裾野市教育情報セキュリティ基本方針

裾野市教育委員会

改訂履歴			
初版	令和５年９月１日	改訂４	年　月　日
改訂１	令和８年４月１日	改訂５	年　月　日
改訂２	年　月　日	改訂６	年　月　日
改訂３	年　月　日	改訂７	年　月　日

教育情報セキュリティ基本方針

１　目的

本基本方針は、本市の小中学校及び教育委員会（以下「学校等」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、学校等が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　用語の定義

（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及びその構成機器（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、ネットワーク及び電磁的記憶媒体で構成され、情報処理を行う仕組みをいう。

（３）　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。

（４）　教育情報セキュリティポリシー

本基本方針及び教育情報セキュリティ対策基準をいう。

（５）　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）　完全性

情報が破壊、改ざん又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、情報にアクセスできる状態を確保することをいう。

（８）　情報資産

ネットワークや情報システム及びこれらに関する設備、電磁的記録媒体、ネットワーク及び情報システムで取り扱う情報及びこれらを印刷した文書、情報システムの仕様書及びネットワーク図等のシステム関連文書をいう。

（９）　教育情報システム

校務や学習などの教職員、児童生徒情報を含む情報を取り扱う、学校教育で利用するシステムの総称

３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）　地震、落雷、火災等の災害並びに事故、故障等による業務の停止等

４　適用範囲

この基本方針は、本市の全ての教職員及び教育委員会職員（以下「教職員等」という。）に適用する。

５　教職員等の義務

教職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって教育情報セキュリティポリシー及び別に定める教育情報セキュリティ実施手順を遵守しなければならない。

６　情報セキュリティ対策

３に規定する脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

（１）　管理体制

情報資産を管理し、機密性、完全性、及び可用性を維持するための体制を確立する。

（２）　情報システム全体の強靭性の向上

教育情報システムにおいてはクラウド利用も含め、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（３）　物理的セキュリティ

サーバ等、通信回線等及び教職員等のパソコン等の管理について、物理的な対策を講じる。

（４）　人的セキュリティ

情報セキュリティに関し、教職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の必要な対策を講じる

（５）　技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（６）　運用

情報システムの監視、教育情報セキュリティポリシーの遵守状況の確認、外部委託を行う際

のセキュリティ確保等、教育情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。また、侵害に備えた対応訓練の定期的な実施等の対策を講ずるよう努める。

（７）　外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

７　監査及び自己点検の実施

教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて監査及び自己点検を実施する。

８　教育情報セキュリティポリシーの見直し

監査及び自己点検の結果、教育情報セキュリティポリシーの見直しが必要となった場合及び教育情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、教育情報セキュリティポリシーを見直すものとする。

９　教育情報セキュリティ対策基準の策定

6、７及び８に規定する対策等を実施するため、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。

２　前項の教育情報セキュリティ対策基準は別に定める。

３　第１項の教育情報セキュリティ対策基準は、非公開とする。

１０　教育情報セキュリティ実施手順の策定

教育長は、教育情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた教育情報セキュリティ実施手順を策定する。

２　前項の教育情報セキュリティ実施手順は、別に定める。

３　第１項の教育情報セキュリティ実施手順は、非公開とする。

１１　委任

この基本方針に定めるもののほか情報セキュリティ対策の実施に関し必要な事項は、別に定める。