第１章　教育情報セキュリティ基本方針

１．目的

岬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、学校のＩＣＴ環境整備が進むにあたり、不正アクセス、ウイルス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・消去など、情報資産の保護に向けた十分な情報セキュリティ対策を講じることは、教職員及び児童生徒等が安心してＩＣＴを活用するために不可欠である。

また、ＧＩＧＡスクール構想の推進により、クラウドサービスの活用を前提としたネットワーク構成等の課題に対応するとともに、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６年１月版）」を参考に、岬町教育委員会において「岬町立学校教育情報セキュリティポリシー」（以下「このポリシー」という。）を策定するものとする。

２．構成

このポリシーは、学校が保有する情報資産（校務系情報・学習系情報）に対する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、学校が保有する情報資産を取り扱う全教職員に浸透、定着させるものであることから、安定した統一的な規範であることが求められる。

一方、情報処理や通信技術の進歩による急速な環境の変化に柔軟に対応することも必要であることから、教育情報セキュリティ対策における統一的な規範として基本的な考え方を定める「教育情報セキュリティ基本方針」と、情報資産を取り巻く環境の変化に柔軟に対応していくための「教育情報セキュリティ対策基準」の２部構成として策定する。

なお、学校に敷設されている行政系ネットワークの取扱いについては、「岬町情報セキュリティーポリシー」に準拠するものとする。

３．用語の定義

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

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、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

５．適用範囲

この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

６．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。また、教職員等は、教育情報セキュリティの重要性を認識し、このポリシーを遵守しなければならない。

７．教育情報セキュリティ対策

情報資産を脅威（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、全教職員等にこの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、この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、このポリシーの運用面の対策を講じるものとする。また、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。

８．監査及び自己点検

この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教育情報セキュリティ監査及び自己点検を実施する。

９．このポリシーの見直し

教育情報セキュリティ監査及び自己点検の結果、この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、このポリシーを見直す。

第２章　教育情報セキュリティ対策基準

１．趣旨

この教育情報セキュリティ対策基準は、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。

２．管理体制

教育情報セキュリティの管理体制は以下のとおりとする。

(1)　教育情報統括管理責任者

教育長を教育情報統括管理責任者とする。教育情報統括管理責任者は、学校における全てのネットワークや教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有する。

(2)　教育情報統括責任者

教育次長を教育情報統括責任者とする。教育情報統括責任者は、学校における情報資産に対するセキュリティ侵害が発生した場合、又はセキュリティ侵害のおそれがある場合に必要かつ十分な措置を行う権限及び責任を有する。

(3)　教育情報セキュリティ管理者

指導課長を教育情報セキュリティ管理者とする。教育情報セキュリティ管理者は、学校における情報資産の管理及び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。

(4)　教育情報セキュリティ担当者

教育情報セキュリティ管理者の指示に従い、学校における情報資産の管理、運用ルールの策定及び情報セキュリティ対策に関する教職員等の教育研修、助言を行う者を教育情報セキュリティ担当者とする。

(5)　教育情報システム管理者

学校教育課長を教育情報システム管理者とする。教育情報システム管理者は、学校における教育情報システムの導入、管理、運用、見直し等に関する統括的な権限及び責任を有するほか、所管する教育情報システムに対する情報セキュリティ対策に関する権限及び責任を負う。

(6)　教育情報システム担当者

教育情報システム管理者の指示に従い、学校における教育情報システムの導入、管理、運用、見直し等の作業を行う。また、学校における情報資産に対するセキュリティ侵害が発生した場合、又はセキュリティ侵害のおそれがある場合に、教育情報セキュリティ管理者を補佐する者を教育情報システム担当者とする。

(7)　学校教育情報セキュリティ責任者

各学校長を学校教育情報セキュリティ責任者とする。学校教育情報セキュリティ責任者は、所属校における教育情報セキュリティ実施手順書を策定し、情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有する。また、学校における情報資産に対するセキュリティ侵害が発生した場合、又はセキュリティ侵害のおそれがある場合には、教育情報セキュリティ管理者、教育情報統括責任者及び教育情報統括管理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。

(8)　学校教育情報セキュリティシステム管理者

各学校の教頭を学校教育情報セキュリティシステム管理者とする。学校教育情報セキュリティシステム管理者は、学校教育情報セキュリティ責任者を補佐するとともに、所属する教職員等の教育情報セキュリティ対策の実施について、管理、指導を行う。また、個々の教育情報システムの管理、運用、見直し等の権限及び責任を有する。

(9) 学校教育情報セキュリティシステム担当者

各学校の情報システムの管理、運用に携わる教職員等を学校情報セキュリティシステム担当者とする。学校教育情報セキュリティシステム担当者は、学校教育情報セキュリティシステム管理者の指示に従い、情報システムの管理、運用、見直し等の作業を行う。また、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者と協力して、全教職員に対してこのポリシーの遵守及び周知・啓発に努める。

(10) 情報セキュリティ委員会への連携

教育情報統括責任者は、情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した事案を正確に把握した上で、情報政策担当部長に報告し、連携を図る。

３．情報資産の分類と管理

学校の情報資産の機密性、完全性及び可用性により、次のとおり分類し、必要に応じて取扱制限を定め、適正な管理を行う。

重要性分類	
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシーに等へ重大な影響を及ぼすもの
Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼすもの
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼすもの
Ⅳ	影響をほとんど及ぼさないもの

【機密性による情報資産の分類】

機密性	分類基準	該当する情報資産のイメージ
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
機密性２Ｂ	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	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２Ａ	学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒等がアクセスすることを想定している情報資産	教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産（教職員及び児童生徒のうち特定の教職員及び児童生徒のみが知り得る状態

		を確保する必要があるもの）
機密性１	機密性２Ａ、機密性２Ｂ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で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）

【完全性による情報資産の分類】

完全性	分類基準	該当する情報資産のイメージ
完全性２Ｂ	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破壊により、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	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に支障ある情報
完全性２Ａ	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破壊により、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確な遂行に支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に軽微な支障ある情報
完全性１	完全性２Ａ又は完全性２Ｂの情報資産以外の情報資産	事故があった場合でも業務の遂行に支障がない情報

【可用性による情報資産の分類】

可用性	分類基準	該当する情報資産のイメージ
可用性２Ｂ	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（軽微なものは除く）を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失、紛失や、情報システムの停止等があった場合、業務の安定的な遂行に支障がある情報
可用性２Ａ	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軽微な支障を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失、紛失や、情報システムの停止等があった場合、業務の安定的な遂行に軽微な支障がある情報
可用性１	完全性２Ａ又は可用性２Ｂの情報資産以外の情報資産	滅失、紛失や情報システムの停止等があっても業務の遂行に支障がない情報

【情報資産の分類】

情報資産の分類					情報資産の例示		
重要性	定　義	機密性	完全性	可用性	校務系	学習系	公開系
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	３	２Ｂ	２Ｂ	・指導要録原本 ・教職員の人事情報 ・教育情報システム仕様書		
Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。	２Ｂ	２Ｂ	２Ｂ	○学籍関係 ・卒業証書授与台帳 ・転退学受付簿 ・転入学受付簿 ・就学児童・生徒移動報告書 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・定期考査・テスト等の答案用紙（記入済のもの）？　自動採点？ ・定期考査素点表 ・成績に関する個票等 ○指導関係 ・児童生徒等の個人写真・集合写真 ・教育相談・面接の記録 ・個別の教育支援計画 ・個別指導計画 ・教務手帳 ○進路関係 ・調査書 ・推薦書 ・公立学校入学者選抜に係る成績一覧表 ・入学者選抜に係る表簿（願書等） ・私立学校入試に係る事前相談一覧表 ・卒業生進路先一覧表 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 ○児童生徒に関する個人情報（生活歴、心身の状況、財産状況等の情報、電話番号、メールアドレス、住所、氏名、生年月日、性別等の基本情報を含むもの）	○児童生徒の学習系情報 ・学習システムログイン ID/PW 管理台帳 ・学習者用端末 ID/PW 台帳	

Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす	２Ｂ	２Ｂ	２Ｂ	○学校教職員に関する個人情報（病歴、心身の状況、収入等の状況、電話番号、メールアドレス、住所、氏名、生年月日等の基本情報を含むもの） ○健康関係 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ・児童生徒等健康調査票 ・健康診断に関する表簿 ・就学時健康診断票 ○教職員に割り当てた機密性の高い情報 ・情報端末ログインID/PW ○その他 ・給食関係書類 ○名簿等 ・児童生徒名簿 ・児童生徒の住所録 ・ＰＴＡ会員名簿 ・職員緊急連絡網・住所録 ・委員会名簿 ○各種帳票ファイル ・指導要録以外の帳票・データ		
Ⅲ Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。 セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす	２Ａ ２Ａ	２Ａ ２Ａ	２Ａ ２Ａ	○児童生徒の氏名 ・出席簿 ・名列表 ・児童生徒委員会名簿 ○学校運営関係 ・卒業アルバム ・学校行事等の児童生徒の写真	○学校運営関係 ・授業用教材 ・生徒用配布プリント ○児童生徒の学習系情報 ・児童生徒の学習記録（確認テスト・レポート・作品等） ・学習活動の記録（動画・写真等）	
Ⅳ	影響をほとんど及ぼさない	1	1	1			○学校運営関係 ・学校要覧 ・使用教科書一覧 ・教育課程編成表 ・学校設定費目の届出 ・学校徴収金会計簿 ・学校行事実施計画 ・保護者等への配布文

							書 ・各種ひな形・校務分掌表 ・ＰＴＡ資料 ・学校・学年・学級だより ・学校ホームページ掲載情報 ・学校行事のしおり ○学校活動の記録 ＊保護者の承諾がある場合、公開可能 ・学校行事等の児童生徒の写真 ・学習活動の記録（動画・写真・作品等）

【情報資産の管理】

情報資産の管理は、以下のとおりとする。

情報資産の分類					情報資産の取扱等								
重要性	定　　義	機密性	完全性	可用性	複製・配布	組織外部への持ち出し＊1	端末制限	組織外部への送信＊2	情報資産の運搬＊3	組織外部での情報処理＊4	使用する電磁的記録媒体	情報資産の保管	情報資産の廃棄
Ⅰ	**セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。**	3	2 B	2 B	必要以上の複製及び配布禁止	本ガイドラインに遵守していることを確認した上で業務遂行上必要な場合には、教育情報セキュリティ管理者の判断で持ち出しを可	支給以外の端末での作業の原則禁止	限定されたアクセスの措置が取られていること＊5	鍵付きケースへの格納	禁止	施錠可能な場所への保管	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ ・６か月以上のログ保管 ・サーバの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁的記録媒体の持ち込み禁止	電子的記録媒体の初期化、復元できないようにして廃棄

Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。	2B	2B	2B	同上	同上		同上	同上	安全管理措置の規定が必要	同上	同上	同上
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。	2A	2A	2A	同上	教育情報セキュリティ管理者の包括的承認で可		同上	同上	同上	同上	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ（推奨事項） ・一定期間以上のログ保管 ・サーバ・ハードディスクの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁的記録媒体の持ち込み禁止	同上
Ⅳ	影響をほとんど及ぼさない	1	1	1									同上

＊１　組織外部への持ち出しとは、教育委員会・学校が構築している環境（このポリシーが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外に情報資産を持ち出すことを示す。

＊２　情報の組織外部への送信とは、情報システムをを構築するネットワーク、端末、サーバの閉じた領域の外側に情報資産をオンラインで持ち出すことを示す。

＊３　情報資産の運搬とは、ＵＳＢメモリやハードディスク等の外部電磁的記録媒体を介して情報資産を運搬する場合を示す。

＊４　組織外部での情報処理とは、教育委員会・学校が管理している環境（このポリシーが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外において情報資産を管理・電算処理することを示す。

＊５　限定されたアクセスの措置とは、適切かつ限定的な利用を前提とし、外部に送信される際に適切なアクセス制限を講じることを示す。

４．物理的セキュリティ

(1)　サーバ等の管理

ア　機器の取り付け等

教育情報システム管理者は、サーバ等を取付けを行う場合、地震、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、容易に取り外せないよう適性に固定する等、必要な措置を講じなければならない。

イ　機器の電源

①　教育情報システム管理者は、　教育情報セキュリティ管理者及び施設管理担当課と連携し、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備えなければならない。

②　教育情報システム管理者は、　教育情報セキュリティ管理者及び施設管理担当課と連携し、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。

ウ　通信ケーブル等の配線

①　教育情報セキュリティ管理者及び教育情報システム管理者は、施設管理担当課と連携し、

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。

② 教育情報セキュリティ管理者及び教育情報システム管理者は、主要な個所の通信ケーブル及び電源ケーブルいついて、学校から損傷等の報告があった場合、連携して対応しなければならない。

③ 教育情報セキュリティ管理者及び教育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。

④ 教育委員会及び学校長から許可を得た者又は契約により操作を認められた外部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、

エ 機器の定期保守及び修理

① 教育情報システム管理者は、情報システムの安定的な運用のために、可用性２A以上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。

② 教育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外部の事業者に修理させる場合、秘密保持体制の確認等を行わなければならない。

オ 機器の廃棄等

教育情報システム管理者は、機器を廃棄、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) 通信回線及び通信回線装置の管理

ア 通信回線の管理

学校教育情報セキュリティ責任者は、学校内の通信回線及び通信回線装置を教育委員会と連携し、適切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切に保管しなければならない。

イ 外部へのネットワーク接続

学校教育情報セキュリティ責任者は、外部へのネットワーク接続ポイント及び当該ポイントに接続される端末を正確に把握し、適正な管理を行わなければならない。

ウ 通信回線の適切な選択と情報の暗号化

① 学校教育情報セキュリティ責任者は、重要性分類Ⅲ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、適切な回線を選択しなければならない。また、必要に応じ、通信回路上での暗号化を行わなければならない。

② 学校教育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。

(3) 教職員等の利用する端末や電磁的記録媒体等の管理

ア 校務用端末、校務外部接続用端末及び指導者用端末について

① 学校教育情報セキュリティシステム管理者は、盗難防止のため、端末のワイヤーによる固定や保管庫等による管理等、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、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。

② 学校教育情報セキュリティシステム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③ 学校教育情報セキュリティシステム管理者は、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）を設定しなければならない。

④ 学校教育情報セキュリティシステム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティーチップが搭

載されている場合、その機能を有効に活用しなければならない。同様に、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。

イ　学習用端末について

① 学校教育情報セキュリティシステム管理者は、盗難防止のため、端末のワイヤーによる固定や保管庫等による管理等、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、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。

② 学校教育情報セキュリティシステム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③ 学校教育情報セキュリティシステム管理者は、授業に支障のないネットワーク構成の選択（帯域や同時接続数等）を行うこと。

④ 学校教育情報セキュリティシステム管理者は、児童生徒等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（フィルタリングソフト、検索エンジンのセーフサーチ、セーフブラウジング等）を講じなければならない。

⑤ 学校教育情報セキュリティシステム管理者は、学校内外での端末におけるマルチウェア感染対策を講じなければならない。

⑥ 学校教育情報セキュリティシステム管理者は、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等が安心して利用できる状態を維持しなければならない。

⑦ 学校教育情報セキュリティシステム管理者は、学校内外での端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理しなければならない。

５．人的セキュリティ

教職員等が情報資産を取り扱う際に遵守すべき人的セキュリティ対策は、以下のとおりとする。

(1)　教職員等の遵守事項

ア　教育情報セキュリティポリシーの遵守

教職員等は、このポリシー及び実施手順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、遵守することが困難な点等がある場合は、速やかに学校教育情報セキュリティシステム管理者に相談し、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

教職員等は、業務以外の目的で情報資産の外部への持ち出し、教育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　モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築管理している環境（このポリシーが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

① 学校教育情報セキュリティ責任者は、重要分類Ⅱ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

② 教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、学校教育情報セキュリティシステム管理者の許可を得なければならない。

③ 教職員等は、外部で情報処理業務を行う場合には、学校教育情報セキュリティシステム管理者の許可を得なければならない。

エ　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

① 教職員等は、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業務に利用してはならない。ただし、業務上必要な場合には、学校教育情報セキュリティシステム管理者の許可を得て利用することができる。

② 教職員等は、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用いる場合に

は、学校教育情報セキュリティシステム管理者の許可を得た上で、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。

オ　持ち出し及び持ち込みの記録

学校教育情報セキュリティシステム管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

カ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を、学校教育情報セキュリティ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

教職員等は、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学校教育情報セキュリティシステム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。

ク　退職時等の遵守事項

教職員等は、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。

ケ　情報セキュリティポリシー等の掲示

学校教育情報セキュリティ責任者は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧できるよう掲示しなければならない。

コ　外部委託事業者に対する説明

学校教育情報セキュリテシステム管理者は、ネットワーク及び情報システムの開発・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、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

学校教育情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

イ　研修計画の策定及び実施

①　学校教育情報セキュリティ責任者は、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、教育委員会の承認を得なければならない。

②　研修計画において、教職員等は、毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

③　新規採用の教職員等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　緊急対応訓練

学校教育情報セキュリティ責任者は、緊急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、訓練実施の体制、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　訓練・研修への参加

全ての教職員等は、定められた研修・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　学校内からの情報セキュリティインシデントの報告

①　教職員等は、情報セキュリティインシデントを認知した場合、速やかに学校教育情報セ

キュリティ責任者に報告しなければならない。
② 報告を受けた学校教育情報セキュリティ責任者は、速やかに教育情報セキュリティ管理者に報告しなければならない。
③ 教育情報セキュリティ管理者は、報告を受けた情報セキュリティインシデントについて、必要に応じて教育情報統括責任者及び教育情報統括管理責任者に報告しなければならない。

イ 住民等外部からの情報セキュリティインシデントの報告
① 教職員等は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、学校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 報告を受けた学校教育情報セキュリテ責任者は、速やかに教育情報セキュリティ管理者に報告しなければならない。
③ 教育情報セキュリティ管理者は、当該情報セキュリティインシデントについて、速やかに教育情報統括責任者及び教育情報統括管理責任者に報告しなければならない。
④ 教育情報統括責任者は、教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

ウ 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
① 教育情報統括責任者は、情報セキュリティインシデントについて、教育情報セキュリティ管理者、教育情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、これらの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。また、教育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、教育情報統括管理責任者に報告しなければならない。
② 教育情報統括管理責任者は、教育情報統括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、その内容を確認し、再発防止策を実施するための必要な措置を支持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

教職員等は、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。
① 自己が利用しているＩＤは、他人に利用させてはならない。
② 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

教職員等は、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。
① 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。
② 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。
③ 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。
④ パスワードが流出したおそれがある場合には、学校教育情報セキュリティ責任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。
⑤ 複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く。）
⑥ 仮のパスワード（初期パスワードを含む。）は、最初のログイン時点で変更しなければならない。
⑦ サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。
⑧ 教職員間でパスワードを共有してはならない。（ただし、共有ＩＤに対するパスワードは除く。）

６．技術的セキュリティ

情報システム等の不正利用を防止し、不正利用に対する証拠の保全をするための技術的セキュリティ対策は以下のとおりとする。

(1)　コンピュータ及びネットワークの管理

ア　文書サーバ及び端末の設定等

①　教育情報システム管理者は、教職員等が使用できる文書サーバの容量を設定し、教職員等に周知しなければならない。

②　教育情報システム管理者は、文書サーバを学校等の単位で構成し、教職員等が他の学校等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。

③　教育情報システム管理者は、住民の個人情報、人事記録等、特定の教職員しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当教職員以外の教職員等が閲覧及び使用できないようにしなければならない。

④　教育情報システム管理者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、機微な個人情報を補完する場合に限る。）については、標的型攻撃等によるファイルの外部流出を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

イ　バックアップの実施

教育情報統括責任者及び教育情報システム管理者は、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、校務系情報及び校務外部接続系情報、学習系情報について、必要に応じて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

教育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、教育情報統括管理責任者及び教育情報統括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

①　教育情報システム管理者は、所属する教育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。

②　教育情報統括責任者及び教育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、改ざん等を去れないように適切に管理しなければならない。

③　教育情報統括責任者、教育情報システム管理者又は教育情報システム担当者及び契約により操作を認められた外部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

教育情報統括責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、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、適切に管理しなければならない。

カ　ログの取得等

①　教育情報統括責任者及び教育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。

②　教育情報統括責任者及び教育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、適切にログを管理しなければならない。

③　教育情報統括責任者及び教育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

教育情報統括責任者及び教育情報システム管理者は、教職員等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、適切に保存しなければならない。

ク　ネットワークの接続制御、経路制御等

①　教育情報統括責任者は、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ェア等を設定しなければならない。

②　教育情報統括責任者は、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

①　教育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、教育情報統括責任者の許可を得なければならない。

②　教育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、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報財産に影響が生じないことを確認しなければならない。

③　教育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によりデータの漏洩、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。

④　教育情報統括責任者及び教育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、教育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。

⑤　教育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、教育情報統括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　複合機のセキュリティ管理

①　教育情報統括責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う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。

②　教育情報統括責任者は、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。

③　教育情報統括責任者は、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する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。

サ　特定用途機器のセキュリティ管理

教育情報統括責任者は、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講じなければならない。

シ　無線ＬＡＮ及びネットワークの盗聴対策

①　教育情報統括責任者は、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。

②　教育情報統括責任者は、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まらない。

ス　電子メールのセキュリティ管理

①　教育情報統括責任者は、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（電子メールの中間処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

②　教育情報統括責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③　教育情報統括責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メ

ールの送受信を不可能にしなければならない。

④　教育情報統括責任者は、教職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員等に周知しなければならない。

⑤　教育情報統括責任者は、システム開発や運用、保守等のため教育委員会及び学校に駐在している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

セ　電子メールの利用制限

①　教職員等は、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。

②　教職員等は、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。

③　教職員等は、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を分からないようにしなければならない。

④　教職員等は、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。

⑤　教職員等は、ウェブで利用できるフリーメールサービス等を教育情報統括責任者の許可なしに使用してはならない。

⑥　教職員等は、情報資産の分類により定めた取扱制限に従い、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、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。

⑦　児童生徒等が扱う電子メールは、学校教育情報セキュリティ責任者が許可した相手だけに送受信できる設定にしなければならない。

ソ　無許可ソフトウェアの導入等の禁止

①　教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②　教職員等は、業務上の必要がある場合は、教育情報セキュリティ管理者及び教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育情報セキュリティ管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

タ　機器構成の変更制限

①　教職員等は、パソコンやモバイル端末に対し、機器の改造及び増設・交換を行ってはならない。

②　教職員等は、パソコンやモバイル端末に対し、機器の改造及び増設・交換を行う必要がある場合には、教育情報統括責任者及び教育情報システム管理者の許可を得なければならない。

チ　無許可でのネットワーク接続の禁止

職員等は、学校教育情報セキュリティ責任者の許可なく、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。

ッ　業務以外の目的でのウェブ閲覧の禁止

①　教職員等は、業務以外の目的でウェブを閲覧してはならない。

②　学校教育情報セキュリティ責任者は、教職員等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、教育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。

テ　無線ＬＡＮ及び移動体通信の利用制限

教職員等は、学校教育情報セキュリティ責任者が認めた場合に限り、教育外部系（授業用）ネットワーク、教育外部系ネットワークの無線ＬＡＮ及び移動体通信を利用することができる。

ト　スマートデバイスに係るセキュリティ管理

①　学校教育情報セキュリティシステム管理者は、スマートデバイスが備える機能や使用環境、取扱う情報、その他業務の特性等に応じ、適正なセキュリティ要件を含め、必要な対

策を実施しなければならない。

② 教職員等は、スマートデバイスを使用するにあたり、学校教育情報セキュリティシステム管理者等が実施したセキュリティ対策及び、使用手順に従い適正にスマートデバイスを使用しなければならない。

⑵ アクセス制御等

ア アクセス制御等

学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、所管するネットワーク又は情報システムごとに、アクセス権限のない教職員等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

① 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、利用の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

② 教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者に通知しなければならない。

③ 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、利用されていないＩＤの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

① 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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のパスワードの漏洩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 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、特権を付与されたＩＤ及びパスワードの変更について、外部委託事業者に行わせてはならない。

③ 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、特権ＩＤを作成・削除する、もしくは、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

④ 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

エ 教職員等による外部からのアクセス等の制限

① 教職員等が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は、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者の許可を得なければならない。

② 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③ 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

④ 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

⑤ 学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、外部からのアクセスに利用するモバイル端末を教職員等に貸与する場合、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。

⑥　教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内の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、パッチの適用状況等を確認しなければならない。

⑦　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、公衆通信回線（公衆無線ＬＡＮ等）を教育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。

オ　ログイン時の表示等

教育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、正当なアクセス権限を持つ教職員等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するよう努めなければならない。

カ　パスワードに関する情報の管理

①　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、教職員等のパスワードに関する情報を厳重に管理しなければならない。パスワード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パスワード設定の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。

②　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、教職員等に対して、パスワードを発行する場合は、仮のパスワードを発行し、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。

キ　特権による接続時間の制限

学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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、保守等

ア　情報システムの調達

①　教育情報統括責任者及び教育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。

②　教育情報統括責任者及び教育情報システム管理者は、機器及びソフトウェ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

①　システム開発における責任者及び作業者の特定

教育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。また、システム開発のための規則を確立し、開発を行う場合には、教育情報統括責任者に報告しなければならない。

②　システム開発における責任者、作業者のＩＤの管理

・　教育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。

・　教育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い。

③　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

・　教育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ェ

ア及びソフトウェアを特定しなければならない。

・　教育情報システム管理者は、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

①　開発環境と運用環境の分離及び移行手順の明確化

・　教育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への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

・　教育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。

・　教育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。

②　テスト

・　教育情報システム管理者は、新たに情報システムを導入しようとする場合、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い、不具合の発見及び解消に努めなければならない。

・　教育情報システム管理者は、運用テストを行う場合、あらかじめ疑似環境による操作確認を行わなければならない。

・　教育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。

・　教育情報システム管理者は、既存のネットワークを利用したシステムを導入しようとするときは、ネットワークへの接続テストを行うとともに、アクセス権限を明確にし、アクセスの管理等に関する事項を定めなければならない、

エ　システム開発・保守に関連する資料等の整備、保管

教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・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

①　教育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。

②　教育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洩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。

③　教育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

教育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・保守用のソフトウェアの更新等

教育情報システム管理者は、開発・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。

ク　システム更新又は統合時の検証等

教育情報システム管理者は、システム更新、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、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　学校教育情報セキュリティ責任者の措置事項

学校教育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。

① 外部ネットワークから受信したファイルは、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進入を防止しなければならない。

② 外部ネットワークに送信するファイルは、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しなければならない。

③ 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、必要に応じ教職員等に対して注意喚起しなければならない。

④ 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ェアを常駐させなければならない。

⑤ 不正プログラム対策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。

⑥ 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。

イ 教職員等の遵守事項

教職員等は、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。

① 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。

② 外部からの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行わなければならない。

③ 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は、速やかに削除しなければならない。

④ 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤ 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を行わなければならない。

⑥ 不正プログラム対策ソフトウェア開発者が提供するウイルス情報を、常に確認しなければならない。

⑦ 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は、以下の対応を行い、速やかに教育情報セキュリティ管理者に報告しなければならない。

- パソコン等の端末の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。
- モバイル端末の場合は、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 専門家の支援体制

教育情報統括責任者は、実施している不正プログラム対策では不十分な状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。

(5) 不正アクセス対策

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

① 使用されていないポートや不要なサービスについて、ポート閉鎖や機能を削除又は停止しなければならない。

② 重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

③ 教育委員会及び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

絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

イ　学校教育情報セキュリティ責任者は、情報システムに攻撃を受けた場合又は攻撃予告があり、攻撃を受けることが明確になった場合には、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。また、教育委員会と連絡を密にし、情報の収集に努めなければならない。

ウ　学校教育情報セキュリティ責任者は、外部から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、教育委員会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　教育情報統括責任者及び教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等のネットワークや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　教育情報統括責任者は、教職員等が学校内にあるパソコン等を利用した不正アクセスを発見した場合は、当該教職員等が所属する学校教育情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

カ　学校教育情報セキュリティ責任者は、標的型攻撃による内部への侵入を防止するために、以下のような対策を講じなければならない。

①　人的対策（標的攻撃型メール）

- 差出人に心当たりのないメールは開封しない。
- 不自然なメールが着信した際は、差出人にメール送信の事実を確認する。
- メールを開封した後で標的型攻撃と気付いた場合、添付ファイルは絶対開封せず、メール本文に書かれたＵＲＬもクリックしない。
- 標的型攻撃と気付いた場合、学校教育情報セキュリティ責任者に対して着信の事実を報告し、組織への注意喚起を依頼した後に、メールを速やかに削除する。
- 学校教育情報セキュリティシステム管理者は、メールやログを確認し、不正なメールがなかったかチェックする。（事後対策）

②　電磁的記録媒体に対する対策

- 出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。
- 電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。
- パソコン等の端末について、自動再生（オートラン）機能を無効化する。
- パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

(6)　セキュリティ情報の収集

ア　教育情報統括責任者及び教育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、学校と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、ソフトウェアの更新等の対策を実施しなければならない。

イ　教育情報統括責任者及び教育情報システム管理者は、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、対処方法について教職員等に周知しなければならない。

ウ　教育情報統括責任者及び教育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、学校と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。

７．運用

(1)　情報システムの監視

ア　教育情報統括責任者及び教育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。特に外部と接続するシステムについ

ては、ファイアウォール等を用い、不正アクセスによる攻撃を受けていないか、監視、分析を行わなければならない。

イ　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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　教育情報統括責任者及び教育情報システム管理者が指名した者は、重要性分類Ⅱ以上の情報資産を格納する校務系システム及び校務外部接続系システムを常時監視しなければならない。

エ　教育情報統括責任者及び教育情報システム管理者が指名した者は、重要性分類Ⅲ以上の情報資産を格納する学習系システムを常時監視しなければならない。

(2)　教育情報セキュリティポリシーの遵守状況の確認

ア　教育情報統括責任者及び教育情報セキュリティ管理者は、このポリシーの遵守状況について確認を行い、問題を認めた場合は、速やかに教育情報統括管理責任者に報告し、適切に対処しなければならない。

イ　教育情報統括責任者及び教育情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定時におけるこの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、適切かつ速やかに対処しなければならない。

(3)　パソコン、モバイル端末及び電磁的記録媒体の利用状況調査

教育情報統括責任者及び教育情報システム管理者が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が得利用しているパソコン、モバイル端末及び電磁的記録媒体のログ、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。

(4)　教職員の報告義務

ア　教職員等は、このポリシーに対する違反行為を発見した場合、直ちに学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム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教育情報統括責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

(5)　侵害時の対応等

ア　緊急時対応計画の策定

教育情報統括責任者は、情報セキュリティインシデント、情報セキュリティ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いて、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切に実施するために、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切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、以下の内容を定めなければならない。

①　関係者の連絡先
②　発生した事案に係る報告すべき事項
③　発生した事案への対応措置
④　再発防止措置の設定

ウ　業務継続計画と整合性確保

自然災害、大規模又は広範囲に及ぶ疾病等に備えて、別途業務継続計画を策定し、当該計画とこのポリシーの整合性を確保しなければならない。

エ　緊急時対応計画の見直し

教育情報統括責任者は、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応じ、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。

(6) 例外措置

ア 例外措置の許可

教育情報統括責任者及び教育情報システム管理者は、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、学校事務及び教育活動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、教育情報統括管理責任者の許可を得て、例外措置を取ることができる。

イ 教育情報統括責任者及び教育情報システム管理者は、学校事務及び教育活動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、事後速やかに教育情報統括管理責任者に報告しなければならない。

ウ 例外措置の申請書の管理

教育情報統括責任者及び教育情報システム管理者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

(7) 法令等遵守

職員等は、職務の遂行において使用する情報財産を保護するために、次の法令のほか、関係法令等を遵守し、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 地方公務員特例法（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（平成 15 年法律第 57 号）
⑥ 行政手続き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）
⑦ サイバーセキュリティ基本法（平成 26 年法律第 104 号）
⑧ 岬町個人情報保護条例（平成 12 年条例第 28 号）
⑨ 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に基づく個人番号の利用に関する条例（平成 27 年条例 29 号）

(8) 懲戒処分等

ア 教育情報統括責任者は、教職員等がこのポリシーに規定する事項及び指示に違反した場合には、当該教職員等が所属する学校教育情報セキュリティ責任者に通知し、ネットワーク及び情報機器等の利用を停止し、その権利を剝奪することができる。

イ 当該教職員等は、違反の重要性、発生した事案の状況等に応じて、地方公務員法をはじめとする関係法令による懲戒処分の対象とする。

8．外部委託

(1) 外部委託事業者の選定基準

ア 教育情報システム管理者は、外務委託事業者の選定に当たり、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 教育情報システム管理者は、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して、事業者を選定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。

- 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
- 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
- 提供されるサービスレベルの保証
- 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
- 外部委託事業者の作業員に対する教育の実施
- 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
- 業務上知り得た情報の守秘義務
- 再委託に関する制限事項の遵守
- 委託業務終了時の情報資産の返還、廃棄等
- 委託業務の定期報告及び緊急時報告事務
- 町による監査、検査
- 町による情報セキュリティインシデント発生時の公表
- 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

教育情報システム管理者は、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定期的に確認し、必要に応じ、前項の契約に基づき措置しなければならない。また、その内容を教育情報統括責任者に報告するとともに、その重要度に応じて教育情報統括管理責任者に報告しなければならない。

(4) 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

教育情報システム管理者は、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。また、当該サービスの利用において、機密性の高い情報が取り扱われないように規定しなければならない。

- 約款によるサービスを利用してよい範囲
- 業務により利用する約款による外部サービス
- 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

教職員等は、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、適切な措置を講じた上で利用しなければならない。

(5) ソーシャルメディアサービスの利用

ア 教育情報システム管理者は、教育委員会又は学校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、情報セキュリティ対策に関する次の事項を定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。

① 教育委員会又は学校のアカウントによる情報発信が、実際のものであることを明らかにするために、本町の自己管理ウェブサイトやプロフィール画面等に情報を掲載して参照可能とするとともに、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行うこと。

② パスワードや認証のためのコード等の認証情報等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

イ 機密性２A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。

ウ 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。

エ　アカウントの乗っ取りを確認した場合は、被害を最小限にするための措置を講じなければならない。

9．事業者に対して確認すべきプライバシー保護に関する事項

外部委託やクラウドサービスの利用に当たり、個人情報の収集・利用範囲や管理期間、データの統制と所有の在り方等について、以下の事項について事業者に確認しなければならない。

(1)　個人情報の利用範囲

教育、学校の目的に必要な情報、又は児童生徒等及び保護者の許可した情報を超えて個人情報の収集・維持、使用、共有をしないこと。

(2)　個人情報の無断提供

クラウドサービスの導入によって知り得た個人情報について、売買も含め、無断提供しないこと。

(3)　個人情報を利用した利用者に対する広告活動等の無断使用の禁止

学校、教育の目的を達成すること以外に、個人情報について児童生徒等及び保護者に対する行動ターゲティング広告をはじめとする広告活動その他無断使用をしないこと。

(4)　不必要な個人プロファイル作成の禁止

教育、学校の目的を達成するため、又は児童生徒等及び保護者によって保護された場合を除き、不必要な個人プロファイルを作成しないこと。

(5)　不適切なポリシー等の変更の禁止

クラウドサービスの運用等において、利用者に対する明確な通知、相談等の対応もなく、利用者のプライバシーポリシーに重大な影響を与えるような変更を行わないこと。

(6)　個人情報の保持期間の定義

サービス提供期間(利用者と合意した機関)を超えて個人を特定する情報を保持しないこと。

(7)　個人情報の利用目的

個人情報を収集、使用、共有及び保持するのは、教育機関、教職員、又は利用者によって承認された目的に限ること。

(8)　個人情報の取扱いについての情報開示

個人情報の取扱いについて、契約又はプライバシーポリシーで明確に示すこと。

(9)　利用者による個人情報管理

個人情報の登録、変更、削除に関するサービスを利用者に提供すること。

(10)　個人情報の適正管理

個人情報に対する不正アクセス又は個人情報の紛失、破壊、改ざん、漏洩、盗難等のリスクに対し、適切な安全対策を講じること。また、個人情報を正確にかつ最新の状態で管理すること。

(11)　再委託

サービス提供の全部又は一部を第三者に再委託、又は代行実施させる場合には、個人情報保護法制等を遵守し、当該再委託先又は代行実施先について、同等の義務を課し、管理すること。

(12)　合併・買収

合併ま又は他社による買収を行う場合、後継企業が以前に収集していた個人情報について、同様の義務を負うことを条件に、個人情報を継続して管理するものとすること。

１０．点検・評価・見直し

(1)　実施方法

教育情報統括責任者及び学校教育情報セキュリティ責任者は、所管する教育情報システム及び教育ネットワーク等の情報資産における情報セキュリティ対策状況について、定期的又は必要に応じて、点検を行わなければならない。また、外部委託事業者に委託している場合、外部委託事業者から下請けとして受託している事業者も含めて、このポリシーの遵守について、

定期的又は必要に応じて、点検を行わなければならない。

(2)　報告

教育情報統括責任者及び学校教育情報セキュリティ責任者は、情報セキュリティ対策状況についての点検結果を教育情報統括管理責任者に報告する。

(3)　保管

教育情報統括責任者及び学校教育情報セキュリティ責任者は、点検の実施を通して収集した点検結果、点検報告書作成のための調書等を、紛失が発生しないように適切に保管しなければならない。

(4)　点検結果への対応

教育情報統括責任者及び学校教育情報セキュリティ責任者は、点検結果に基づき、必要な改善を行わなければならない。また、点検結果において、このポリシーの記載事項に疑義が生じた場合には、速やかに教育情報統括管理責任者に報告し、対処しなければならない。

(5)　教育情報セキュリティポリシー及び関係規程等の見直し・変更

ア　教育情報統括管理責任者及び教育情報統括責任者は、新たに必要な対策が発生した場合又は点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、このポリシー及び関係規程等について、定期的に又は必要に応じて評価を行い、必要があると認めた場合、見直し、変更等を行わなければならない。

イ　教育情報統括管理責任者及び教育情報統括責任者は、教育情報セキュリティ対策基準の変更を行った場合には、速やかに学校教育情報セキュリティ責任者及びその他関係者に周知を行わなければならない。

ウ　教育情報統括責任者は、所管する教育情報システム及び教育ネットワーク等について、このポリシーの変更並びに情報セキュリティに関する状況の変化等に応じて、適宜情報セキュリティ対策の見直しを行い、必要があると認めた場合、当該システム及びネットワークの関係規程の変更を行わなければならない。