大牟田市教育委員会学校情報セキュリティポリシー

（目的）

第１条　大牟田市教育委員会学校情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）は、大牟田市立学校（以下「学校」という。）において取り扱う情報資産の機密性、完全性及び可用性を確保し、児童生徒及び保護者等の個人情報を保護するとともに、学校事務及び教育活動の安定的な継続を図ることを目的とする。

（定義）

第２条　情報セキュリティポリシーにおける用語の定義は、次の各号に定めるところによる。

1. 情報資産：大牟田市教育委員会（以下「教育委員会」という。）及び学校が保有する全ての情報及び情報システムをいう。
2. 機密性：許可さ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。
3. 完全性：情報及び処理方法が正確かつ完全であることを保護することをいう。
4. 可用性：許可された利用者が必要な時に情報及び関連資産にアクセスできる状態を確保することをいう。
5. 教職員等：学校に勤務する全ての教員、職員、臨時的任用職員、非常勤職員及び外部委託業者等をいう。

（想定する脅威）

第３条　学校情報セキュリティにおいて想定される脅威は、次のとおりとする。

1. 部外者の侵入、盗難、紛失、破壊等の物理的脅威
2. 不正アクセス、ウイルス感染、サイバー攻撃等の技術的脅威
3. 操作ミス、内部不正、ソーシャルエンジニアリング等の人的脅威
4. 地震、落雷、火災、水害等の災害による脅威

（規範）

第４条　教育委員会及び学校は、情報資産の重要度に応じた適切な人的、物理的、技術的な対策を講じるものとする。また、著作権法、個人情報の保護に関する法律等の関係法令を遵守し、情報倫理に基づいた行動をとるものとする。

（教職員等の遵守義務）

第５条　教職員等は、情報セキュリティポリシー及び関連する実施手順等を遵守しなければならない。

2. 教職員等は、業務上知り得た情報を許可なく第三者に開示、漏えい、または目的外に使用してはならない。その職を退いた後も同様とする。
3. 教職員等は、情報セキュリティ事故またはその恐れがある事象を発見した場合、直ちに管理職へ報告しなければならない。

（組織体制）

第６条　学校における情報セキュリティ対策を推進・管理するため、教育委員会及び学校に以下の管理体制を整備する。

（最高教育情報セキュリティ責任者）
第７条　教育委員会に最高教育情報セキュリティ責任者を置き、教育長をもって充てる。
2. 最高教育情報セキュリティ責任者は、学校情報セキュリティに関する最終的な権限と責任を有する。
（統括教育情報セキュリティ責任者）
第８条　教育委員会に統括教育情報セキュリティ責任者を置き、事務局長をもって充てる。
2. 統括教育情報セキュリティ責任者は、最高教育情報セキュリティ責任者を補佐し、学校全体の情報セキュリティ対策を統括する。
（教育情報セキュリティ責任者）
第９条　各学校に教育情報セキュリティ責任者を置き、校長をもって充てる。
2. 教育情報セキュリティ責任者は、当該学校における情報セキュリティ対策の実施及び管理について責任を負う。
（教育情報セキュリティ管理者）
第１０条　各学校に教育情報セキュリティ管理者を置き、教頭をもって充てる。
2. 教育情報セキュリティ管理者は、教育情報セキュリティ責任者を補佐し、学校内の情報資産の管理及び教職員への指導・監督を行う。
（教育情報システム管理者）
第１１条　教育委員会事務局に教育情報システム管理者を置き、学校教育課長指導室長をもって充てる。
2. 教育情報システム管理者は、学校ネットワーク及びセンターサーバー等の基盤システムの導入、運用、保守及び管理を行う。
（教育情報システム担当者）
第１２条　各学校に教育情報システム担当者を置き、校長が指名する教職員（情報担当教員等）をもって充てる。
2. 教育情報システム担当者は、当該学校における端末等の実務的な管理運用を行う。
（教育 CSIRT の設置）
第１３条　情報セキュリティインシデント発生時の迅速な対応及び再発防止を図るため、教育委員会内に教育 CSIRT（Computer Security Incident Response Team）を設置する。
2. 教育 CSIRT は、大牟田市首長部局の CSIRT 及び外部専門機関と連携し、情報の収集、分析及び対応支援を行う。
（教育情報セキュリティ対策）
第１４条　教育委員会及び学校は、以下の情報セキュリティ対策を講じるものとする。
1. アクセス制御：情報システムへのアクセス権限は、業務上必要な最小限の範囲で付与する。
2. 認証管理：パスワードの適切な設定・管理や多要素認証の導入等により、本人確認を厳格に行う。
3. 不正プログラム対策：セキュリティソフトの導入及び定義ファイルの常時更新を行う。
4. 脆弱性対策：OS 及びソフトウェアの更新プログラムを適用し、最新の状態を保つ。

5. 物理的対策：サーバ室の施錠管理、端末の盗難防止措置等を講じる。

（緊急時の連絡及び報告体制）

第１５条　情報セキュリティ事故またはその予兆が発生した場合、発見者は直ちに教育情報セキュリティ責任者に報告しなければならない。

2. 教育情報セキュリティ責任者は、事態の緊急性等を判断し、速やかに統括教育情報セキュリティ責任者及び教育 CSIRT へ報告しなければならない。

3. 教育委員会は、重大な事故が発生した場合、関係機関への通報及び被害拡大防止措置を迅速に講じるものとする。

（教育情報セキュリティに関する監査等）

第１６条　教育委員会は、情報セキュリティポリシーの遵守状況について、定期的または必要に応じて監査及び自己点検を実施する。

2. 監査等の結果に基づき、不備が認められた場合は速やかに是正措置を講じるものとする。

（教育情報セキュリティポリシー等の見直し）

第１７条　教育委員会は、法令の改正、社会情勢の変化、技術の進歩及び監査結果等を踏まえ、必要に応じて情報セキュリティポリシーの見直しを行うものとする。

（補則）

第１８条　情報セキュリティポリシーの実施に関し必要な事項は、教育委員会が別に定める「大牟田市教育情報セキュリティ実施手順書」によるものとする。

附則　この情報セキュリティポリシーは、令和８年４月１日から施行する。