南知多町教育情報セキュリティポリシー

令和８年４月１日

〈 目　　次 〉

第１章　教育情報セキュリティ基本方針 ・・・・・・・・・・・・・・・・・・・・・・・・ 1
第１　目的 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
第２　用語の定義 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　１　ネットワーク ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　２　情報セキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　３　機密性 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　４　完全性 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　５　可用性 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　６　校務系情報 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　７　校務外部接続系情報 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
　８　学習系情報 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　９　サーバ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　10　端末機 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　11　校務用端末 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　12　学習者用端末 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　13　指導者用端末 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　14　教育情報システム ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　15　情報セキュリティインシデント ・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　16　記録媒体 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　17　スマートデバイス ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　18　情報資産 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　19　無線ＬＡＮ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　20　クラウド ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　21　ソーシャルメディアサービス ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　22　教職員 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
第３　対象とする脅威 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
第４　適用範囲 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
第５　教職員等の遵守義務 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
第６　教育情報セキュリティ対策 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
　１　管理体制 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
　２　情報資産の分類と管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
　３　物理的セキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
　４　人的セキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
　５　技術的セキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4
　６　運用 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4
　７　外部サービスの利用 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4
第７　情報セキュリティ監査及び自己点検の実施 ・・・・・・・・・・・・・・・・・・・・・ 4
第８　ポリシーの見直し ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4
第９　教育情報セキュリティ対策基準の策定 ・・・・・・・・・・・・・・・・・・・・・・・ 4

第10　教育情報セキュリティ実施手順の策定 ・・・・・・・・・・・・・・・・・・・・・・・・ 4
第２章　教育情報セキュリティ対策基準 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 5
第１　趣旨 ・・ 5
第２　組織体制 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 5
第３　教育情報資産の分類と管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 6
　１　教育情報資産の分類 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 6
　２　教育情報資産の管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 6
第４　情報システム全体のセキュリティの向上 ・・・・・・・・・・・・・・・・・・・・・・・ 8
第５　物理的セキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 8
　１　サーバ等の管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 8
　２　通信回線の管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 9
　３　職員室等のパソコン等の管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 9
　４　１人１台端末におけるセキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・ 10
第６　人的セキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 10
　１　校長の措置事項 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 10
　２　教職員の遵守事項 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 11
　３　教育委員会事務局職員の遵守事項 ・・・・・・・・・・・・・・・・・・・・・・・・・ 14
　４　研修 ・・ 15
　５　教育情報セキュリティインシデントの連絡体制の整備 ・・・・・・・・・・・・・・・・ 15
第７　技術的セキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 15
　１　コンピュータ等及びネットワークの設定管理 ・・・・・・・・・・・・・・・・・・・・ 15
　２　アクセス制御 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 17
　３　システム開発、導入、保守等 ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 17
　４　不正プログラム対策 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 18
　５　不正アクセス対策 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 19
　６　セキュリティ情報の収集 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 19
第８　運用 ・・ 19
　１　情報システムの監視 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 19
　２　ドキュメントの管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 20
　３　教職員のＩＤ及びパスワードの管理 ・・・・・・・・・・・・・・・・・・・・・・・・ 20
　４　特権を付与されたＩＤの管理等 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 20
　５　教育情報セキュリティポリシーの遵守状況の確認・管理 ・・・・・・・・・・・・・・ 20
　６　専門家の支援体制等 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 21
　７　侵害時の対応等 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 21
　８　例外措置 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 21
　９　法令遵守 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 22
第９　外部サービスの利用 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 22
　１　外部委託 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 22
　２　約款による外部サービスの利用 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 23
　３　ソーシャルメディアサービスの利用 ・・・・・・・・・・・・・・・・・・・・・・・・ 23
　４　クラウドサービスの利用 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 23

第10　評価・見直し ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 24
　1　監査 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 24
　2　自己点検 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 24
　3　本基準及び関連規程等の見直し ・・・・・・・・・・・・・・・・・・・・・・・・ 24

第１章　教育情報セキュリティ基本方針

第１　目的

南知多町立小学校及び中学校（以下「学校」という。）においては、令和元年度以降、ＧＩＧＡスクール構想に基づく１人１台端末の整備、クラウドサービスの活用が進み、個別最適な学びと協働的な学びを充実させることができるようになった。

学校には、児童生徒、保護者、教職員等の個人情報及び学校運営上重要な情報が保管されており、外部への漏洩等が発生した場合は、二次被害も含め、極めて重大な結果を招くおそれがある。

そのため、ＧＩＧＡスクール構想が進展する中で１人１台端末の活用や次世代校務ＤＸの取組が進む中、アクセス権限設定の不徹底や教職員の不注意などの理由で重要性の高い情報を児童生徒が閲覧してしまうような事故が複数発生している。クラウド環境での教育データの利活用を安全に進めていくためには、その前提となる教育現場の情報セキュリティ確保が何より重要である。又、情報セキュリティの確保のためには、何より教育委員会・学校が教育情報セキュリティの考え方について十分に理解していることが不可欠である。

児童生徒等の端末と教職員の端末から得られる各種教育情報を効果的に活用して教育の質的改善を図るため、文部科学省の「教育情報セキュリティポリシーに関するガイドライン（令和７年３月版)」を参考に、南知多町教育委員会において「南知多町教育情報セキュリティポリシー」（以下「ポリシー」という。）を策定するものとする。

第２　用語の定義

１　ネットワーク

学校、教育委員会における学校用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）をいう。

２　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。

３　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う。

４　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。

５　可用性

情報にアクセスすることが認められた者だけが、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。

６　校務系情報

学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

７　校務外部接続系情報

校務系情報のうち、保護者メールや学校ホームページ等の外部とインターネット接続を前

提とした校務で利用される情報をいう。

8　学習系情報

学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教職員及び児童生徒がアクセスすることが想定されている情報をいう。

9　サーバ

ネットワーク上で学校情報を処理し、端末に提供するコンピュータをいう。

10　端末機

ネットワークを通じてサーバに接続されたパソコンやモバイル端末（タブレット等）機器をいう。

11　校務用端末

校務系情報全てにアクセス可能な端末をいう。

12　学習者用端末

学習系情報にアクセス可能な端末で、児童生徒が利用する端末をいう。

13　指導者用端末

学習系情報にアクセス可能な端末で、教職員のみが利用可能な端末をいう。

14　教育情報システム

情報資産を扱うハードウェア、ソフトウェア、クラウドサービス等をいう。

15　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問題としてとらえられる事象（障害、事件、事故、欠陥、攻撃、侵害等）をいう。

16　記録媒体

情報システムでデータ等を記録するための媒体（メディア)。サーバ、端末機、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内臓電磁的記録媒体と、外付けハードディスク、ＣＤ－ＲＯＭ、ＤＶＤ－Ｒ、ＵＳＢメモリ、ＳＤカード等の外部電磁的記録媒体をいう。

17　スマートデバイス

情報処理端末（デバイス）のうち、スマートフォンやタブレット等、携行可能な多機能端末をいう。

18　情報資産

情報システム及びネットワーク並びにこれらで取り扱われる学校情報（これらを印刷したものを含む。）をいう。

19　無線ＬＡＮ

電波等を利用してデータの送受信を行う構内通信網システムをいう。

20　クラウド

学校外、庁舎外でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念をいう。

21　ソーシャルメディアサービス

インターネット上における、ホームページ、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等をいう。

22　教職員

教育委員会所管の学校に勤務する教職員等をいう。

第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、教育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洩・破壊・改ざん・消去、重要情報の搾取、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則違反、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洩・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

第４　適用範囲

ポリシーが対象とする情報資産は、次のとおりとする。

１　ネットワーク及び教育情報システム並びにこれらに関する設備及び記録媒体

２　教育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

第５　教職員等の遵守義務

学校長、教頭、教職員、会計年度任用職員やその他学校に所属する職員（以下「教職員等」という。）は、情報セキュリティについて共通認識を持ち、情報資産の利用にあたっては、関係法令を遵守しなければならない。又、教職員等は、教育情報セキュリティの重要性を認識し、ポリシーを遵守しなければならない。

第６　教育情報セキュリティ対策

情報資産を脅威（第３　対象とする脅威）から保護するため、以下の教育情報セキュリティ対策項講じる。

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　情報資産の分類と管理

学校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　物理的セキュリティ

情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講じる。

４　人的セキュリティ

教育情報セキュリティに関する権限や責任を定めるとともに、全教職員等にポリシーを周知徹底させるための教育及び啓発を行う等の人的な対策を講じる。

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、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の確保等、ポリシーの運用面の対策を講じるものとする。又、自用法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切に対応するため、緊急的対応計画を策定する。

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。

約款による外部サービス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。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、利用できるソーシャルメディアごとの責任者を定める。

第７　情報セキュリティ監査及び自己点検の実施

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

第８　ポリシーの見直し

教育情報セキュリティ監査及び自己点検の結果、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、ポリシーを見直す。

第９　教育情報セキュリティ対策基準の策定

上記第６、第７及び第８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教育情報セキュリティ対策基準を策定する。

第10　教育情報セキュリティ実施手順の策定

教育情報セキュリティ対策基準に基づき、教育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ものとする。

なお、教育情報セキュリティ実施手順は、公にすることにより本町の教育行政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する。

第２章　教育情報セキュリティ対策基準

第１　趣旨

教育情報セキュリティ対策基準とは、教育情報セキュリティ基本方針を実行に移すための、学校における教育情報セキュリティ対策の基準を定めたものである。

第２　組織体制

１　教育情報セキュリティ対策を実施するにあたり、次の表の左欄に掲げる職の職員は、同表右欄に掲げる事務を分掌するものとする。

職	事　務　分　掌
教育長	最高教育情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）として、本町の教育情報セキュリティ対策に関する最終決定を行う。
教育部長	統括教育情報セキュリティ責任者として、CISOを補佐又は代理し、本町の教育情報セキュリティ対策に関する総合調整及び異例な事項についての決定を行う。
教育課長	教育情報セキュリティ・システム責任者として、統括教育情報セキュリティ責任者を補佐又は代理し、本町の教育情報資産に関する教育情報セキュリティ及び情報システムに関する統括的な権限及び責任を有する。
指導主事	統括教育情報セキュリティ管理者として、南知多町立小中学校の教育情報セキュリティ対策に関する統括的な権限及び責任を有する。
南知多町立小中学校長（以下「校長」という。）	教育情報セキュリティ管理者として、該当校の教育情報セキュリティ対策に関する権限及び責任を有する。
教職員	学校が所有する所管する情報資産の取扱者として、校長の指導の下、教育情報セキュリティポリシーを遵守しなければならない。
教育委員会事務局職員	学校の情報資産にアクセスできる立場にあり、教育課長の指導の下、教育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　教育情報セキュリティに関する特に重要な事項については、教育長、教育部長、指導主事、教育課長、校長並びに教育長が必要と認める者が参加する会議等において、審議及び調整等を行うものとする。

３　教育情報セキュリティに関する統一的な窓口の設置

(1)　教育長は、教育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（以下「教育情報セキュリティインシデント」という。）の統一的な窓口の機能を有する組織（以下「統一的な窓口」という。）を整備し、教育情報セキュリティインシデントについて学校等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

(2)　統一的な窓口は教育課に置き、教育長による教育情報セキュリティ戦略の意思決定が行われた際には、その内容を関係する学校等に提供する。

(3)　統一的な窓口は、教育情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

(4)　統一的な窓口は、教育情報セキュリティに関して、関係機関や他の地方公共団体の統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

第３　教育情報資産の分類と管理

１　教育情報資産の分類

教育情報資産は、次の表のとおり分類し、当該分類に基づき教育情報セキュリティ対策を行うものとする。

分類	区分	分　類　基　準
重要性１	最高	ア　個人情報の保護に関する法律（平成１５年法律第５７号）第２条第１項に規定する個人情報 イ　南知多町情報公開条例（平成１２年条例第４２号）第７条に規定する非公開情報
重要性２	高	ア　破壊、改ざん又は滅失等した場合に、教育行政の信頼性を損なうおそれがある情報 イ　破壊、改ざん又は滅失等した場合に、教育行政の円滑な執行を妨げるおそれがある情報
重要性３	中	重要性１及び重要性２以外の情報

２　教育情報資産の管理

(1)　管理責任

ア　教育長は、教育情報システムとその運用管理を定めた南知多町立小中学校の教育情報セキュリティ対策基準を策定しなければならない。

イ　校長は、自校の所管する情報資産について管理責任を有する。

ウ　校長は、教職員の情報資産の取扱いに際し、運用管理について指導しなければならない。

エ　教職員は、南知多町教育情報セキュリティ対策基準（以下「教育情報セキュリティ対策基準」という。）に基づき、適切に教育情報資産を取り扱わなければならない。

(2)　教育情報資産の取扱い

ア　教育情報の作成

(ｱ)　教職員は、業務上必要のない情報を作成してはならない。

(ｲ)　教育情報を作成する教職員は、作成途上の教育情報についても、取扱いを許可されていない者の閲覧や紛失や流出等を防止しなければならない。又、教育情報の作成途上で不要になった場合は、当該教育情報を消去しなければならない。

イ　教育情報資産の入手

(ｱ)　教育情報資産を入手した教職員は、教育情報資産の分類に応じ、適正な取扱いをしなければならない。

(ｲ) 教育情報資産を入手した教職員は、その教育情報資産の分類が不明な場合、校長に判断を仰がなければならない。

ウ　教育情報資産の利用

(ｱ) 教育情報資産を利用する教職員は、業務以外の目的に教育情報資産を利用してはならない。

(ｲ) 教育情報資産を利用する教職員は、教育情報資産の分類に応じ、適正な取扱いをしなければならない。

(ｳ) 教育情報資産を利用する教職員は、電磁的記録媒体又は保存されている領域（フォルダやサーバ）に教育情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体又は保存されている領域を取り扱わなければならない。

(3)　教育情報資産の保管

ア　校長の措置事項

(ｱ) 教育情報資産の保管先を定め、教職員に周知しなければならない。

(ｲ) 教育情報資産を記録したＵＳＢメモリ等の外部電磁的記録媒体を長期保管する場合は、外部電磁的記録媒体への書込禁止の措置を講じなければならない。

(ｳ) 重要性１及び重要性２の教育情報を記録した電磁的記録媒体を保管する場合は、耐火、耐熱、耐水及び耐湿を考慮した施錠可能な場所に保管しなければならない。

イ　教職員の遵守事項

(ｱ) 教職員は、校長が指定した保管先にのみ教育情報資産を保管しなければならない。

(ｲ) 教職員は、児童生徒が生成する学習系情報の保管先について児童生徒に指示し、それ以外の場所に保管しないよう指導しなければならない。

(4)　教育情報の送信

ア　電子メールによる情報の送信

教育情報資産が組織内部（組織が利用するサーバやクラウドサービス等）から組織外部（家庭や地域、事業者等）に電子メール等により外部送信される場合は、教育情報資産分類に応じ以下を実施しなければならない。

(ｱ) 電子メール等により重要性１の情報を外部送信する場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。

(ｲ) 利用する電子メールは、教育委員会から提供される公式サービスのみを利用し、私的に契約したサービスを利用してはならない。

イ　ＦＡＸによる情報の送信

ＦＡＸによる情報の送信は、限定されたアクセスの措置（アクセス制限や暗号化）が不可能であること、誤送信のリスクがあることに鑑み、送信相手がＦＡＸ受信を指定してきた場合にのみ利用することが望ましい。

(5)　教育情報資産の運搬

ア　車両等により重要性１の教育情報資産を運搬する場合は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、教育情報資産の不正利用を防止するための措置を講じなければならない。

イ　重要性１の教育情報資産を運搬する教職員は、学校においては該当校の校長に、そ

れ以外は教育課長に許可を得なければならない。

(6)　教育情報資産の提供、公開

ア　重要性１の教育情報資産を外部（町以外のものをいう。以下同じ。）に提供する場合は、限定されたアクセスの措置設定をしなければならない。

イ　重要性１の教育情報資産を外部に提供する場合は、学校においては該当校の校長に、それ以外は教育課長に許可を得なければならない。

ウ　住民に教育情報資産を公開する場合は、完全性を確保しなければならない。

(7)　教育情報資産の廃棄

ア　教育情報資産を廃棄する教職員は、重要性１以上の情報が記載された紙媒体の書類を廃棄する場合には、内容が復元できないように細断、熔解又はこれに準ずる方法にて廃棄しなければならない。

イ　重要性１及び重要性２の教育情報資産を廃棄する場合で、教育情報を記録している電磁的記録媒体が不要になったときは、電磁的記録媒体の初期化等、教育情報を復元できないように処置した上で廃棄しなければならない。

第４　情報システム全体のセキュリティの向上

１　校務系及び学習系

校務系及び学習系においては、教育情報セキュリティインシデントの早期発見と対処等の教育情報セキュリティ対策を推進しなければならない。

２　校務系と学習系との分離

校務系と学習系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。

３　教育情報のアクセス及び持ち出しにおける対策

(1)　教育情報のアクセス対策

端末（モバイル端末を除く。）が正規の利用者かどうかを判断する認証手段のうち、２つ以上を併用する認証（多要素認証）を利用しなければならない。

(2)　教育情報の持ち出し不可設定

原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの教育情報の持ち出しができないように設定しなければならない。

第５　物理的セキュリティ

１　サーバ等の管理

(1)　機器の取付け

教育課長は、サーバ等の機器の取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、適正に固定する等、外部委託事業者と連携し、必要な措置を講じなければならない。

(2)　サーバの冗長化

ア　教育課長は、重要情報を格納しているサーバ、セキュリティサーバ及びその他の基幹サーバを冗長化し、同一データを保持することが望ましい。

イ　教育課長は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを

起動し、システムの運行停止時間を最小限にすることが望ましい。

(3)　機器の電源

ア　教育課長は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を外部委託事業者と連携し、備え付けなければならない。

イ　教育課長は、落雷等による過電流に対して、外部委託事業者と連携し、サーバ等の機器を保護するための措置を講じなければならない。

(4)　通信ケーブル等の配線

ア　教育課長は、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

イ　教育課長は、許可した以外の者が配線を変更できないように必要な措置を講じなければならない。

(5)　機器の定期保守及び修理

ア　教育課長は、重要性１及び重要性２のサーバ等の機器の定期保守を実施しなければならない。

イ　教育課長は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。ただし、修理を委託する事業者との間で、守秘義務契約を締結し、秘密保持体制の確認等を行った場合はこの限りではない。

(6)　外部委託事業者等のデータセンタ等への機器の設置

教育課長は、外部委託事業者等のデータセンタ等にサーバ等の機器を設置する場合、教育長の承認を得なければならない。又、定期的に当該機器への教育情報セキュリティ対策状況について確認しなければならない。

(7)　機器の廃棄等

教育課長は、機器を廃棄又は、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

２　通信回線の管理

(1)　情報システムに通信回線を接続する場合は、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。又、必要に応じ、送受信される情報の暗号化をしなければならない。

(2)　ネットワークに使用する回線は、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分な教育情報セキュリティ対策を実施しなければならない。

３　職員室等のパソコン等の管理

(1)　教育課長は、不正アクセス防止のため、ログイン時のＩＤパスワードによる認証、多要素認証の実施等、使用する目的に応じた適切な物理的措置を講じなければならない。

電磁的記録媒体については、教育情報が保存される必要がなくなった時点で速やかに記録した教育情報を消去しなければならない。

(2)　教育課長は、特に強固なアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な教育情報資産を取り扱う端末に対し、当該データの暗号化等の措置により、不正アクセスや教職員の不注意等による情報流出への対策を講じなければならない。

(3)　教育課長は、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。

(4)　教育課長は、インターネットへ接続をする場合、教職員のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止するWebフィルタリング等の対策を講じなければならない。

4　１人１台端末におけるセキュリティ

(1)　教育課長は、１人１台端末におけるセキュリティ対策を講じなければならない。

(2)　学習者用端末のセキュリティ対策

ア　授業に支障のないネットワーク構成の選択（帯域や同時接続数など）

教育課長は、クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。又、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

イ　不適切なウェブページの閲覧防止

教育課長は、児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

ウ　マルウェア感染対策

教育課長は、学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

エ　端末を不正利用させないための防止策

教育課長は、端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

オ　セキュリティ設定の一元管理

教育課長は、児童生徒への端末配布後においても、端末のセキュリティ設定やＯＳアップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を一元管理すること。

カ　情報機器の盗難・紛失時の情報漏えい対策

教育課長は、児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏えいを防ぐ等の安全管理措置を講じなければならない。

第６　人的セキュリティ

１　校長の措置事項

(1)　教職員の教育情報セキュリティ意識醸成

ア　校長は、教職員に対して、日頃から教育情報セキュリティに関する話題を積極的に提供し、教育情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

イ　校長は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員が事案を発見した際に、ただちに対処し、すみやかに報告が上がるよう、教職員に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に

努めなければならない。

(2)　教職員への教育情報セキュリティ対策基準の遵守指導

校長は、新規採用教職員、他自治体から本町に新規赴任した教職員、非常勤及び臨時の教職員に対し、遵守すべき内容を理解・浸透するように指導を行わなければならない。

(3)　インターネット接続及び電子メール利用の制限

校長は、教職員に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員に指導しなければならない。

(4)　自己点検の実施

校長は、年１回、学校の自己点検を行わなければならない。

2　教職員の遵守事項

教職員は、校長の指導の下、以下の規定を遵守しなければならない。

(1)　教育情報セキュリティの遵守

教職員は、教育情報セキュリティを遵守しなければならない。又、教育情報セキュリティ対策基準について不明な点、遵守することが困難な点等がある場合は、速やかに校長に相談し、指示を仰がなければならない。

(2)　執務上での管理

ア　執務室の施錠管理

執務室にて教職員が不在となる場合には、執務室を施錠しなければならない。

イ　来校者等への対応

来校者等を執務室に入れる場合には、校長の許可を求めなければならない。

ウ　机上の書類・端末等の管理

教職員は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

(3)　支給端末の取扱い

ア　教職員は、業務目的以外で支給端末を利用してはならない。

イ　教職員は、外部のソフトウェアを無断で支給端末にインストールしてはならない。

ウ　教職員は、支給端末の利用において、下記のカスタマイズを無断でしてはならない。

(ｱ) セキュリティ機能に関する設定変更

(ｲ) メモリ増設等の改造

エ　教職員は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をすること。

オ　業務端末から離れる時は、端末をロックするなど、他者が閲覧できないようにしなければならない。

カ　業務終了後と外出時には、電源を落とさなければならない。

キ　マイナンバーを取り扱う事務について、事務を担当する教職員（以下「事務取扱担当者」という。）は、事務取扱担当者以外の者がマイナンバー情報等を容易に閲覧等できないよう留意しなければならない。

(4)　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

ア　教職員は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則として業務に利用してはならない。ただし、業務上必要な電磁的記録媒体について、校長の許可を得て利用することができる。

イ　教職員は、支給以外の電磁的記録媒体を用いる場合には、校長の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

(5)　モバイル端末や電磁的記録媒体等の持ち出し

教職員は、職員室等のモバイル端末、電磁的記録媒体、教育情報資産及びソフトウェアを外部に持ち出す場合及び外部で情報処理業務を行う場合には、該当校の校長の許可を得なければならない。

(6)　ＩＤの取扱い

教職員は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

ア　自己が利用しているＩＤは、他人に利用させてはならない。

イ　共用ＩＤを利用する場合は、許可された共用ＩＤの利用者以外に利用させてはならない。

(7)　パスワードの取扱い

教職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ　パスワードの文字列は想像しにくいものにしなければならない。

エ　パスワードが流出したおそれがある場合には、パスワードを速やかに変更しなければならない。

(8)　外部電磁的記録媒体の取扱い

ア　利用する外部電磁的記録媒体は教育委員会又は学校から支給された公式の媒体を使用しなければならない。

イ　外部電磁的記録媒体は、職員室の書庫等の鍵のかかる場所に施錠保管しなければならない。

(9)　電子メールの利用制限

ア　教職員は、自動転送機能を用いて、電子メールを転送してはならない。

イ　教職員は、業務上必要のない送信先に電子メールを送信してはならない。

ウ　教職員は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

エ　教職員は、教育課長の許可なくウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。

オ　教職員は、重要な電子メールを誤送信した場合、校長に報告しなければならない。

カ　情報ファイルを添付する場合には、パスワード設定等の対策を講じなければならない。その際、パスワードを同一メールに記載しないこと。

キ　送信時には誤送信を予防するため、送信先のメールアドレス、添付ファイルの内容を確認しなければならない。

ク　差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合には、

添付ファイルの閲覧やリンク先（URL）にアクセスせずに、校長に指示を仰がなければならない。

(10) クラウドサービス、ソーシャルメディアサービス利用制限

ア　私的に契約したクラウドサービスを業務利用してはならない。

イ　ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

(11) 不正プログラム対策に関する教職員の遵守事項

教職員は、不正プログラム対策に関し、次の事項を遵守しなければならない。

ア　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックをしなければならない。

ウ　差出人が不明な電子メールを受信した場合並びに添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックしなければならない。

エ　コンピュータウイルス等の不正プログラムに感染した、又は感染が疑われる場合は、すみやかに校長に報告し、指示を仰がなければならない。又、以下の対応を行わなければならない。

(ｱ) パソコン等の端末の場合

有線ＬＡＮにつながる業務端末の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。

(ｲ) モバイル端末の場合

無線ＬＡＮにつながる業務端末（校務用、指導者及び学習者用端末）の場合は、直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

(ｳ) 指示があるまでは、端末の電源は切らずに保持しなければならない。

(12) 暗号化

ア　教職員は、教育情報資産の分類により、外部に送るデータの機密性又は完全性を確保することが必要な場合には、指定された暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

イ　教職員は、暗号化を行う場合に指定されていない方法を用いてはならない。

(13) 無許可ソフトウェアの導入等の禁止

ア　教職員は、校長の許可なくパソコンやモバイル端末にソフトウェアを導入してはならない。なお、導入する際はソフトウェアのライセンスを管理しなければならない。

イ　教職員は、不正にコピーしたソフトウェアを利用してはならない。

(14) 機器構成の変更の制限

教職員は、校長の許可なくパソコンやモバイル端末に対し機器の改造、増設及び交換を行ってはならない。

(15) 無許可でのネットワーク接続の禁止

教職員は、教育課長の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

(16) 業務以外の目的でのウェブ閲覧の禁止

教職員は、業務以外の目的でウェブを閲覧してはならない。

(17) 児童生徒への指導事項

教職員は、児童生徒に学習者用端末等を利用させるにあたり、以下の事項について指導を行わなければならない。

ア　学習用途の利用限定

学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

イ　利用者認証情報の秘匿管理

ＩＤ及びパスワードは他の人に知られないようにすること。

ウ　ウイルス対策ソフトウェアの管理

ウイルス対策ソフトウェアは常に最新の状態に保つこと。

エ　端末のソフトウェアに関するセキュリティ機能の設定変更禁止

利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

オ　学習系情報保管

学習者用端末へのローカル保存は必要最小限とすること。

カ　無断で外部ソフトウェアをインストール禁止

無断で外部ソフトウェアをインストールしないようにすること。

キ　コミュニケーションツールの利用制限

学校から許可されたコミュニケーションツール（ＳＮＳ、チャット等）のみを利用すること。

ク　ウイルス感染が疑われる場合の報告

学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状がでた場合、すぐに担任教員に報告すること。

ケ　端末は大事に取扱い、盗難・紛失・破損等に注意すること。

コ　私物端末利用禁止

私物端末など承認されていない端末を学校に持ち込んで、学校のネットワークにつながないこと。

(18) 異動・退職時等の遵守事項

教職員は、異動、退職等により業務を離れる場合には、利用していた教育情報資産を、返却しなければならない。

3　教育委員会事務局職員の遵守事項

教育委員会事務局職員は、教育課長の指導の下、以下の規定を遵守しなければならない。

(1)　教育情報セキュリティポリシー等の遵守

(2)　業務以外の目的での使用の禁止

(3)　重要性１及び重要性２の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止

(4)　知り得た情報の秘匿

(5)　業務を離れる場合の遵守事項

異動、退職等により業務を離れる場合には、利用していた情報資産をすべて返却する。又、その後も業務上知り得た情報を漏らさない。

4　研修

(1)　教育情報セキュリティに関する研修

教職員は、定期的に教育情報セキュリティに関する研修に参加しなければならない。

(2)　研修計画の策定及び実施

ア　教育課長は、新規採用の教職員を対象とする教育情報セキュリティに関する研修を実施しなければならない。

イ　教育課長は、校長を含め全ての教職員に対する教育情報セキュリティに関する研修計画の策定と実施計画の構築を定期的に実施しなければならない。

5　教育情報セキュリティインシデントの連絡体制の整備

(1)　教職員は、教育情報セキュリティインシデントを認知した場合、速やかに該当校の校長に報告しなければならない。

(2)　報告を受けた校長は、速やかに指導主事及び教育課長に報告しなければならない。

(3)　指導主事及び教育課長は、当該教育情報セキュリティインシデントについて、必要に応じて教育長に報告するとともに、教育情報セキュリティインシデント原因を究明し、記録を保存しなければならない。又、教育情報セキュリティインシデントの原因究明結果から、再発防止策を検討しなければならない。

第7　技術的セキュリティ

1　コンピュータ等及びネットワークの設定管理

(1)　文書サーバの設定等

ア　教育課長は、教職員が使用できる文書サーバの容量を設定し、教職員に周知しなければならない。

イ　文書サーバは、業務又は学校の単位で構成し、教職員が他の業務又は学校のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

(2)　バックアップの実施

ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、定期的にバックアップを実施しなければならない。

(3)　ログの取得等

ア　教育課長は、重要性1の情報を取り扱う情報システムについて、各種ログ及び教育情報セキュリティの確保に必要な記録を取得し、一定の期間保存することが望ましい。

イ　教育課長は、ログとして取得する項目、保存期間、取得方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理することが望ましい。

ウ　教育課長は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施することが望ましい。

(4)　ネットワークの接続制御、経路制御等

ア　教育課長は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、所管するネットワークの内部におけるファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

イ　教育課長は、不正アクセスを防止するため、所管するネットワークに適正なアクセス制御を施さなければならない。

(5)　外部の者が利用できるシステムの分離等

教育課長は、保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に重要性２以上を扱うシステムとの論理的又は物理的な分離、若しくは各システムにおけるアクセス権管理の徹底を行うこと。

(6)　外部ネットワークとの接続制限等

ア　教育課長は、所管するネットワークを外部ネットワークと接続しようとする場合には、教育長の許可を得なければならない。

イ　教育課長は、接続しようとする外部ネットワークに関するネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の教育情報資産に影響が生じないことを確認しなければならない。

ウ　教育課長は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

エ　教育課長は、情報システムを外部に公開する場合、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

オ　教育課長は、接続した外部ネットワークのセキュリティに問題が認められ、教育情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(7)　複合機のセキュリティ管理

ア　教育課長は、複合機（プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能のうち複数のものが一つにまとめられている機器をいう。以下同じ。）を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う教育情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　教育課長及び校長は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する教育情報セキュリティインシデントへの対策を講じなければならない。

ウ　教育課長は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

(8)　特定用途機器のセキュリティ管理

教育課長は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

(9)　電子メールのセキュリティ管理

ア　教育課長は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバを設定しなければならない。

イ　教育課長は、電子メールの送受信容量の上限及び電子メールボックスの容量を設定しなければならない。

2　アクセス制御

(1)　アクセス制御

教育課長は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員がアクセスできないように、システム上制限しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、当該システムへの認証強度の向上とアクセス権管理を徹底すること。

(2)　外部からのアクセス等の制限

ア　教育課長は、内部のネットワーク又は情報システムに対する外部からのアクセスが必要な場合は、必要最小限の者に限定しなければならない。

イ　教育課長は、民間事業者等の外部組織からのアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る等の措置を講じるとともに、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

ウ　教育課長は、公衆通信回線（公衆無線ＬＡＮ等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、教育情報セキュリティ確保のために必要な措置を講じなければならない。

(3)　認証情報の管理

ア　教育課長は、教職員の認証情報を厳重に管理しなければならない。

イ　教育課長は、認証情報の不正利用を防止するための措置を講じなければならない。

3　システム開発、導入、保守等

(1)　情報システムの調達

教育課長は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

(2)　情報システムの開発

ア　情報システム開発における責任者及び作業者の特定

教育課長は、情報システム開発の責任者及び作業者を特定しなければならない。

イ　情報システム開発における責任者、作業者のＩＤの管理

(ｱ) 教育課長は、情報システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

(ｲ) 教育課長は、情報システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

ウ　情報システム開発に用いるハードウェア及びソフトウェアの管理

(ｱ) 教育課長は、情報システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(ｲ) 教育課長は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアを情報システムから削除しなければならない。

(3)　情報システムの導入

ア　教育課長は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験をしなければならない。

イ　教育課長は、運用テストを行う場合、あらかじめ擬似環境による操作確認をしなければならない。

ウ　教育課長は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

エ　教育課長は、開発した情報システムについて受入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

(4)　情報システム開発及び保守に関連する資料等の整備・保管

ア　教育課長は、情報システム開発及び保守に関連する資料及び情報システム関連文書を適正に整備・保管しなければならない。

イ　教育課長は、テスト結果を一定期間保管しなければならない。

ウ　教育課長は、情報システムに係るソースコード及び使用したオープンソースのバージョン（リポジトリ）を適正な方法で保管しなければならない。

(5)　情報システムにおける入出力データの正確性の確保

ア　教育課長は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

イ　教育課長は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ　教育課長は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6)　情報システムの変更管理

教育課長は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(7)　開発及び保守用のソフトウェアの更新等

教育課長は、開発及び保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8)　情報システム更新又は統合時の検証等

教育課長は、情報システム更新又は統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証をしなければならない。

4　不正プログラム対策

教育課長は、不正プログラム対策として、次の事項を措置しなければならない。

(1)　外部ネットワークにより受信するファイルは、コンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

(2)　サーバ及びパソコン等の端末（モバイル端末を除く。）は、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させ、ソフトウェア及びパターンファイルは、常に最新の状態に保たなければならない。又、インターネットに接続していないパソコ

ン等の端末についても、感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

(3)　パソコン等の端末（モバイル端末を除く。）に対する不正プログラム対策ソフトウェアによるフルチェックは、定期的に実施しなければならない。

(4)　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員に対して注意喚起しなければならない。

(5)　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

5　不正アクセス対策

(1)　攻撃への対処

教育課長は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。又、関係機関と連絡を密にして情報の収集に努めなければならない。

(2)　サービス不能攻撃

教育課長は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(3)　標的型攻撃

教育課長は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の対策を講じなければならない。又、通信をチェックする等の内部対策を講じなければならない。

6　セキュリティ情報の収集

(1)　セキュリティホール等に関する情報の収集及び共有並びにソフトウェアの更新等

教育課長は、セキュリティホール等に関する情報を収集し、必要に応じ、関係者間で共有しなければならない。又、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(2)　教育情報セキュリティに関する情報の収集及び共有

教育課長は、教育情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。又、教育情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第８　運用

1　情報システムの監視

教育課長は、セキュリティに関する侵害を検知するため、情報システムを監視しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、侵入検知システム（ＩＤＳ）や侵入防御システム（ＩＰＳ）などの対策を講じなければならない。

2　ドキュメントの管理

(1)　システム管理記録及び作業の確認

ア　教育課長は、情報システムの運用において実施した作業について、作業記録を作成しなければならない。

イ　教育課長は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

ウ　システム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

(2)　情報システム仕様書等の管理

教育課長は、ネットワーク構成図、情報システム仕様書について記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

(3)　障害記録の管理

教育課長は、教職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

(4)　記録の保存

教育課長は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

3　教職員のＩＤ及びパスワードの管理

(1)　教育課長は、利用者の登録、変更、抹消等の教育情報管理、教職員の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

(2)　教育課長は、利用されていないＩＤが放置されないよう、点検しなければならない。

4　特権を付与されたＩＤの管理等

(1)　教育課長は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

(2)　教育課長は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

5　教育情報セキュリティポリシーの遵守状況の確認・管理

(1)　遵守状況の確認及び対処

教育課長及び校長は、教育情報セキュリティポリシーの遵守状況について確認を行い、問題が発生した場合には、適正かつ速やかに対処しなければならない。

(2)　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

教育課長は、不正アクセス、不正プログラム等の調査のため必要がある場合は、職員が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(3)　業務以外の目的でのウェブ閲覧の禁止

教育課長は、教職員のウェブ利用について、明らかに業務に関係のないサイトを閲覧

していることを発見した場合は、該当校の校長に通知し適正な措置を求めなければならない。

(4)　教職員による不正アクセスの管理

教育課長は、教職員による不正アクセスを発見した場合は、該当校の校長に通知し、適正な処置を求めなければならない。

6　専門家の支援体制等

(1)　専門家の支援体制

教育課長は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

(2)　他団体との情報システムに関する情報等の交換

他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、教育課長の許可を得なければならない。

7　侵害時の対応等

(1)　実施手順の策定

教育課長は、教育情報セキュリティインシデント、教育情報セキュリティポリシーの違反、自然災害、大規模又は広範囲にわたる疫病等により教育情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合の連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するため、あらかじめ実施手順を定めるとともに、セキュリティ侵害時には当該手順に従って適正に対処しなければならない。

(2)　実施手順に盛り込むべき内容

実施手順には、以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

(3)　実施手順の見直し

教育情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて実施手順を見直さなければならない。

(4)　実施手順の公開

実施手順の内、公にすることにより本市の教育情報セキュリティ対策に重大な支障を及ぼすおそれがある事項については、非公開とする。

8　例外措置

(1)　例外措置の許可

教育課長は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、教育長の許可を得て、例外措置を講じることができる。

(2)　緊急時の例外措置

教育課長は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施する

ことができないときは、事後速やかに教育長に報告しなければならない。

9　法令遵守

教職員は、職務の遂行において使用する教育情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

(1)　地方公務員法（昭和25年法律第261号）
(2)　教育公務員特例法（昭和24年法律第１号）
(3)　著作権法（昭和45年法律第48号）
(4)　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
(5)　個人情報の保護に関する法律
(6)　サイバーセキュリティ基本法（平成26年法律第104号）
(7)　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）

第９　外部サービスの利用

1　外部委託

(1)　外部委託事業者の選定基準

教育課長は、外部委託事業者の選定に当たり、委託内容に応じた教育情報セキュリティ対策が確保されることを確認しなければならない。

(2)　契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の教育情報セキュリティ要件を明記した契約を締結しなければならない。

ア　教育情報セキュリティポリシー及び教育情報セキュリティ実施手順の遵守
イ　外部委託事業者の責任者、委託内容、作業者、作業場所の特定
ウ　提供されるサービスレベルの保証
エ　外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
オ　外部委託事業者の従業員に対する教育の実施
カ　提供された情報の目的外利用及び受託者以外の者への提供の禁止
キ　業務上知り得た情報の守秘義務
ク　再委託に関する制限事項の遵守
ケ　委託業務終了時の教育情報資産の返還、廃棄等
コ　委託業務の定期報告及び緊急時報告義務
サ　教育委員会による監査、検査
シ　教育委員会による教育情報セキュリティインシデント発生時の公表
ス　教育情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

(3)　確認、措置等

教育課長は、外部委託事業者において必要な情報セキュリティ対策が確保されていることを必要に応じ確認し、契約に基づき措置を実施しなければならない。

(4)　外部委託事業者に対する説明

教育情報ネットワーク及び情報システムの開発、保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、教育情報セキュリティポリシー等のうち外部委託事業者が守るべき内容及び機密事項等を説明し、遵守させなけれ

ばならない。

2　約款による外部サービスの利用

(1)　約款による外部サービスの利用に係る規定の整備

教育課長は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。又、当該サービスの利用において、重要性２以上の情報が取り扱われないように規定しなければならない。

ア　約款によるサービスを利用して良い範囲

イ　業務により利用する約款による外部サービス

ウ　利用手続及び運用手順

(2)　約款による外部サービスの利用における対策の実施

教職員は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

3　ソーシャルメディアサービスの利用

(1)　教育課長は、教育委員会が管理するアカウントでソーシャルメディアサービスを利用する場合、教育情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

ア　教育委員会のアカウントによる情報発信が、実際の教育委員会のものであることを明らかにするために、教育委員会の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

イ　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ＩＣカード等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

(2)　重要性２以上の情報はソーシャルメディアサービスで発信してはならない。

(3)　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なければならない。

4　クラウドサービスの利用

(1)　教育課長は、クラウドサービスを利用する場合、取り扱う教育情報資産の分類を踏まえ、情報の取扱いをゆだねることの可否を判断しなければならない。

(2)　教育課長は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法、裁判管轄を指定しなければならない。

(3)　教育課長は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件としなければならない。

(4)　教育課長は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。

(5)　教育課長は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定、認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的、客観的に評価し判断しなければならない。

第１０　評価、見直し

１　監査

(1)　実施方法

教育委員会（外部委託事業者及び再委託事業者を含む。）は、ネットワーク及び情報システム等の教育情報資産における教育情報セキュリティ対策状況について、必要に応じて監査を行うものとする。

(2)　監査を行う者の要件

ア　教育委員会（外部委託事業者及び再委託事業者を含む。）は、被監査部門から独立した者に対して、監査の実施を依頼するものとする。

イ　監査を行う者は、監査及び教育情報セキュリティに関する専門知識を有する者とする。

(3)　保管

監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書は、紛失等が発生しないように適正に保管するものとする。

(4)　監査結果への対応

教育課長及び校長は、監査結果に対応しなければならない。

(5)　本基準及び関連規程等の見直し等への活用

監査結果は、本基準及び関連規程等の見直し、その他教育情報セキュリティ対策の見直し時に活用しなければならない。

２　自己点検

(1)　実施方法

教育課長は、ネットワーク及び情報システムについて教育情報セキュリティポリシーに沿った教育情報セキュリティ対策状況について、必要に応じて自己点検を実施するものとする。

(2)　自己点検結果の活用

ア　教職員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　点検結果は、本基準及び関連規程等の見直し、その他教育情報セキュリティ対策の見直し時に活用しなければならない。

３　本基準及び関連規程等の見直し

教育情報セキュリティ監査及び自己点検の結果並びに教育情報セキュリティに関する状況の変化等を踏まえ、本基準及び関係規程等について必要があると認めた場合、改善を行うものとする。

附　則

この基準は、令和８年４月１日から施行する。