松前町立小中学校
情報セキュリティポリシー

松前町教育委員会

令和５年３月23日制定

目次

序　松前町立小中学校情報セキュリティポリシーの構成

情報セキュリティポリシーとは、組織において保有する情報資産に関する情報セキュリティ対策について、総合的及び体系的に取りまとめたものである。この情報セキュリティポリシーは、組織が保有する情報資産に関する業務に携わる全ての教職員に浸透させ、普及させ、及び定着させるものであり、安定的な規範であることが要請されるとともに、技術の進歩等に伴う情報セキュリティ対策を取り巻く急速な状況の変化に対応することが必要である。

そのため、松前町立小中学校情報セキュリティポリシー（以下「本ポリシー」という。）は、一定の普遍性を備えた情報セキュリティ基本方針及び情報資産を取り巻く状況の変化に適切に対応するための情報セキュリティ対策基準の２階層に分け、それぞれ策定することとする。

本ポリシーの構成

本ポリシー	内容
情報セキュリティ基本方針	学校における情報セキュリティ対策の基本的な考え方を定めるもの
情報セキュリティ対策基準	情報セキュリティ基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めるもの

第１章　情報セキュリティ基本方針

１　目的

松前町立小中学校（以下「学校」という。）の情報システムで取り扱われる情報には、児童生徒の個人情報や学校運営上重要な情報など、外部に漏えいした場合に極めて重大な被害をもたらすおそれがある情報が多数含まれていることから、情報資産、情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、児童生徒の財産及びプライバシーを守るため、かつ、学校の安定的な運営のために必要不可欠であり、ひいては、町民からの町教育に対する信頼の維持向上に寄与するものである。そのため、本ポリシーのうち、情報セキュリティ基本方針では、本ポリシーの対象範囲、情報資産の取扱いその他情報セキュリティ対策の基本的な事項について定めるものとする。

２　定義

(1) ネットワーク

松前町教育委員会（以下「教育委員会」という。）が管理しているコンピュータを相互に接続するための通信網並びにその通信網を構成する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) 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。

(5) 完全性

情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

(6) 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。

(7) 校務ネットワーク接続系

校内LANにより、愛媛スクールネット（以下「Esnet」という。）を経由してインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(8) 学習ネットワーク接続系

校内LANにより、Esnetを経由せずにインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(9)通信経路の分割

校務ネットワーク接続系と学習ネットワーク接続系の両環境間の通信環境を分離することをいう。

3　情報資産への脅威

情報資産への脅威として、次に掲げる事項が想定されるため、６の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、重要情報の詐取又は内部不正

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用その他情報資産の取扱いに関する規定違反、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、委託管理の不備、マネジメントの欠陥、機器故障の非意図的要因による情報資産の漏えい・破壊・消去

(3) 地震、落雷、火災その他の災害によるサービス及び業務の停止

(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

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等による波及

4　適用範囲

(1) 組織の範囲

情報セキュリティ基本方針が適用される組織は、学校とする。

(2) 情報資産の範囲

情報セキュリティ基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備並びに電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した書面を含む。）

ウ　情報システムの仕様書、ネットワーク図等のシステム関連文書

5　教職員の義務

教職員及び委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって、本ポリシーを遵守する義務を負うものとする。

6　情報セキュリティ対策

教育長は、３に掲げる脅威から、４に定める情報資産を保護するため、次の対策を講ずるものとする。

(1) 組織体制

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ものとする。

(2) 情報資産の分類と管理

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行うものとする。

(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、業務の効率性及び利便性の観点を踏まえつつ、情報システム全体に対し次の対策を講ずるものとする。

ア　校務ネットワーク接続系においては、通信経路の分割を行い、端末からの情報の持ち出しを不可とする設定及び端末へログインする際の認証システムの導入により、情報の流出を防ぐ。

イ　学習ネットワーク接続系においては、通信経路の分割を行い、不正通信の監視機能

を持ったソフトウェアの導入により、情報の流出を防ぐ。

(4) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入りを防ぐため、及び情報資産への損傷・妨害から情報資産を保護するため、物理的な対策を講ずるものとする。

(5) 人的セキュリティ対策

情報セキュリティに関し、教職員及び委託事業者が遵守すべき事項を明確に定めるとともに、教職員及び委託事業者に対し、十分な教育、啓発及び訓練を行えるよう人的な対策を講ずるものとする。

(6) 技術的セキュリティ対策

情報資産へのアクセス制御、ネットワーク管理及び不正プログラム対策、不正アクセス対策等の技術的な対策を講ずるものとする。

(7) 運用

ア　情報システムの監視、本ポリシーの遵守状況の確認その他の情報セキュリティの運用面の対策を講ずるものとする。

イ　情報資産に対するセキュリティ侵害が発生した場合に迅速かつ適切に対応するため、情報セキュリティインシデント発生時の対応手順書を策定するものとする。

(8) 業務委託及び外部サービスの利用

ア　業務委託を行う場合には、情報セキュリティ要件を明記した契約を締結し、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かどうかを確認の上、必要に応じて当該契約に基づく措置を講ずるものとする。

イ　外部サービスを利用する場合には、利用するサービスの約款等を確認し、必要な情報セキュリティ対策を講ずるものとする。

7　情報セキュリティ監査及び自己点検の実施

教育長は、本ポリシーが遵守されていることを検証するため、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するものとする。

8　評価及び見直しの実施

教育長は、情報セキュリティ監査及び自己点検の結果、本ポリシーの見直しが必要となった場合又は情報資産を取り巻く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、本ポリシーの見直しを行うものとする。

9　情報セキュリティ対策基準の策定

教育長は、６から８までに規定する情報セキュリティ対策等を実施するため、具体的な遵守事項及び判断基準を明記した情報セキュリティ対策基準を策定するものとする。

10　情報セキュリティ実施手順の策定

教育長は、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するものとする。ただし、情報セキュリティ実施手順については、公にすることにより学校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、非公開とする。

第２章　情報セキュリティ対策基準

１　適用範囲

情報セキュリティ対策基準の適用範囲は、学校の教職員とする。

２　組織体制

情報セキュリティ対策を実施するための組織体制は、次のとおりとする。

(1) 最高情報セキュリティ責任者

教育長を最高情報セキュリティ責任者とする。最高情報セキュリティ責任者は、学校における全ての情報資産の情報セキュリティ対策に関する最終決定権限及び責任を有する。

(2) 情報セキュリティ責任者

ア　教育委員会事務局の長を情報セキュリティ責任者とする。情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐する。

イ　情報セキュリティ責任者は、学校の全てのネットワークにおける開発、設定の変更、運用、見直しを行う権限及び責任を有する。

ウ　情報セキュリティ責任者は、学校の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

エ　情報セキュリティ責任者は、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

オ　情報セキュリティ責任者は、学校の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置をとる権限及び責任を有する。

カ　情報セキュリティ責任者は、学校の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持及び管理を行う権限並びに責任を有する。

キ　情報セキュリティ責任者は、緊急時の円滑な情報共有を図るため、最高情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を整備しなければならない。

ク　情報セキュリティ責任者は、緊急時には最高情報セキュリティ責任者に早急に報告を行うとともに、事態の回復のための対策を行わなければならない。

ケ　情報セキュリティ責任者は、学校において所有している情報システムについて、緊急時における連絡体制の整備、本ポリシーの遵守に関する意見の集約並びに教職員に対する教育、訓練、助言及び指示を行う。

(4) 情報セキュリティ管理者

ア　各学校の校長を情報セキュリティ管理者とする。

イ　情報セキュリティ管理者は、所管する学校等の情報セキュリティ対策に関する権限及び責任を有する。

ウ　情報セキュリティ管理者は、所管する学校等において情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者及び最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

(5) 情報システム管理者

ア　学校の情報システムを所管する課の長を当該情報システムに関する情報システム管理者とする。

イ　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直しを行う権限及び責任を有する。

ウ　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

エ　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持及び管理を行う。

(6) 情報システム担当者

情報システム管理者の指示に従い、情報システムの開発、設定の変更、運用、見直しの作業を行う職員を情報システム担当者とする。

(7) 情報セキュリティインシデントに関する統一的な窓口

ア　情報セキュリティ担当部局の課を情報セキュリティインシデントの統一的な窓口とする。

イ　情報セキュリティインシデントの統一的な窓口は、情報セキュリティインシデントの発生に関する予兆の検知及び発見並びに内外からのセキュリティ事故に関する連絡、報告の受付を行う。

(8) 兼務の禁止

ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

イ　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

【管理体制図】

最高情報セキュリティ責任者	教育長
情報セキュリティ責任者	教育委員会事務局の長
情報セキュリティ管理者	各学校の校長
情報システム管理者	情報システムを所管する課の長
情報システム担当者	情報システムの運用等を担当する職員
情報セキュリティインシデントに関する統一的な窓口	情報セキュリティを所管する課

3　情報資産の分類及び管理

(1) 情報資産の分類

情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

ア　機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産 ・特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの	・教育委員会が配置したもの以外のパソコン及びモバイル端末での作業禁止（機密性３の情報資産に対する取扱） ・必要以上の複製及び配付の禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体の持ち込みの禁止 ・情報の送信並びに情報資産の運搬及び提供時における暗号化、パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産 ・教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む）	
機密性１	機密性２又は機密性３の情報資産以外の情報資産 ・公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む）	

イ　完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場

	確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	所への保管
完全性１	完全性２情報資産以外の情報資産	

ウ　可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	

(2) 情報資産の管理

ア　管理責任

(ｱ) 情報資産は、情報セキュリティ管理者がそれぞれ所管する情報資産について管理責任を有する。

(ｲ) 情報資産が複製又は伝送された場合には、当該複製等も原本と同様に管理しなければならない。

イ　情報資産の分類の表示

教職員は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダ・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

ウ　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) 情報を作成する者は、情報の作成時に情報資産の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ) 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

エ　情報資産の入手

(ｱ) 教職員が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(ｲ) 教職員以外の者が作成した情報資産を入手した者は、情報資産の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ) 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリ

ティ管理者に判断を仰がなければならない。

オ　情報資産の利用

(ｱ) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(ｲ) 情報資産の利用においては、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) 情報資産を利用する者は、電磁的記録媒体又は紙媒体に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を取り扱わなければならない。

カ　情報資産の保管

(ｱ) 情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に基づいて、情報資産を適正に保管しなければならない。

(ｲ) 情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

(ｳ) 情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

キ　情報の送信

電子メールにより機密性２以上の情報の送信をする者は必要に応じパスワード等による暗号化を行なわなければならない。

ク　情報資産の運搬

(ｱ) 機密性２以上の情報資産を運搬する者は、必要に応じて鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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) 機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

ケ　情報資産の提供・公表

(ｱ) 機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

(ｲ) 機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

(ｳ) 情報セキュリティ管理者は、外部に公開する情報資産について、完全性を確保しなければならない。

コ　情報資産の廃棄及び機器のリース返却

(ｱ) 情報資産の廃棄や機器のリース返却を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(ｲ) 情報資産の廃棄や機器のリース返却を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ｳ) 情報資産の廃棄や機器のリース返却を行う者は、情報セキュリティ管理者の許可

を得なければならない。

4　情報システム全体の強じん性の向上

(1) 校務ネットワーク接続系

校務ネットワーク接続系と学習ネットワーク接続系は、両環境間の通信環境を分離しなければならない。

(2) 学習ネットワーク接続系

インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見、対処及びEsnet への不適切なアクセスの監視等の情報セキュリティ対策を講じなければならない。

5　物理的セキュリティ

(1) サーバ等の管理

ア　機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、ほこり、振動、温度、湿度の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等必要な措置を講じなければならない。

イ　サーバ等の冗長化

情報システム管理者は、重要情報を格納しているサーバ等について冗長化し、同一データを保持する対策を行わなければならい。

ウ　機器の電源

(ｱ) 情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、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、当該機器が適切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備え付けなければならない。

(ｲ) 情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、落雷等による過電流に対して、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。

エ　通信ケーブル等の配線

(ｱ) 情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷を防止するために、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) 情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷の報告があった場合、連携して対応しなければならない。

(ｳ) 情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

(ｴ) 情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できな

いように必要な措置を講じなければならない。

オ　機器の定期保守及び修理

(ｱ) 情報システム管理者は、可用性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) 情報システム管理者は、電磁的記録媒体を内蔵する機器を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。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持に関する体制の確認を行わなければならない。

カ　施設外への機器の設置

情報セキュリティ責任者及び情報システム管理者は、施設外にサーバ等の機器を設置する場合、最高情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への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。

キ　機器の廃棄及びリース返却

情報システム管理者は、機器を廃棄、リース返却を行う場合、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) 通信回線及び通信回線装置の管理

ア　情報セキュリティ責任者は、施設内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

イ　情報セキュリティ責任者は、 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

ウ　情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、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。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

エ　情報セキュリティ責任者は、ネットワークに使用する回線について、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セキュリティ対策を実施しなければならない。

オ　情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

(3) 教職員の使用するパソコン又はモバイル端末及び電磁的記録媒体等の管理

ア　情報セキュリティ管理者は、盗難防止のため、パソコンを使用する執務室等の施錠、モバイル端末を充電する保管庫の施錠、電磁的記録媒体の使用時以外の施錠管理等の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、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情報を消去しなければならない。

イ　情報システム管理者は、情報システムへのログインに際し、パスワード等の認証情報の入力を必要とするように設定しなければならない。

ウ　情報システム管理者は、必要に応じて、パソコン又はモバイル端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用するものとする。

エ　情報システム管理者は、パソコン又はモバイル端末におけるデータの暗号化の機能を有効に利用しなければならない。また、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

オ　情報セキュリティ管理者は、パソコン又はモバイル端末を庁外で業務利用する場合は、上記対策に加え、端末の紛失・盗難対策として、普段からパスワードによる端末ロックを設定しておかなければならない。

(4)　校内 LAN 接続について

ア　情報セキュリティ責任者は、パソコン又はモバイル端末の通信機器等が、校内 LAN に接続されないよう措置を講じなければならない。

イ　情報セキュリティ責任者は、教育委員会が配置したパソコン又はモバイル端末以外のモバイル端末等がネットワークに接続できないよう、ネットワーク接続用 ID・パスワードを設定しなければならない。

６　人的セキュリティ

(1) 教職員の遵守事項

ア　教職員の遵守事項

(ｱ) 本ポリシー等の遵守

教職員は、本ポリシーを遵守しなければならない。また、情報セキュリティ対策について不明な点及び遵守することが困難な点がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

(ｲ) 業務以外の目的での使用の禁止

教職員は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

(ｳ) パソコン又はモバイル端末及び電磁的記録媒体の持ち出し並びに外部における情報処理作業の制限

a　教職員は、パソコン、モバイル端末、電磁的記録媒体、情報資産及びソフトウエアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

b　教職員は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

(ｴ) 教育委員会が配置したもの以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用

a　教職員は、教育委員会が配置したもの以外のパソコン、モバイル端末及び電磁的記録媒体を原則業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ責任者の許可を得て利用することができる。

b　教職員は、教育委員会が配置したパソコン、モバイル端末及び電磁的記録媒体

を用いる場合において、当該利用が外部で情報処理作業を行うものであるときは、機密性３の情報資産を扱ってはならない。

(ｵ) 持ち出しの記録

情報セキュリティ管理者は、パソコン、モバイル端末及び電磁的記録媒体の持ち出しについて、記録を作成し、保管しなければならない。

(ｶ) パソコン及びモバイル端末におけるセキュリティ設定変更の禁止

教職員は、パソコン及びモバイル端末のソフトウエアに関するセキュリティ機能の設定を情報システム管理者の許可なく変更してはならない。

(ｷ) 机上の端末等の管理

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について、第三者に使用されること又は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、離席時のパソコン及びモバイル端末のロック、又は電磁的記録媒体及び文書の容易に閲覧されない場所への保管等適正な措置を講じなければならない。

(ｸ) 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、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

イ　非常勤職員及び会計年度任用職員への対応

(ｱ) 本ポリシー等の遵守

情報セキュリティ管理者は、非常勤職員及び会計年度任用職員に対し、本ポリシー等のうち、非常勤職員及び会計年度任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

(ｲ) インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤職員及び会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続、電子メール及び校内 LAN の使用が不要の場合、これを利用できないようにしなければならない。

ウ　本ポリシー等の掲示

情報セキュリティ管理者は、教職員が常に本ポリシー及び情報セキュリティ実施手順を閲覧できるよう掲示に努めなければならない。

エ　委託事業者に対する説明

情報システム管理者は、ネットワーク及び情報システムの開発並びに保守等を事業者に発注する場合、再委託事業者も含めて、本ポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(2) 研修・訓練

ア　情報セキュリティに関する研修・訓練

情報セキュリティ管理者は、定期的に情報セキュリティに関する研修及び訓練の実施に努めなければならない。

イ　研修計画の策定及び実施

(ｱ) 情報セキュリティ管理者は、教職員を対象とする情報セキュリティに関する研修計画を定期的に策定しなければならない。

(ｲ) 情報セキュリティ管理者は、毎年度、新規採用の教職員を対象とする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。

(ｳ) 研修は、受講する教職員それぞれの役割や情報セキュリティに関する理解度に応じたものにしなければならない。

ウ　緊急時対応訓練

情報セキュリティ管理者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるようにしなければならない。

エ　研修・訓練への参加

全ての教職員は、情報セキュリティに関する意識を深め情報セキュリティ上の問題がないようにするため、定められた研修及び訓練に参加しなければならない。

(3) 情報セキュリティインシデントの報告

ア　情報セキュリティインシデントの報告

(ｱ) 教職員は、情報セキュリティインシデントを発見した場合、又は住民等外部から報告を受けた場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

(ｲ) 報告を受けた情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、当該情報セキュリティインシデントの重要性又は緊急性によって、最高情報セキュリティ責任者に報告しなければならない。

イ　情報セキュリティインシデント原因の究明・記録、再発防止等

(ｱ) 括情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした学校の情報セキュリティ管理者、情報システム管理者及び情報セキュリティインシデントの統一的な窓口と連携し、当該セキュリティインシデントの原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。

(ｲ) 最高情報責任者は、情報セキュリティ責任者から情報セキュリティインシデントについて報告を受けた場合は、再発防止策を実施するために必要な措置を指示しなければならない。

(4) ID及びパスワード等の管理

ア　IDの取扱い

教職員は、自己が管理する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、共用IDの利用者以外に利用させてはならない。

イ　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) パスワードは秘密にし、パスワードの照会等には一切応じてはならない。
(ｳ) パスワードは十分な長さとし、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、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
(ｵ) 複数の情報システムを扱う教職員は、同一のパスワードをシステム間で用いてはならない。
(ｶ) 仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
(ｷ) サーバ、ネットワーク機器及びパソコン等の端末は、パスワードを記憶させてはならない。
(ｸ) パスワード（共有 ID に対するパスワードを除く）は教職員間で共有してはならない。

7 技術的セキュリティ

(1) コンピュータ及びネットワークの管理

ア ファイルサーバの設定等

情報システム管理者は、情報を共有するためのファイルサーバを設置する場合、次の事項を守らなければならない。

(ｱ) 教職員が使用できるファイル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) ファイルサーバを学校等の単位で構成し、教職員が他校のフォルダ及びファイルを閲覧し、及び使用することができないように設定しなければならない。
(ｳ) 特定の教職員のみが取り扱う権限を持つデータについて、同一校であっても、教職員以外の教職員が閲覧及び使用できないようにしなければならない。

イ バックアップの実施

情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ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。

ウ 他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウエアを交換する場合、情報セキュリティ責任者の許可を得なければならない。

エ システム管理記録及び作業の確認

(ｱ) 情報システム管理者は、所管する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) 情報システム管理者は、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) 情報システム管理者又は情報システム担当者及び契約により操作を認められた委託事業者が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。

オ　情報システム仕様書等の管理

情報システム管理者は、所管するシステムの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、紛失したりすること等がないよう、適正に管理しなければならない。

カ　ログの取得等

(ｱ) 情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

(ｲ) 情報システム管理者は、ログとして取得する項目、保存期間、取扱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、適正にログを管理しなければならない。

(ｳ) 情報セキュリティ責任者及び情報システム管理者は、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しなければならない。

キ　障害記録

情報セキュリティ責任者及び情報システム管理者は、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。

ク　ネットワークの接続制御及び経路制御等

(ｱ) 情報セキュリティ責任者は、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、ファイアウォール、ルータ等の通信ソフトウエア等を設定しなければならない。

(ｲ) 情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

ケ　外部ネットワークとの接続制限等

(ｱ) 情報システム管理者は、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、最高情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

(ｲ) 情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成及び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及び情報システム等の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) 情報システム管理者は、接続した外部ネットワークの瑕疵（かし）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) 情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、ネットワークへの侵入を防御するために、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) 情報システム管理者は、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、情報資産に脅威が生じることが想定される場合には、情報セキュリティ責任者の判断に従い、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。

コ　無線 LAN 及びネットワークの盗聴対策

(ｱ) 情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

(ｲ) 情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

サ　無許可ソフトウエアの導入等の禁止

(ｱ) 教職員は、パソコンやモバイル端末に無断でソフトウエアを導入してはならない。

(ｲ) 情報セキュリティ管理者は、業務を円滑に遂行するために必要なソフトウエアがある場合は、情報セキュリティ責任者の許可を得て導入することができる。

(ｳ) 教職員は、不正にコピーしたソフトウエアを利用してはならない。

シ　機器構成の変更の制限

(ｱ) 教職員は、パソコン及びモバイル端末に対して、機器の改造、増設及び交換を行ってはならない。

(ｲ) 情報セキュリティ管理者は、業務を円滑に遂行するためにパソコンやモバイル端末に対して、機器の改造、増設及び交換を行う必要がある場合は、情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

ス　業務外でのネットワークへの接続の禁止

(ｱ) 教職員は、教育委員会が配置した端末を、有線であるか無線であるかを問わず、その端末を接続して利用するよう情報セキュリティ責任者及び情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

(ｲ) 情報セキュリティ責任者は、教育委員会が配置した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限するよう努めなければならない。

セ　業務以外の目的でのウェブ閲覧の禁止

(ｱ) 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。

(ｲ) 情報セキュリティ責任者は、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、情報セキュリティ管理者に通知し適切な措置を求めなければならない。

ソ　Web 会議サービスの利用時の対策

(ｱ) 教職員は、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

(ｲ) 教職員は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を行うこと。

(2) アクセス制御

ア　アクセス制御等

(ｱ) アクセス制御

情報セキュリティ責任者又は情報システム管理者は、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。

(ｲ) 利用者 ID の取扱い

a　情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、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。

b　情報セキュリティ管理者は、所属する教職員の利用者登録が業務上不要となった場合は、情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

c　情報セキュリティ責任者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

(ｳ) 特権を付与された ID の管理等

a　情報セキュリティ責任者及び情報システム管理者は、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。

b　情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、情報セキュリティ責任者及び情報システム管理者が指名し、最高情報セキュリティ責任者が認めた者でなければならない。

c　情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

d　情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、教職員の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

e　情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

イ　教職員による外部からのアクセス制限

(ｱ) 教職員は、外部から内部のネットワーク又は情報システムにアクセスする場合、情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

(ｲ) 情報セキュリティ責任者及び情報システム管理者は、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を、最低限の者に限定しなければならない。

(ｳ) 情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

(ｴ) 情報セキュリティ責任者は、外部からのアクセスを認める場合、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。

(ｵ) 情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を教職員に貸与する場合、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。

(ｶ) 教職員は、持ち込んだ又は外部から持ち帰ったモバイル端末をネットワークに接続する前に、コンピュータウイルスに感染していないこと及びパッチの適用状況等を確認し、情報セキュリティ管理者の許可を得て接続しなければならない。

(ｷ) 情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを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、パスワード及び生体認証に係る情報等の認証情報並びに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、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。

ウ　自動選別の設定

情報セキュリティ責任者及び情報システム管理者等は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定するなど、不正な機器がネットワークに接続されないための必要な措置を講ずるよう努めなければならない。

エ　ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員がログインしたことを確認することができるようシステムを設定しなければならない。

オ　認証情報の管理

(ｱ) 情報セキュリティ責任者又は情報システム管理者は、教職員の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

(ｲ) 情報セキュリティ責任者又は情報システム管理者は、教職員のパスワードを発行する場合において、仮のパスワードを発行する場合、ログイン後直ちに仮のパスワードを変更させなければならない。

(ｳ) 情報セキュリティ責任者又は情報システム管理者は、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。

カ　特権による接続時間の制限

情報システム管理者は、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。

(3) システム開発、導入及び保守等

ア　情報システムの調達

(ｱ) 情報セキュリティ責任者及び情報システム管理者は、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。

(ｲ) 情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウエアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題

のないことを確認しなければならない。

イ　情報システムの開発

(ｱ) システム開発における責任者及び作業者の特定

情報システム管理者は、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) システム開発における責任者及び作業者の ID の管理

a　情報システム管理者は、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。

b　情報システム管理者は、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らない。

(ｳ) システム開発に用いるハードウエア及びソフトウエアの管理

a　情報システム管理者は、システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定しなければならない。

b　情報システム管理者は、利用を認めたソフトウエア以外のソフトウエアが導入されている場合、当該ソフトウエアをシステムから削除しなければならない。

ウ　情報システムの導入

(ｱ) 開発環境と運用環境の分離及び移行手順の明確化

a　情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

b　情報システム管理者は、システム開発、保守及びテスト環境からシステム運用環境への移行について、システム開発及び保守計画の策定時に手順を明確にしなければならない。

c　情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

d　情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

(ｲ) テスト

a　情報システム管理者は、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行わなければならない。

b　情報システム管理者は、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行わなければならない。

c　情報システム管理者は、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。

d　情報システム管理者は、開発したシステムについて受け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。

エ　システム開発及び保守に関連する資料等の整備及び保管

(ｱ) 情報システム管理者は、システム開発及び保守に関連する資料及び文書を適正に

整備及び保管しなければならない。

(ｲ) 情報システム管理者は、テスト結果を一定期間保管しなければならない。

(ｳ) 情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

オ　情報システムにおける入出力データの正確性の確保

(ｱ) 情報システム管理者は、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) 情報システム管理者は、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) 情報システム管理者は、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。

カ　情報システムの変更管理

情報システム管理者は、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。

キ　開発及び保守用のソフトウエアの更新等

情報システム管理者は、開発及び保守用のソフトウエア等を更新又は修正プログラムの適用をする場合、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。

ク　システム更新又は統合時の検証等

情報システム管理者は、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行わなければならない。

(4) 不正プログラム対策

ア　情報セキュリティ責任者の措置事項

情報セキュリティ責任者は、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。

(ｱ) 外部ネットワークから受信したファイルについて、インターネットのゲートウェイにおいて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すること。

(ｲ) 外部ネットワークに送信するファイルについて、インターネットのゲートウェイにおいて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、不正プログラムの外部への拡散を防止すること。

(ｳ) 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すること。

(ｴ) 所掌するサーバ及びパソコン等の端末に、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エアを常駐させること。

(ｵ) 不正プログラム対策ソフトウエアのパターンファイルについて、常に最新の状態に保つこと。

(ｶ) 不正プログラム対策のソフトウエアについて、常に最新の状態に保つこと。

(ｷ) 業務で利用するソフトウエアについて、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エアを利用しないこと。また、当該製品の利用を予定している期間中に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する予定がないことを確認すること。

イ　情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

(ｱ) 所掌するサーバ及びパソコン等の端末に、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エアをシステムに常駐させること。

(ｲ) 不正プログラム対策ソフトウエアのパターンファイルについて、常に最新の状態に保つこと。

(ｳ) 不正プログラム対策のソフトウエアについて、常に最新の状態に保つこと。

(ｴ) インターネットに接続していないシステムにおいて、電磁的記録媒体を使用する場合、コンピュータウイルス等の感染を防止するため、教育委員会が管理している電磁的記録媒体以外のものを教職員に利用させてはならない。また、不正プログラムの感染及び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エアを導入し、定期的に当該ソフトウエア及びパターンファイルの更新を実施すること。

(ｵ) 不正プログラム対策ソフトウエア等の設定変更権限について、一括管理し、情報システム管理者が許可した教職員を除く教職員に当該権限を付与しないこと。

ウ　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の端末において、不正プログラム対策ソフトウエアが導入されている場合、当該ソフトウエアの設定を変更しないこと。

(ｲ) 外部からデータ又はソフトウエアを取り入れる場合、必ず不正プログラム対策ソフトウエアによるチェックを行うこと。

(ｳ) 差出人が不明又は不自然に添付されたファイルを受信した場合、速やかに削除すること。

(ｴ) 端末に対して、不正プログラム対策ソフトウエアによるフルチェックを定期的に実施すること。

(ｵ) 添付ファイルが付いた電子メールを送受信する場合、不正プログラム対策ソフトウエアでチェックを行うこと。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化すること。

(ｶ) 情報セキュリティ責任者が提供するウイルス情報を、常に確認すること。

(ｷ) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合、LAN ケーブルの取り外し又は機器の電源遮断等、他への感染を防止する措置をとること。

(5) 不正アクセス対策

ア　情報セキュリティ責任者の措置事項

情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。

(ｱ) 使用されていないポートを閉鎖すること。

(ｲ) 不要なサービスについて、機能を削除又は停止すること。

(ｳ) 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定すること。

(ｴ) 情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築すること。

イ　攻撃への対処

最高情報セキュリティ責任者及び情報セキュリティ責任者は、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。

ウ　記録の保存

最高情報セキュリティ責任者及び情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が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）における違反行為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。

エ　内部からの攻撃

情報セキュリティ責任者及び情報システム管理者は、教職員及び委託事業者が使用しているパソコン等の端末からの教育委員会のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

オ　教職員による不正アクセス

情報セキュリティ責任者及び情報システム管理者は、教職員による不正アクセスを発見した場合は、当該教職員が所属する施設の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

カ　サービス不能攻撃

情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対し、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。

キ　標的型攻撃

情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、標的型メール受信時等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

(6) セキュリティ情報の収集

ア　セキュリティホールに関する情報の収集及び共有並びにソフトウエアの更新

情報セキュリティ責任者及び情報システム管理者は、セキュリティホール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。また、当該セキュリティホールの緊急度に応じて、ソフトウエア更新等の対策を実施しなければならない。

イ　不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員に周知しなければならない。

ウ　情報セキュリティに関する情報の収集及び共有

情報セキュリティ責任者及び情報システム管理者は、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。また、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。

8　運用

(1) 情報システムの監視

ア　情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

イ　情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

ウ　情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

(2) 本ポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

(ｱ) 情報セキュリティ管理者は、本ポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

(ｲ) 最高情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

(ｳ) 情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における本ポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

イ　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

最高情報セキュリティ責任者は、不正アクセス、不正プログラム等の調査のために、教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。

ウ　教職員の報告義務

(ｱ) 教職員は、本ポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

(ｲ) 当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情

報セキュリティ責任者が判断した場合において、教職員は、緊急時対応計画に従って適正に対処しなければならない。

(3) 侵害時の対応等

ア　緊急時対応計画の策定

最高情報セキュリティ責任者は、情報セキュリティインシデント、本ポリシーの違反等により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における連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

イ　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めるものとする。

(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

ウ　緊急時対応計画の見直し

最高情報セキュリティ責任者は、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的確に対応するため、必要に応じて緊急時対応計画の規定を見直さなければならない。

(4) 例外措置

ア　例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、行政事務の適正な遂行に当たり、本ポリシー及び情報セキュリティ実施手順に定める事項を遵守することが困難である場合は、遵守事項とは異なる方法を採用する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、最高情報セキュリティ責任者の許可を得て、例外措置を講じることができる。

イ　緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、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不可避のときは、事後速やかに最高情報セキュリティ責任者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。

ア　地方公務員法（昭和25年法律第261号）

イ　教育公務員特例法（昭和24年1月12日法律第1号）

ウ　著作権法（昭和45年法律第48号）

エ　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）

オ　個人情報の保護に関する法律（平成15年法律第57号）

カ　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）

キ　サイバーセキュリティ基本法（平成28年法律第31号）

ク　松前町個人情報保護条例（平成17年条例第１号）

10　懲戒処分等

(1) 懲戒処分

本ポリシーに違反した教職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法または教育公務員特例法による懲戒処分の対象とする。

(2) 違反時の対応

ア　情報セキュリティ責任者は、教職員における本ポリシーの違反を確認した場合は、速やかに当該教職員が所属する施設の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

イ　情報セキュリティ管理者は、所属する教職員について本ポリシーの違反の報告を受けた場合は、当該教職員への再発防止の指導その他適正な措置を講じなければならない。

ウ　情報セキュリティ責任者は、情報セキュリティ管理者の指導によっても改善されない場合、当該教職員のネットワーク又は情報システムを使用する権限を停止又は剥奪することができる。

エ　情報セキュリティ責任者は、教職員の情報システムを使用する権限を停止又は剥奪したときは、その旨を最高情報セキュリティ責任者及び当該教職員が所属する施設の情報セキュリティ管理者に通知しなければならない。

11　業務委託と外部サービスの利用

(1) 業務委託

ア　委託事業者の選定基準

情報システム管理者は、特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を委託する場合、委託事業者の選定に当たり、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にするほか、委託内容に応じた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。

イ　契約項目

特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を委託する場合は、委託事業者との間で必要に応じて次の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) 本ポリシーの遵守

(ｲ) 委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

(ｳ) 提供されるサービスレベルの保証

(ｴ) 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) 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委託事業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) 町による監査、検査
(ｼ) 町による情報セキュリティインシデント発生時の公表
(ｽ) 本ポリシーが遵守されなかった場合の規定

ウ　確認・措置等

(ｱ) 情報システム管理者は、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定期的に確認し、必要に応じ、契約に基づく措置を講じなければならない。

(ｲ) 情報システム管理者は、契約に基づく措置を講じたときは、その内容を最高情報セキュリティ責任者に報告しなければならない。

(2) 外部サービスの利用

ア　約款による外部サービスの利用

(ｱ) 約款による外部サービスの利用に係る規定の整備

情報セキュリティ責任者は、次の内容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するものとする。また、当該サービスの利用において、機密性２以上の情報が取り扱われないように規定するものとする。

a　約款によるサービスを利用して良い範囲
b　業務により利用する約款による外部サービス
c　利用手続及び運用手順

(ｲ) 約款による外部サービスの利用における対策の実施

情報セキュリティ管理者は、利用するサービスの約款そのほか提供条件から、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。

イ　クラウドサービスの利用

(ｱ) 情報セキュリティ管理者は、クラウドサービスを利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。

(ｲ) 情報システム管理者は、クラウドサービスの利用を通じて教育委員会が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス事業者を選定し、必要に応じて教育委員会の情報が取り扱われる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。

(ｳ) 情報システム管理者は、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、クラウドサービス事業者を選定する際の要件としなければならない。

(ｴ) 情報システム管理者は、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。

(ｵ) 情報システム管理者は、クラウドサービス事業者におけ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。

12　評価・見直し

(1) 自己点検

ア　実施方法

(ｱ) 情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、必要に応じ自己点検を実施しなければならない。

(ｲ) 情報セキュリティ管理者は、所管における本ポリシーに沿った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行わなければならない。

(ｳ) 教育委員会は必要に応じて監査を行う。

イ　報告

情報システム管理者及び情報セキュリティ管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、最高情報セキュリティ責任者に報告しなければならない。

ウ　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) 情報セキュリティ責任者は、この点検結果を本ポリシーの見直し、その他情報セキュリティ対策の見直しに活用しなければならない。

(3) 本ポリシーの見直し

情報セキュリティ責任者は、自己点検の結果及び情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合、本ポリシーの見直しを行うものとする。