学校法人明徳学園　情報セキュリティポリシー基本方針

１．趣旨

学校法人明徳学園（以下、「本学園」という。）は、中・高等教育機関である京都明徳高等学校、京都成章高等学校、京都経済短期大学を擁し、「働く人づくり日本一の教育機関」を目指して、社会で生きていく力の育成に努めている。高度情報化社会において、情報基盤の整備とコンピュータ・ネットワークの活用は教育・研究活動に不可欠なものであり、これまで本学園でも積極的に推進している。しかし、同時に個人情報をはじめとする情報資産の適切な保護が、社会的責務となっている。

このような背景から、本学園は、個人情報保護に関する基本方針を定めるとともに、その実現に必要なセキュリティ対策の基本となる情報セキュリティポリシーをここに策定する。

情報セキュリティポリシーによって目指すものは、以下の通りである。

（1）学園の情報セキュリティに対する侵害を阻止し、情報資産を保護する。

（2）内外の情報セキュリティを損ねる加害行為を抑止し、社会的信頼を確保する。

（3）適切な管理により、情報資産を有効に活用する。

本学園のすべての関係者はこのことを十分に理解したうえで、高度情報化社会における情報セキュリティの重要性を認識し、本情報セキュリティポリシーを遵守しなければならない。

２．適用範囲

（1）本ポリシーが対象とする組織は、本学園の各部門（学園法人本部、京都経済短期大学、京都明徳高等学校、京都成章高等学校）とする。

（2）対象となる情報資産の範囲は、本学園が所有するすべての情報資産および、本学園以外の情報システムで、本学園のネットワークに接続されるものである。

（3）対象者は、本学園の情報システムを利用するすべての関係者であり、教職員（非常勤教職員・派遣職員を含む）、学生（単位互換・科目等履修生を含む）、生徒、委託業者、来学者等を含む。

３．ポリシーの位置づけと構成

情報セキュリティポリシーは、本学園が所有し管理する情報資産に関する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ものである。ただし、個人情報については「個人情報の保護に関する規程」および関係規則に定める。

情報セキュリティポリシーは以下の構成とする。

（1）基本方針

本学園の情報セキュリティに対する基本的な考えを、学園内および学園外に対して明示するもの。（本文書）

（2）対策基準

基本方針を具体化し、情報セキュリティを確保する上で、遵守すべき事項や判断の基準を明記したもの。学園全体で共通に適用されるものと、それに追加して各部門で定めるものがある。

また、対策基準に基づいた具体的な実施手順は、各部門において別途定めるものとする。

4．定義

情報セキュリティポリシーにおける用語の定義については、政府の情報セキュリティ対策推進会議が定めた「情報セキュリティポリシーに関するガイドライン」にあるものと同様とする。

5．遵守義務

情報セキュリティポリシー適用対象者は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用にあたっては本ポリシーおよび情報セキュリティに関する法令や諸規則を遵守しなければならない。

6．組織と体制

本学園の情報セキュリティ対策を推進するための組織を置く。当該業務は個人情報保護委員会が担当する。

また、学園は本規程の目的を達成するために、各部門ごとに情報セキュリティ管理者を置く。

7．罰則

本ポリシーに違反した者に対しては、本学園の情報資産へのアクセスを禁止または制限し、学園の各規定及び関係法令に基づき相応の措置をとることができるものとする。

8．情報セキュリティ対策の方針

（1）情報資産の分類と管理

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行う。

（2）物理的セキュリティ

情報システム設置場所について、機密性や安全性を維持するため、入退室管理

等の物理的対策や危機管理上の対策を講じる。

(3) 人的セキュリティ

情報セキュリティの管理責任体制を定め、情報セキュリティポリシーの適用対象者に対してポリシーを周知徹底させると共に、情報セキュリティを確保するための啓発や教育活動を行う等の必要な対策を講じる。

(4) 技術的セキュリティ

不正プログラムによる脅威や内外からの不正なアクセスから情報資産を適切に保護するため、情報ネットワークのアクセス制御や監視、コンピュータウイルス対策等の必要な技術対策を講じる。

9．情報セキュリティポリシーの運用ならびに評価・見直し

(1) 実施手順の策定

情報セキュリティポリシーを確実に実施していくため、各部門において、情報システムや業務などの適用範囲ごとに、情報セキュリティ対策基準に基づいた具体的な実施手順を策定する。

(2) 評価・見直し

情報システムの変更や新たな脅威など情報セキュリティに関する状況の変化に対応して有効性を維持するため、定期的または必要に応じて、情報セキュリティポリシーの評価と見直しを実施する。