学校法人新静岡学園情報セキュリティポリシー

（目　的）

第１条　学校法人新静岡学園（以下「法人」という。）において、健全な教育・研究活動を実践し、社会的責務を果たすためには、情報基盤の整備に加えて、情報資産のセキュリティを確保することが不可欠である。そこで、法人が設置する学校の教職員及び学生・生徒が情報セキュリティの重要性を認識し、法人における情報資産を適切に保護・管理するために、情報セキュリティポリシー（以下「ポリシー」という。）を定める。

（用語の定義）

第２条　この規程における用語の定義は、次のとおりとする。

(1) ネットワーク	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）をいう。
(2) 情報システム	コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。
(3) 情報機器	情報の処理、保存、入出力の機能を持つ電子機器で、サーバ、パソコン、スマートフォン等の本体及びディスプレイ、プリンタ等の周辺機器をいう。
(4) 情報資産	法人にとって価値を有する情報が記録された媒体及び情報システムをいう。
(5) 機密性	情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。
(6) 完全性	情報資産が破棄、改ざんまたは消去されていない状態を確保することをいう。
(7) 可用性	情報資産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、情報資産にアクセスできる状態を確保することをいう。
(8) 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。
(9) 脅威	情報資産の価値を失わせる事象をいう。不正アクセス等の意図的脅威、入力ミス等の偶発的脅威、災害時の環境的脅威、人的脅威を指す。
(10) 部局	静岡産業大学、静岡学園中学校・高等学校、法人事務局をいう。

（ポリシーの構成）

第３条　ポリシーは、次のとおり構成する。

(1) 情報セキュリティ基本方針（以下「基本方針」という。）

法人が情報セキュリティに取り組む上での統一的かつ基本的な方針

(2) 情報セキュリティ対策基準（以下「対策基準」という。）

基本方針に基づき情報セキュリティ対策を実施する上での遵守事項及び判断基準

２　情報セキュリティの実施手順については、対策基準に基づき、各部局において定める。

（対象範囲）

第４条　このポリシーは、次の各号に定める情報資産を対象とする。情報資産を利用するすべての者（以下「利用者」という。）は、業務の遂行にあたり、このポリシーを遵守しなければならない。

(1) 法人が管理するネットワーク、情報システム及びそれらに接続された情報機器

(2) 利用者が法人の教育、研究その他の業務のために作成または取得した情報で、前号のネットワーク、情報システム、情報機器に記憶させたもの

(3) その他法人が情報資産と認めるもの

Ⅰ　情報セキュリティ基本方針

（基本方針）

第５条　第１条の目的を達成するため、法人の基本方針を次のとおり定める。

(1) 個人情報保護法、不正アクセス禁止法など、情報セキュリティに関する法令を遵守する。

(2) 情報セキュリティに関する責任を明確にし、対策を実施するための体制を整備する。

(3) 情報セキュリティに関するリスクを識別し、組織的、物理的、人的、技術的に適切な対策を実施する。

(4) 情報セキュリティに関する教育及び啓発を実施し、情報システムを安全に利用するために必要な知識や判断力の向上に努める。

(5) 情報セキュリティに関する問題が生じたときは、速やかに対策を講じるとともに、原因究明及び再発防止に努める。

(6) 情報セキュリティを脅かす者に対し適切な措置を講じる。

(7) 情報セキュリティに関する管理体制及び取り組みについて点検を実施し、組織的に改善・見直しを行う。

（監査及び自己点検）

第６条　ポリシーの遵守状況を検証するため、必要に応じて、情報セキュリティ監査及び自

己点検を実施する。

（ポリシーの見直し）

第７条　情報セキュリティ監査及び自己点検の結果や情報セキュリティに関する状況・環境の変化などにより、新たに対策が必要になった場合には、ポリシーの見直しを行う。

Ⅱ　情報セキュリティ対策基準

第１章　総則

（趣　旨）

第８条　この対策基準は、法人の基本方針に基づき、適切な情報セキュリティ対策を講ずるために必要な組織・体制、基準、遵守事項等について定めるものである。

第２章　組織・体制

（組織・体制）

第９条　法人における情報基盤を整備し、情報資産の有効活用及びセキュリティ確保を実現するための組織を次のとおり設置し、その体制図を別表のとおり定める。

(1) 情報セキュリティ管理統括責任者

各部局に情報セキュリティ管理統括責任者（以下「管理統括責任者」という。）を置き、大学事務局長、中学・高校長、法人事務局長をもってこれに充てる。管理統括責任者は、当該情報資産に関わる情報セキュリティについて責任を負うとともに、緊急時にはあらゆる所管を超えて緊急措置を取る権限を有する。

(2) 情報セキュリティ管理者

管理統括責任者の下に情報セキュリティ管理者（以下「管理者という。」）を置き、大学事務局次長、中学・高校事務長、法人事務局DX推進課長をもってこれに充てる。管理者は、当該所管における情報資産に関わる情報セキュリティ管理を統括し、緊急時には情報資産の保護を最優先とし、当該所管に対して緊急措置をとる権限を有する。

(3) 情報セキュリティ技術担当者

管理者の下に情報セキュリティ技術担当者（以下「技術担当者」という。）を置き、大学事務局情報システム課長、中学・高校情報管理課長、法人事務局DX推進課職員をもってこれに充てる。技術担当者は、当該所管における情報セキュリティ対策の実施に係る作業を行い、インシデント発生時には管理者の指示に従い、迅速かつ適切に対応する。

(4) 情報セキュリティ会議

法人に情報セキュリティ会議（以下「会議」という。）を置き、常任理事会をもって

充てる。会議は、法人の情報資産に関わる情報セキュリティについて総括的な意思決定を行う。

(5) 情報セキュリティ管理部会

情報セキュリティ管理部会は、管理統括責任者、管理者、技術担当者及び各部局の管理統括責任者が必要と認める教職員で構成し、情報資産をセキュリティリスクから守り、業務を継続するために必要な施策について検討する。インシデント発生時は会議の指示に従って速やかに対応を行い、その状況や原因、再発防止策について会議に報告する。

(6) 情報セキュリティ監査部会

情報セキュリティ監査部会（以下「監査部会」という。）は、監査室長及び監事で構成し、情報セキュリティ施策の遵守状況及び情報資産が適正に管理・運用されているかについて、必要に応じて監査を行い、監査結果及び改善指導等を会議に報告する。また、会議の承認により、業務の一部を専門の第三者機関に委託することができる。

第３章　情報資産の分類と管理

（情報資産の分類）

第10条　機密性の観点から、情報資産を次のとおり分類し、法人が所有する情報資産のうち、機密性２及び３の情報資産を「重要な情報資産」という。

機密性	レベル	分　類　基　準
1	公開	外部に公開可能
2	秘密	法人関係者に限り、取り扱い可能
3	極秘	一部の法人関係者に限り、取り扱い可能

（情報資産の管理）

第11条　情報資産の作成、入手、利用及び保管に関しては、前条の分類に基づき適切に取り扱う。また、利用者は業務以外の目的に情報資産を利用してはならない。

（情報資産の持出）

第12条　利用者は、原則として重要な情報資産を外部に持ち出してはならない。やむを得ず持ち出す場合は、情報漏えいが起きないよう、情報セキュリティ対策を講じなければならない。

（情報資産の廃棄）

第13条　利用者は、重要な情報資産が含まれる電磁的媒体を廃棄する場合は、残存情報が第

三者に読み取られることがないよう、物理破壊、ソフトウェア消去、または磁気消去等の情報セキュリティ対策を講じなければならない。

第４章　物理的セキュリティ

（サーバ室の管理）

第14条　技術担当者は、重要な情報資産を保管しているサーバ室の施錠や入退室の制限など必要な対策を講じなければならない。

（情報機器の管理）

第15条　技術担当者は、情報機器の盗難対策、定期保守及びデータのバックアップを必要に応じて実施する。

第５章　人的セキュリティ

（利用者の遵守事項）

第16条　利用者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたっては、本ポリシー及び情報セキュリティに関する法令を遵守しなければならない。

（教育及び研修）

第17条　管理統括責任者は、情報セキュリティに関する啓発や教育を実施するため、必要に応じて研修を実施する。

（ID及びパスワードの管理）

第18条　利用者は、ID及びパスワードについて、各自が責任を持って管理し、貸与、販売、譲渡等により第三者に使用させてはならない。

（事故及び障害時の報告）

第19条　利用者は、情報セキュリティに関する事故及び情報システムの障害を発見した場合は、直ちに技術担当者または管理者に報告しなければならない。

２　技術担当者は、情報セキュリティに関する事故及び情報システムの障害等を発見した場合または利用者からその報告を受けた場合は、速やかに調査を行わなければならない。不正が確認されたときは、関係する通信の遮断、情報システムの切り離し等必要な措置を講じ、管理者及び管理統括責任者に報告しなければならない。

３　管理者及び管理統括責任者は、報告を受けた事故等についての記録を一定期間保存し、必要に応じて会議に報告する。

４　会議は、報告を受けた重大な事故等について総括的な意思決定を行う。

（外部委託）

第20条　情報システムの開発または運用管理を外部委託する場合は、外部委託業者から再委託を受ける業者も含め、本ポリシーを遵守することを明記した契約を締結するものとする。

第６章　技術的セキュリティ

（不正アクセス対策）

第21条　技術担当者は、不正アクセスを防止するため、情報機器へのアクセス制御、ネットワーク管理についての対策を講じなければならない。不正アクセスが認められた場合は、当該利用者が所属する管理者及び管理統括責任者に連絡し、適切な措置を求める。

（ウイルス対策）

第22条　技術担当者は、ウイルス情報を収集し、必要に応じて利用者に注意喚起を行うとともに、ウイルス対策を講じなければならない。利用者の情報機器からウイルスが発見された場合は、当該利用者が所属する管理者及び管理統括責任者に連絡し、適切な措置を求める。

（ログの保存）

第23条　技術担当者は、サーバ等への不正アクセス、ウイルス感染等の脅威が認められた場合は、ログ等の記録を保存し、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にし、関連情報の収集に努める。

第７章　評価・見直し等

（自己点検）

第24条　管理統括責任者は、対策基準の実効性について必要に応じて自己点検を実施し、改善が必要と認められた場合には、改善策を実施する。

（情報セキュリティ監査）

第25条　監査部会は、法人における情報セキュリティの現状を把握するため、必要に応じて情報セキュリティ監査を実施する。

２　会議は、情報セキュリティ監査結果をポリシーの見直しに活用する。

第８章　罰則

（罰　則）

第26条　利用者がポリシーに違反した場合は、その重大性、発生した事案の状況等に応じ、

法人の規程等に基づく懲戒処分を行うことがある。

第９章　改正

（改　正）

第27条　このポリシーの改正は、理事会の議決を経て行う。

附　則

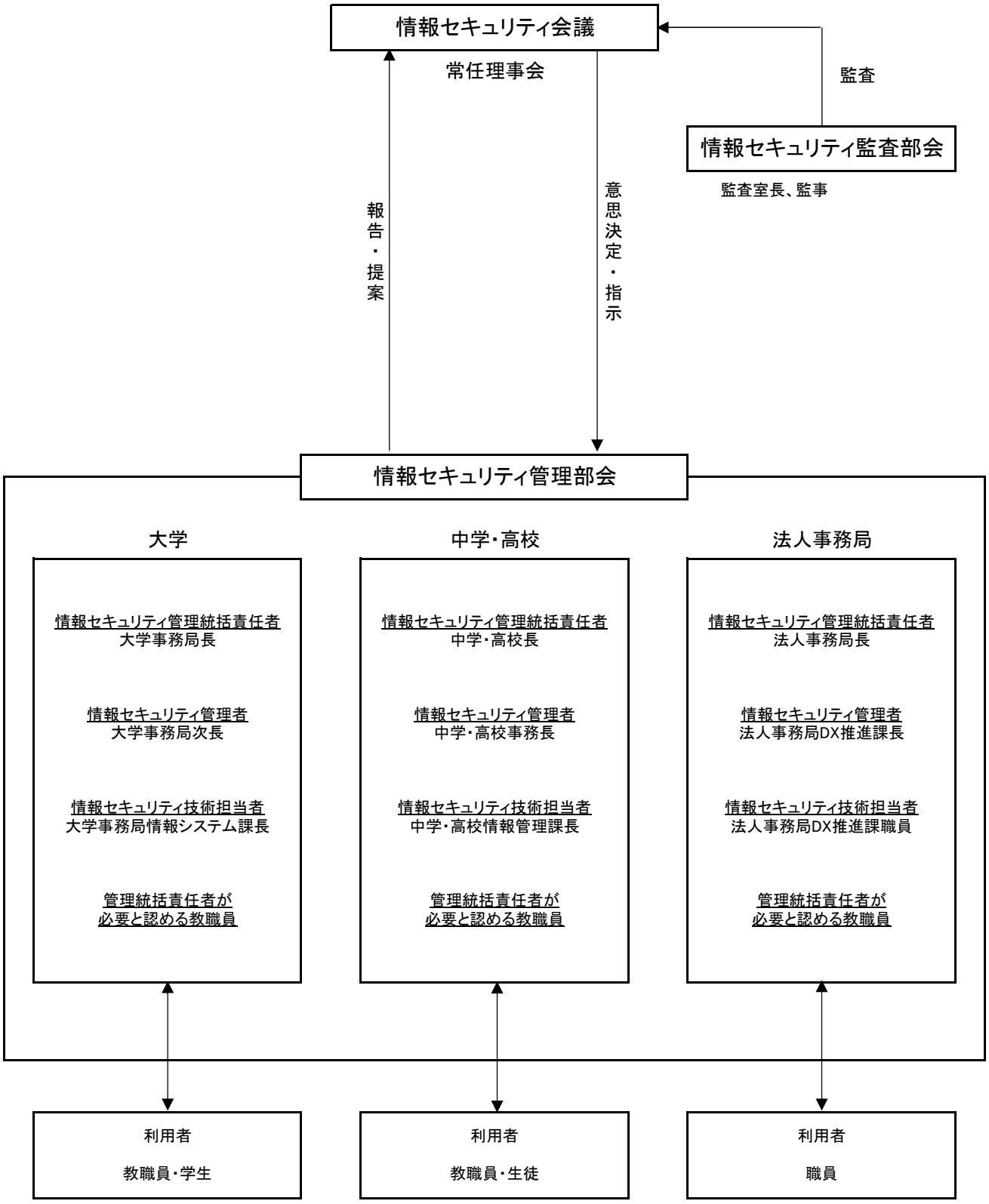
１　このポリシーは、令和７年４月１日から適用する。

２　このポリシーの施行に伴い、「学校法人新静岡学園情報セキュリティ基本方針（平成22年９月１日施行)」及び「学校法人新静岡学園情報セキュリティ対策基準（平成26年４月１日施行)」は令和７年３月31日をもって廃止する。

附　則

このポリシーの改正は、令和８年４月１日から適用する。

別表


情報セキュリティ会議
常任理事会
監査
情報セキュリティ監査部会
監査室長、監事
報告・提案
意思決定・指示
情報セキュリティ管理部会
大学
中学・高校
法人事務局
情報セキュリティ管理統括責任者
大学事務局長
情報セキュリティ管理者
大学事務局次長
情報セキュリティ技術担当者
大学事務局情報システム課長
管理統括責任者が
必要と認める教職員
情報セキュリティ管理統括責任者
中学・高校長
情報セキュリティ管理者
中学・高校事務長
情報セキュリティ技術担当者
中学・高校情報管理課長
管理統括責任者が
必要と認める教職員
情報セキュリティ管理統括責任者
法人事務局長
情報セキュリティ管理者
法人事務局DX推進課長
情報セキュリティ技術担当者
法人事務局DX推進課職員
管理統括責任者が
必要と認める教職員
利用者
教職員・学生
利用者
教職員・生徒
利用者
職員