大分市立学校における情報セキュリティの基本方針

大分市教育委員会

１．目的

本基本方針は、本市立小学校、中学校及び義務教育学校（以下「学校」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、学校におけ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しています。

２．定義

（１）学校ネットワーク

学校の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）をいいます。

（２）学校情報システム

学校のコンピュータ、学校ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいいます。

（３）情報資産

本基本方針が対象とする情報資産は、次のとおりです。

①学校ネットワーク、学校情報システム、これらに関する設備、電磁的記録媒体

②学校ネットワーク及び学校情報システムで取り扱う情報(これらを印刷した文書を含む。)

③学校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

④学校が保有し、校務及び授業において取り扱うすべての情報（紙等に出力された情報も含む。）

（４）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います。

①機密性

情報にアクセスすることが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います。

②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います。

③可用性

情報にアクセスすることが認められた者が、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います。

（５）学校情報セキュリティポリシー

本基本方針及び大分市立学校における情報セキュリティ対策基準（以下「学校情報セキュリティ対策基準」という。）のことをいいます。

（６）教職員等

情報資産にアクセスするすべての職員（臨時的任用又は非常勤の職にあるものを含む。）をいいます。

（７）児童生徒

学校に在学している児童及び生徒をいいます。

（８）外部委託事業者

業務委託等により情報資産を取り扱う業務に従事する事業者（下請けを行う者を含む。）をいいます。

（９）アクセス

情報資産に対し、何らかの利用目的を持って接触又は接続することで、帳票、簿冊等の記載内容を閲覧･転記するために接すること及び情報システムへネットワークを介したデータ取得のために端末を接続すること等をいいます。

３．適用範囲

本基本方針が適用される範囲は、学校、教職員等及び情報資産とします。

４．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します。

（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、火災等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

５．教職員等の責務

教職員等は、学校における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学校情報セキュリティポリシー及び情報セキュリティ実施手順を遵守します。

６．児童生徒への対応

教職員等は、児童生徒に授業又は教育以外の目的で情報資産を使用させないよう、適切に指導します。

教職員等は、児童生徒が情報資産を使用するに当たり、あらかじめ情報セキュリティ対策上遵守すべき事項を明示した上で、適切に指導します。

７．情報セキュリティ対策

脅威から情報資産を保護するために、以下の情報セキュリティ対策を実施します。

（１）組織・体制

学校における情報セキュリティ対策は、責任や役割を明確にした組織・体制のもとに行うものとします。

（２）情報の分類と管理

学校の保有する情報資産について、重要度に応じた情報分類の定義を行い、情報の管理責任及び管理方法を明確にします。

（３）物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び教職員等のパソコン等の管理について、物理的な対策を実施します。

（４）人的セキュリティ

学校における情報セキュリティに関し、教職員等、児童生徒が遵守すべき事項を定めるとともに、十分な研修及び啓発を行う等の人的な対策を実施します。

（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

技術的対策を実施します。

（６）運用

学校情報システムの監視、学校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、学校情報セキュリティポリシーの運用面の対策を実施します。

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します。

（７）委託

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行います。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じます。

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ます。

（８）評価・見直し

学校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情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図ります。学校情報セキュリティポリシーの見直しが必要な場合は、学校情報セキュリティポリシーの見直しを行います。

８．学校情報セキュリティポリシーの監査及び自己点検の実施

学校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情報セキュリティ監査及び自己点検を実施します。

９．学校情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、学校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、学校情報セキュリティポリシーを見直します。

１０．学校情報セキュリティ対策基準の策定

上記、７、８及び９に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める学校情報セキュリティ対策基準を策定します。

なお、学校情報セキュリティ対策基準は、公にすることにより本市の学校運営に重大な支障を及ぼすおそれがあることから非公開とします。

１１．情報セキュリティ実施手順の策定

学校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情報セキュリティ実施手順を策定します。

なお、情報セキュリティ実施手順は、公にすることにより本市の学校運営に重大な支障を及ぼすおそれがあることから非公開とします。

１２．公開範囲

本基本方針は、教職員等に対して学校の情報セキュリティ対策への指針を示すため、また市民・団体等に対して学校の情報セキュリティ対策への理解を得るため、広く公開を行うものとします。

附　則

この基本方針は、平成２２年４月１日から施行する。

附　則

この基本方針は、平成２６年４月１日から施行する。

附　則

この基本方針は、平成２９年４月１日から施行する。

附　則

この基本方針は、令和３年４月１日から施行する。