直方市立学校情報セキュリティポリシー

基本方針

１．目的

本基本方針は、直方市の学校教育に係る情報資産の機密性、完全性及び可用性を維持するために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．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、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録媒体で構成され、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）情報セキュリティポリシー

本基本方針をいう。

（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）情報セキュリティインシデント

情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。

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、監査機能の不備、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

4．適用範囲

（1）行政機関の範囲

本基本方針が適用される学校等は、次のとおりとする。

① 直方市立小学校
② 直方市立中学校
③ 直方市教育支援センター
④ 直方市教育研究所
⑤ 学校情報システムを所管する教育部課係（学校情報システムを所管する教育部課係については、学校情報システムの開発・保守・運用に係る事項を学校情報セキュリティポリシーの対象範囲とし、その他の範囲は、直方市が定める直方市情報セキュリティポリシーを適用するものとする。）

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
② ネットワーク及び情報システムで取り扱う情報（これらを印刷し、配布された文書を含む。）
③ 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

5．教職員等の遵守義務

上記 4 に示す学校等に所属する教職員等（以下「教職員等」という。）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は、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。

6．情報セキュリティ対策

上記 3 の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講じる。

（1）組織体制

学校等の情報資産について、情報セキュリティ対策を推進する体制を確立する。

（2）情報資産の分類と管理

学校等の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（3）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、適切な対策を講じる。

（4）物理的セキュリティ

通信回線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。

（5）人的セキュリティ

情報セキュリティに関し、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人的な対策を講じる。

（6）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。

（7）運用

学校情報システムの監視、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、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。

（8）業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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た上で、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するものとする。

なお、必要に応じて契約に基づき措置を講じる。また、クラウドサービス及びインターネット媒体を利用する場合には、利用に係る規定を整備し対策を講じる。加えて、上記サービス等を利用する場合には、運用手順を定め、利用するサービスごとの責任者を定める。

（9）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、必要に応じて情報セキュリティ監査又は自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7．情報セキュリティ監査又は自己点検の実施

情報セキュリティ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又は自己点検を実施する。

8．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や自己点検の結果、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、情報セキュリティポリシーを見直す。