情報セキュリティ基本方針

学校法人静岡理工科大学情報セキュリティ基本方針

情報セキュリティポリシー

学校法人静岡理工科大学（以下「学園」という）は、学園の建学の精神に基づき、高度情報化社会において地域社会に貢献する有為な人材を育成するために、教育・研究活動を実践しています。
当学園は、学園が保有する学生生徒の個人情報を始めとした全ての情報資産をあらゆる脅威から守るために厳格に管理・保護するとともに、適切な情報リテラシー教育を行い、在学する学生生徒とその保護者、卒業生並びに学園を取り巻く人々からの信頼を維持して社会的責任を果たしていきたいと考えています。
当学園は、これらの目的を達成するため、情報セキュリティ基本方針に基づく情報セキュリティポリシーを策定しました。

1. 全ての情報資産を各種の脅威から保護することの重要性を認識し、情報セキュリティ基本方針、情報セキュリティ対策基準、情報セキュリティ実施手順を定め、情報セキュリティの確保に取り組んでまいります。
2. 情報資産の管理・保護の重要性を認識し、学園の全役員及び教職員（嘱託職員、派遣職員、非常勤職員を含む）に対して個人情報保護法を始めとした情報資産保護のための関連法規並びに当学園が定めた情報セキュリティポリシーの遵守の徹底を図るとともに、情報セキュリティ教育・訓練を実施します。
3. 情報セキュリティの確保を図るための管理体制を整備し、情報資産への不正な侵入や情報の漏洩、消失、改ざん、破壊等の脅威に対処するため、情報セキュリティ基本方針、情報セキュリティ対策基準、情報セキュリティ実施手順が有効に機能しているかを継続的に検証し、改善してまいります。

情報セキュリティ基本方針

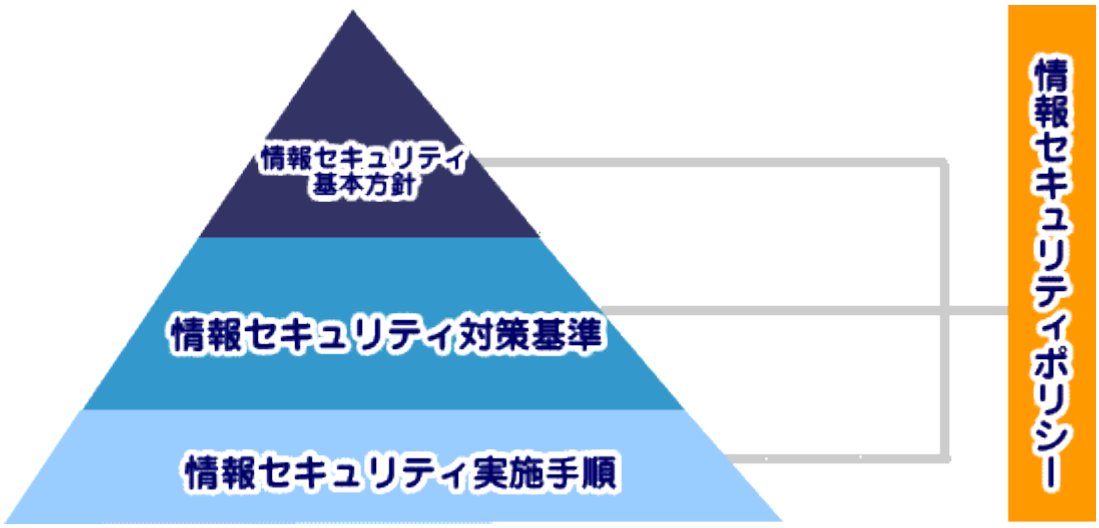
1. **目的**
   情報セキュリティ基本方針は当学園の情報セキュリティに関し、包括的な対策を図ることにより、学園が保有する情報資産を適切に保護することを目的とする。
2. **定義**

情報セキュリティポリシーで対象とする情報資産とは、当学園の教育・研究活動において入手及び知り得た情報並びに当学園が業務運営上保有する全ての情報とする。

3. 情報セキュリティ対策の体系

学園は、情報セキュリティ対策について総合的・体系的かつ具体的に取りまとめた情報セキュリティポリシーを策定する。

情報セキュリティポリシーは、情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順から構成される。



（1）情報セキュリティ基本方針

情報セキュリティ基本方針は、当学園における情報セキュリティに関する指針であり、個人情報保護、情報公開、各種サービスの遂行や情報セキュリティに関する学園の責務・体制についての基本的な考え方を示したものである。

（2）情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針を実現するために、学園の業務を運営するに当って統一して遵守すべき対策の基準を示したものである。

（3）情報セキュリティ実施手順

情報セキュリティ実施手順は、情報セキュリティ対策基準に基づき、各所属の実情に則して情報システム又は業務における具体的な手順や対処方法を示したものである。

4. 情報セキュリティポリシーの公開

情報セキュリティの確保の観点から公開するものは、情報セキュリティ基本方針

とする。

5. 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は、学園が取扱う情報資産及び情報資産を取り扱う者すべて（外部委託先を含む）に適用する。

6. 情報セキュリティ組織運営

情報セキュリティ推進及び向上のための組織は次のとおりとする。

① 情報セキュリティの最高責任者として、情報セキュリティ統括責任者を置き、専務理事をもって充てる。

② 情報セキュリティ統括責任者を補佐し、学園の情報セキュリティ対策に関する助言並びに担当部門の情報セキュリティの実施における指導・監督を行う者として、法人本部に情報セキュリティ副統括責任者を置き、常勤の理事、監査室長、大学学長及び本部長の内から情報セキュリティ統括責任者が選任する。

③ 各所属には情報セキュリティ責任者、情報セキュリティ副責任者（高等学校部門のみ）及び情報セキュリティ管理者を置くとともに、必要に応じてネットワークまたは情報システムを管理する担当者を置く。

④ 情報セキュリティの確保、向上を統一的な視点で行うとともに情報セキュリティ事件・事故等の対応を行うために、情報セキュリティ統括責任者及び情報セキュリティ副統括責任者をもって構成する情報セキュリティ委員会を設置する。

7. 情報管理基準

（1）各所属における情報を適切に取り扱うため、情報セキュリティ管理者は重要性に基づいて情報を分類する。

（2）情報の作成、配布、持ち出し、消去、廃棄等を行う場合には、定められた情報分類に応じて必要な措置を行う。

8. 情報セキュリティ行動基準

情報セキュリティの確保を図るため、次の事項を守らなければならない。

① 業務上知り得た情報は、許可なく第三者に開示したり漏洩してはならない。

② 学園が保有する情報資産は、業務目的以外で使用しない。なお、個人情報においては、その取得の際に明示した目的以外には使用しない。

③ 個人が所有するもので学園の情報を外部に持ち出すことができる機器等は、原則として学園内に持ち込まない。

④ 情報セキュリティに関する事件・事故等があった場合には、直ちに情報セキュリティ管理者に報告する。

9. 教育・訓練

学園は、情報セキュリティ確保のため、役員及び教職員等に対して情報セキュリテ

ィについての教育・訓練を実施する。

10. 環境・危機管理

情報セキュリティを確保し、不正な立ち入りや盗難、自然災害等から情報資産を適切に保護するため、入退館管理や物理的に必要な措置を行う。

11. 情報システム管理

情報システムの運用管理はシステム担当者が行うものとし、情報セキュリティの確保を図るため次の事項を定める。

① 情報システムの重要度に応じて障害対策及び障害発生時の対応及びその復旧について定める。

② 情報の漏洩を防ぐため、端末等の不正使用防止、情報資産の持ち出しや廃棄、外部システムとのデータ交換について必要な措置を定める。

12. ネットワーク管理

ネットワークの管理はネットワーク担当者が行うものとし、情報セキュリティの確保を図るため次の事項を定める。

① 最新のネットワーク構成と機器の状況を常に把握し、ネットワークの管理を行う。

② 情報の漏洩を防ぐため、不正アクセスの防止等必要な措置を行う。

13. 情報システム開発

（1）情報システムの企画、設計、開発及び導入を行う場合は、事前に情報セキュリティ統括責任者または情報セキュリティ委員会の承認を得なければならない。

（2）情報システムの開発に当っては、情報セキュリティを確保するために必要な措置を講じ、開発終了後にその検査を行う。

14. 外部委託

業務を外部に委託する場合は、事前に情報サービスの内容及びレベルを評価し、セキュリティ要件を明記した契約を取り交わすとともに、外部委託先の管理・監督を行う。

15. 情報セキュリティに関する事件・事故等

情報セキュリティに関する事件・事故が発生した場合には、必要な情報が遅滞なく連絡される体制を構築するとともに、被害拡大を防止するための応急措置を行う。

16. 情報セキュリティの評価・見直し

情報セキュリティポリシーの遵守状況を定期的に監査し、監査結果に基づいて必要な改善を実施する。

17. 法令等の遵守

情報資産を取扱う場合、関係法令及び諸規程等を遵守する。特に個人情報に関しては、その保護を具体化するために必要な規程・ガイドラインを作成し実行する。

18. 違反への対応

教職員の情報セキュリティポリシーの遵守状況を確認し、違反を発見した場合の報告義務及び違反者への対応を定め、再発防止に必要な措置を行う。

附則　この情報セキュリティ基本方針は、平成１８年４月１日から施行する。