高事務長
(9) 附属こども園事務室においては、附属こども園事務室長
(10) 学園事務局においては、総務部総務課長

2　部局情報システム総括責任者は、部局における運用方針の決定や情報システム上での各種問題に対する処置を担当する。

（部局情報システム運用部会）

第 13 条　各部局に部局情報システム運用部会を置く。

2　部局情報システム運用部会は以下の各号に掲げる事項を実施する。
(1) 部局における情報システムポリシーの遵守状況の調査と周知徹底に関する事項
(2) 部局における情報システムの運用と利用及び教育に係わる内規及び手順に関し、部局において必要な内規の制定及び改廃に関する事項
(3) 部局における情報システムのリスク管理及び非常時行動計画の策定及び実施に関する事項
(4) 部局における情報セキュリティインシデントの再発防止策の策定及び実施に関する事項
(5) 部局における部局情報システム技術担当者向け教育の計画と企画に関する事項

（部局情報システム運用部会の構成員）

第 14 条　部局情報システム運用部会は、部会長及び次の各号に掲げる者を委員として組織する。
1　部局情報システム技術責任者
2　部局情報システム技術担当者
3　その他部局情報システム総括責任者が必要と認める者

（部局情報システム運用部会の部会長）

第 15 条　部局情報システム運用部会の部会長は、部局情報システム総括責任者をもって充てる。

（部局情報システム技術責任者）

第 16 条　部局に部局情報システム技術責任者を置き、部局情報システム総括責任者が任命する。なお、部局情報システム総括責任者は部局情報システム技術責任者を兼務することができる。

2　部局情報システム技術責任者は、部局情報システムの構成の決定や技術的問題に対する処置を担当する。

3　部局情報システム技術責任者は、部局情報システム技術担当者に対して、情報システムポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

（部局情報システム技術担当者）
第 17 条　部局情報システム技術責任者は、当該部局の情報システムの管理業務において必要な単位ごとに、部局情報システム技術担当者を置く。部局情報システム技術担当者は部局情報システム技術責任者が推挙し部局情報システム総括責任者が任命する。なお、部局情報システム技術責任者自ら部局情報システム技術担当者を兼務することができる。
２　部局情報システム技術担当者は、部局情報システム技術責任者の指示により、部局の情報システムの運用の技術的実務を担当し、利用者への教育を補佐する。

（区域情報セキュリティ責任者の設置）
第 18 条　部局情報システム総括責任者は、施設及び環境に係る対策を行う単位ごとの区域を定め、その区域ごとに、区域情報セキュリティ責任者 1 人を置く。
２　区域情報セキュリティ責任者は、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を総括する。

（職場情報セキュリティ責任者の設置）
第 19 条　部局情報システム総括責任者は、教室、研究室、事務室等の管理組織ごとに、職場情報セキュリティ責任者 1 人を置く。
２　職場情報セキュリティ責任者は、教室、研究室、事務室等の管理組織における情報の取扱いその他の情報セキュリティ対策に関する事務を総括する。

（全学情報セキュリティアドバイザーの設置）
第 20 条　全学情報システム総括責任者は、情報セキュリティについて専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして置くことができる。
２　全学情報システム総括責任者は、全学情報セキュリティアドバイザーを置く場合は、以下を例とする全学情報セキュリティアドバイザーの業務内容を定める。
(1)　本学園全体の情報セキュリティ対策の推進に係る全学情報システム総括責任者への助言
(2)　情報セキュリティ関係規程の整備に係る助言
(3)　対策推進計画の策定に係る助言
(4)　教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
(5)　情報システムに係る技術的事項に係る助言
(6)　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
(7)　利用者に対する日常的な相談対応
(8)　情報セキュリティインシデントへの対処の支援
(9)　前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（情報セキュリティインシデントに備えた体制の整備）
第 21 条　全学情報システム総括責任者は、CSIRT を整備し、その役割を明確化する。
２　全学情報システム総括責任者は、教職員等のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち、本学における情報セキュリティイ

ンシデントに対処するための責任者としてCSIRT責任者を置く。
3　全学情報システム総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

（CSIRTの役割）
第22条　全学情報システム総括責任者は、以下を含むCSIRTの役割を規定する。
(1) 報告窓口からの情報セキュリティインシデントの報告の受付
(2) 情報セキュリティインシデントの全学情報システム総括責任者等への報告
(3) 対外的な連絡
(4) 被害の拡大防止を図るための応急措置の指示又は勧告
2　全学情報システム総括責任者は、CSIRTの責任者（PoC（Point of Contact））を置く。

（役割の分離）
第23条　情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。
(1) 承認又は許可事案の申請者とその承認又は許可を行う者（以下、本項において「承認権限者等」という。）
(2) 監査を受ける者とその監査を実施する者
2　前項の定めに係わらず、教職員等は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をする。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。
3　教職員等は、前事項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずる。

（情報の格付け）
第24条　情報システム委員会は、情報システムで取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備する。

（学外の情報セキュリティ水準の低下を招く行為の防止）
第25条　全学情報システム実施責任者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備する。
（注）学外の情報セキュリティ水準の低下を招く行為としては、例えば、以下のものが挙げられる。
・本学園のウェブのコンテンツを利用するために、ブラウザのセキュリティ設定の下方修正を明示的に要求する行為
・本学園のウェブにより実行形式のファイル（Windows® の場合、「.exe」ファイル）を提供（メールに添付する場合も同様）する行為
・本学園のウェブにより署名していない実行モジュール（Java® アプレットやWindows®のActiveX® ファイル）を提供する行為
・本学園からHTML メールを送信する行為

なお、後者の２つについては、利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある行為である。

２　本学園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、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

（情報システム運用の外部委託管理）

第 26 条　全学情報システム総括責任者は、本学園情報システムの運用業務のすべてまたはその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

（情報セキュリティ監査）

第 27 条　情報セキュリティ監査責任者は、情報システムのセキュリティ対策が情報システムポリシー（情報システム運用基本方針及び本規程）に基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別途定める情報セキュリティ監査規程に従う。

（見直し）

第 28 条　情報システムポリシー、実施規程及び手順を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。

２　本学園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。

（所管）

第 29 条　この規程の実施に関する事務の所管は、学園事務局総務部とする。

（改廃）

第 30 条　この規程の改廃は、理事長の決裁をもって行うものとする。

附則

この規程は、平成 29 年 11 月 1 日から施行する。