斜里町立学校情報セキュリティポリシー

令和６年１２月

斜里町教育委員会

目次

序　斜里町立学校情報セキュリティポリシーの構成

斜里町立学校情報セキュリティポリシーとは、学校が所掌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、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、学校が所掌する情報資産に関する業務に携わる学校長、教頭、教諭、養護教諭、事務官、公務補等（以下「教職員」という。）に浸透、普及、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。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、本セキュリティポリシーを町立学校における情報セキュリティ対策の最上位に位置づけ、一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、①情報セキュリティ基本方針②情報セキュリティ対策基準の２階層に分け、それぞれを策定することとする。

情報セキュリティポリシーの構成

文書名		内容
斜里町立学校情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための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。

第１章　情報セキュリティ基本方針

１．目的

斜里町立学校が取り扱う情報には、児童・生徒の個人情報のみならず、保護者等の情報など、部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報を、様々な脅威から防御することは、学校にかかわる町民の財産、プライバシー等を守るため、また、安定的な学校運営のためにも必要不可欠である。ひいては、このことが斜里町立学校に対する町民からの信頼の維持向上に寄与するものである。さらに近年、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大しており、学校現場においても ICT 教育の更なる発展が期待されているところである。斜里町立学校がこれらに積極的に対応するためには、学校現場における全てのネットワークと管理しているすべての情報システムが高度な安全性を有することが不可欠な前提条件となる。

よって、基本方針は、斜里町立学校が保有する情報資産を様々な脅威から防御し、機密性、完全性及び可用性を維持するため、斜里町立学校の情報セキュリティ対策の統一的かつ基本的な考え方及び方策を定め、情報資産の管理を徹底することを目的とする。

２．定義

（１）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。

（２）情報資産

情報システムで取扱う全てのデータ及び行政情報のことで、町立学校が保有している以下の資産のこと。

①情報

１）住民情報

２）企業や団体情報

３）契約書、帳票類、運用手順書等の文書・記録

４）その他重要情報

②情報システム

１）ハードウェア

２）ソフトウェア

３）ネットワーク

４）電子記憶媒体

（３）教職員等

臨時的任用教職員、非常勤講師を含めた教職員全員（以下「教職員等」という。）及び町立学校管理下で業務を行う要員のこと。

（４）情報システム

コンピュータ、ネットワーク及び記憶媒体で構成され、情報処理を行う仕組みをいう。

（５）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（６）電子記憶媒体

行政情報の記録、管理に使用される文書、図面、写真、ファイル及び電磁的記録（電子的方式、電磁的方式、その他の人の知覚によっては認識することができない方式で作られた記録をいう。）で磁気ディスク、磁気テープ、光ディスク等の媒体をいう。

（７）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（８）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。

（９）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。

(10) 可用性

情報にアクセスすることを認められた者が、必要な時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。

(11) セキュリティインシデント

システム障害、機密漏えい、被災等、人為的ミスを含む情報セキュリティ事件・事故のこと。

(12) 脅威

情報資産の機密性、完全性、可用性を失わせ、損失を発生させる直接の要因のこと。

(13) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の

詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、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えい・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、水道供給途絶等の提供サービスの障害からの波及等

４．適用範囲

（１）行政機関等の範囲

本対策基準が適用される行政機関等は、教育委員会及び斜里町立学校設置条例（昭和５３年条例１７号）第２条に掲げる小中学校及び義務教育学校をいう。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① 教育 ネットワーク、教育 情報システム、これらに関する設備、電磁的記録媒体

② 教育 ネットワーク及び 教育 情報システムで取り扱う情報（これらを印刷した文書を含む。

③ 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

５．教職員等の遵守義務

学校が所掌する情報資産に関する業務に携わる全ての教職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって学校情報セキュリティポリシー及び学校情報セキュリティ実施手順を遵守しなければならない。

６．情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）組織体制

斜里町の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制と、学校を含む管理体制を確立する。

（２）情報資産の分類と管理

斜里町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行う。

（３）物理的セキュリティ

サーバ等、コンピュータ室等、通信回線等及び職員等のパソコン等の管理について、

物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び技術的対策を講じる。

（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、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画の策定に努める。

（７）業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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。

外部サービスを利用する場合には、利用にかか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、利用するソーシャルメディアサービスごとの責任者を定める。

（８）評価・見直し

情報セキュリティ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情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、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。

８．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため、新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

９．情報セキュリティ対策基準の策定

上記６，７及び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情報セキュリティ対策基準を策定する。

１０．情報セキュリティに関する違反への対応

本ポリシー、その他の関連規定等に違反した場合は、その重大性、発生した事案の状況に応じて条例や規定等に基づき、懲戒処分等の対象とする。

１１．情報セキュリティ実施手順の策定

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。

なお、情報セキュリティ実施手順は、公にすることにより町立学校の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

斜里町立学校における情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、教育委員会及び町立学校の情報資産に関する情報セキュリティ対策の基準である。

１．対象範囲

（１）行政機関の範囲

本対策基準が適用される行政機関等は、斜里町教育委員会及び斜里町立学校設置条例（昭和５３年条例１７号）第２条に掲げる小中学校及び義務教育学校をいう。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

（３）用語説明

本対策基準における用語は、以下のとおりとする。

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・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
校務外部接続系情報（公開系情報）	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
学習系情報	児童生徒のワークシート、作品など、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
校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	校務外部接続系情報にアクセス可能な端末
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
指導者用端末	学習系情報にアクセス可能な端末で、教員教員のみが利用可能な端末
支給端末	教育委員会が学校に設置している校務及び指導者用端末

校務系システム	校務系ネットワーク、校務系サーバ及び及び校務用端末から構成される校務系情報を取り扱うシステム 及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム 及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

２．組織体制

（１）最高情報セキュリティ責任者（ＣＩＳＯ）

①副町長を、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、斜里町における全てのネットワーク、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最終決定権限及び責任を有する。

②最高情報セキュリティ責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

（２）統括教育情報セキュリティ責任者

①教育長を、CISO 直属の統括教育情報セキュリティ責任者とする。統括教育情報セキュリティ責任者は CISO を補佐しなければならない。

② 統括教育情報セキュリティ責任者は、斜里町の全ての教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 統括教育情報セキュリティ責任者は、斜里町の全ての教育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。

④ 統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者、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教育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。

⑤ 統括教育情報セキュリティ責任者は、斜里町の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、CISO の指示に従い、CISO 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行う権限及び責任を有する。

⑥ 統括教育情報セキュリティ責任者は、斜里町の共通的な教育ネットワーク、教育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・管理を行う権限及び責任を有する。

⑦ 統括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑧ 統括教育情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。

（3）教育情報セキュリティ責任者

① 教育委員会教育部長を教育情報セキュリティ責任者とする。

② 教育情報セキュリティ責任者は、本町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。

③ 教育情報セキュリティ責任者は、本町において所有している教育情報システムにおける開発、設定の変更、運用、見直し等を行う際の情報セキュリティ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責任者は、本町において所有している教育情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等（教職員、非常勤教職員及び臨時教職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

（4）教育情報セキュリティ管理者

① 校長を、教育情報セキュリティ管理者とする。

② 教育情報セキュリティ管理者は当該学校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。

③ 教育情報セキュリティ管理者は、当該学校において、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責任者、統括教育情報セキュリティ責任者及びCISO へ速やかに報告を行い、指示を仰がなければならない。

（5）教育情報システム管理者

① 教育委員会学校教育課長を、教育情報システムに関する教育情報システム管理者とする。

② 教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、

運用、見直し等を行う権限及び責任を有する。

③ 教育情報システム管理者は、所管する教育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。

④ 教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（６）教育情報システム担当者

① 教育委員会学校教育課総務係長及び学校教育係長を、教育情報システムに関する教育情報システム担当者とする。

② 教育情報システム担当者は、教育情報システム管理者の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の作業を行う。

（７）兼務の禁止

① 情報セキュリティ対策の実施においては、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。

② 情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

（８）教職員等

① 臨時的任用教職員、非常勤講師を含めた教職員全員を、教職員等と称する。

② 教職員等は学校が所管する情報資産を取り扱う立場にあり、教育情報セキュリティ管理者の指導の下、情報セキュリティを遵守しなければならない。

（９）教育委員会事務局職員

① 教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局職員を指す。

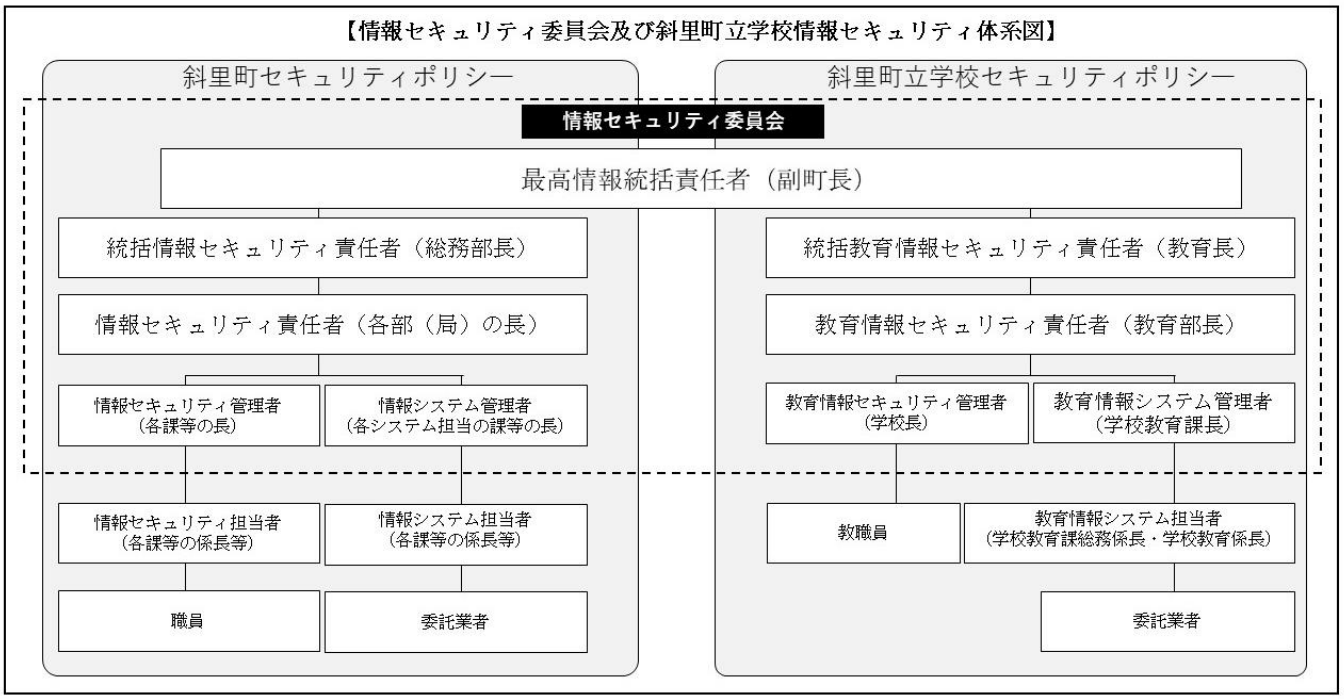
② 教育委員会事務局職員は学校の情報資産にアクセスできる立場にあり、教育情報セキュリティ責任者の指導の下、情報セキュリティを遵守しなければならない。

（１０）情報セキュリティ委員会

① 斜里町の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

② 情報セキュリティ委員会は、毎年度、斜里町における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

【斜里町立学校情報セキュリティ組織体系図】



３．情報資産の分類と管理方法

（１）情報の分類

斜里町における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じて取扱制限を行うものとする。

【機密性による情報資産の分類】

分類	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	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を含む）
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）

※機密性：情報にアクセスすることが許可された者だけがアクセスできることを確実にすること。

【完全性による情報資産の分類】

分類	分類基準	該当する情報のイメージ
完全性２B	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学区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確な遂行に軽微な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、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

※完全性：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

【可用性による情報資産の分類】

分類	分類基準	該当する情報のイメージ
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（軽微なものを除く）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	可用性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

※可用性：許可された利用者が必要な時に情報にアクセスできることを確実にすること。

（２） 情報資産の管理

① 管理責任

（ア） 教育情報セキュリティ管理者は、その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、複製等された情報資産も（１）の分類に基づき管理しなければならない。

② 情報資産の分類の表示

教職員等は、情報資産について、その分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

③ 情報の作成

（ア） 教職員等は、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（１）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。

④ 情報資産の入手

（ア） 学校内の者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り扱いをしなければならない。

（イ） 学校外の者が作成した情報資産を入手した者は、（１）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、その情報資産の分類が不明な場合、教育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。

⑤ 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） 情報資産を利用する者は、情報資産の分類に応じ、適切な取り扱いをしなければならない。

（ウ） 情報資産を利用する者は、電磁的記録媒体または保存されている領域（フォルダやサーバ）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または保存されている領域を取り扱わなければならない。

⑥ 情報資産の保管

（ア） 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、情報資産の分類に従って、情報資産を適切に保管しなければならない。

（イ） 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、情報資産を記録した電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。

（ウ） 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、機密性２A 以上、完全性２A 以上又は可用性２A 以上の情報を記録した電磁的記録媒体を保管する場合、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管するよう努めなければならない。

⑦ 情報の送信

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、情報資産分類に応じ以下を実施しなければならない。

（ア）電子メールにより機密性２A 以上の情報を外部送信する者は、限定されたアクセスの措置設定を行わなければならない。

（イ）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、電子メール等による外部送信の安全性を高めるため、添付される情報資産を監視する等、出口対策を実施しなければならない。

⑧ 情報資産の運搬

（ア） 車両等により機密性２A 以上の情報資産を運搬する者は、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、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２A 以上の情報資産を運搬する者は、教育情報セキュリティ管理者に許可を得なければならない。

⑨ 情報資産の提供・公表

（ア） 機密性２A 以上の情報資産を外部に提供する者は、限定されたアクセスの措置設定（アクセス制限や暗号化、パスワード設定等）を行わなければならない。

（イ） 機密性２A 以上の情報資産を外部に提供する者は、教育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） 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、住民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。

⑩ 情報資産の廃棄

（ア） 機密性２A 以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置したうえで廃棄しなければならない。

（イ） 情報資産の廃棄を行う者は、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） 情報資産の廃棄を行う者は、教育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．物理的セキュリティ

４－１　サーバ等の管理

（１）機器の取付け

教育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、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切に固定する等、必要な措置を講じるよう努めなければならない。

（２）サーバの冗長化

① 教育情報システム管理者は、校務系サーバその他の校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、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、システムの運用停止時間を最小限にしなければならない。

② 教育情報システム管理者は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを冗長化しなければならない。

（３）機器の電源

① 教育情報システム管理者は、統括教育情報セキュリティ責任者及び施設管理部門と連携し、校務系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。

② 教育情報システム管理者は、統括教育情報セキュリティ責任者及び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。

（４）通信ケーブル等の配線

① 統括教育情報セキュリティ責任者及び教育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等を防止するために、配線収納管を使用する等必要に応じて措置を講じなければならない。

② 統括教育情報セキュリティ責任者及び教育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 統括教育情報セキュリティ責任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切に管理しなければならない。

④ 統括教育情報セキュリティ責任者、教育情報システム管理者は、自ら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以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

（５）機器の定期保守及び修理

① 教育情報システム管理者は、可用性2A以上のサーバ等の機器の定期的に保守を実施

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、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、教育情報システム管理者は、外部の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とともに秘密保持体制の確認等を行わなければならない。

（６）施設外又は学校外への機器の設置

統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、CISO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。

（７）機器の廃棄等

教育情報システム管理者は、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。

４－２　管理区域（電算室）の設置

（１）管理区域の構造等

① 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワークの基幹機器及び重要な情報システムについて、サーバラック等の施錠管理を行わなければならない。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、サーバラック等を、立ち入りを許可されていない不特定多数の者が出入りできる場所に設置してはならない。

④ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

⑤ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じるよう努めなければならない。

⑥ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（２）管理区域の入退室管理等

① 教育情報システム管理者は、管理区域への入退室を許可された者のみに制限すること。

② 教育情報システム管理者は、サーバラック等の施錠管理にあたり、管理簿の記載等による管理を行わなければならない。

③ 教職員は、児童生徒が管理区域に入室する場合、必要に応じて立ち入り区域を制限した上で、児童生徒に付き添うものとする。

④ 外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

⑤ 教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された教職員等が付き添うものとし、外見上教職員等と区別できる措置を講じなければならない。

（３）機器等の搬入出

① 教育情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ委託した業者に確認を行わせなければならない。

② 教育情報システム管理者は、情報システム室の機器等の搬入出について、管理区域への入退室を許可された教職員を立ち会わせなければならない。

４－３　通信回線及び通信回線装置の管理

（１）統括教育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。

（２）統括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該当ポイントに接続される端末を正確に把握し、適切な管理を行わなければならない。

（３）統括教育情報セキュリティ責任者は、機密性２A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、通信経路上での暗号化を行わなければならない。

（４）統括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。

（５）統括教育情報セキュリティ責任者は、可用性２B 以上の情報資産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。

（６）統括教育情報セキュリティ責任者は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講じなければならない。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す配慮を含めてネットワーク構成を設計する。また、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。

４－４　教職員等の利用する端末や電磁的記録媒体等の管理

（１）教育情報システム管理者は、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、加えて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、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）教育情報システム管理者は、校務系システム、教育情報システムへアクセスする端末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）教育情報システム管理者は、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）教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定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、校務情報等の重要な情報資産へのアクセスについては、多要素認証を必須とすること。

（５）教育情報システム管理者は、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。端末に暗号化機能を持つセキュリティ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。

（６）教育情報システム管理者は、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情報資産を取り扱う端末に対し、当該データ暗号化等の措置により、不正アクセスや教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。

（７）教育情報システム管理者は、モバイル端末の学校外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

（８）教育情報システム管理者は、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。なお、OSによっては標準的にウイルス対策ソフトを備えている製品、OSとしてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。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情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

（９）教育情報システム管理者は、インターネットへ接続をする場合、教職員等のパソコン、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。

４－５　学習者用端末のセキュリティ対策

（１）不適切なウェブページの閲覧防止

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。

＜対策例＞

①フィルタリングソフト

②検索エンジンのセーフサーチ

③セーフブラウジング

（２）マルウェア感染対策

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。

（３）端末を不正利用させないための防止策

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。

（４）セキュリティ設定の一元管理

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、離れた場所からでも一元管理できることが望ましい。

（５）端末の盗難・紛失時の情報漏洩対策

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洩を防ぐ等の安全管理措置を講じなければならない。

４－６パソコン教室等における学習者用端末や電磁的記録媒体の管理

（１）教育情報システム管理者は、盗難防止のため、教室等で利用するパソコンの保管庫による管理等の物理的措置を講じなければならない。

（２）教育情報システム管理者は、パソコン及び電磁的記録媒体について、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。

（３）教育情報システム管理者は、情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定しなければならない。

５．人的セキュリティ

（１）教職員等の情報セキュリティポリシーの遵守

教職員等は、学校情報セキュリティ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、遵守することが困難な点等がある場合は、速やかに教育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。

（２）執務上での管理

① 執務室の施錠管理執務室にて教職員等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。

② 机上の書類・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）支給端末の取り扱い

（ア）教職員等は、業務目的以外で支給端末を利用してはならない。

（イ）教職員等は、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。業務上必要な場合には、事前に学校セキュリティ管理者の許可を得ること。

（ウ）教職員等は、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。

(a)セキュリティ機能に関する設定変更

(b)メモリ増設等の改造

（エ）教職員等は、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。

（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

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、業務上必要な場合は、教育情報セキュリティ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、教育情報セキュリティ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。

（５）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（本ガイドライン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 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、教育情報セキュリティ管理者の許可を得なければならない。

② 教職員等は、外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

（６）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。

③ 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、統括教育情報セキュリティ責任者又は教育情報システム管理者に通知しなければならない。

（７）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、教育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。

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 教職員等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）

⑨ 共有IDに対するパスワードは定期的に又はアクセス回数に基づいて変更しなければならない。

（８）ICカード等の取扱い

教職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。

① 認証に用いるICカード等を、教職員等間で共有してはならない。

② 業務上必要のないときは、ICカード等をカードリーダ若しくはパソコン等の端末のスロット等から抜いておかなければならない。

③ ICカード等を紛失した場合には、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に通報し、指示に従わなければならない。

（９）外部電磁的記録媒体の取り扱い

① 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。その他の媒体の使用は禁止。

② 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。

（１０）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が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統括教育情報セキュリティ責任者の許可無しに使用してはならない。

⑥ 情報ファイルを添付する場合には、必要に応じて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 。

⑦ 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。

⑧ 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、教育情報セキュリティ管理者に指示を仰ぎなければならない。

（１１）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

① 機密性２A以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。なお、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は、その限りではない。

② 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 。

③ 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。

（１２）不正プログラム対策に関する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。 OS及びコンピュータウイルス対策 ソフトウェアが常に最新の状態に保てるようにしなければならない。自動更新される設定の場合は、自動更新設定を変えてはならない。

② 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うなど対策を講じるよう努めなければならない。

⑥ 統括教育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、すみやかに教育情報セキュリティ管理者に報告し、指示を仰がなければならない。また、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（校務用端末等）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（指導者用端末及び学習者用端末）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。

（１３）電子署名・暗号化

① 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、CISOが定めた電子署名、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。

② 教職員等は、暗号化を行う場合にCISOが定める以外の方法を用いてはならない。また、CISOが定めた方法で暗号のための鍵を管理しなければならない。

③ CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（１４）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、統括教育情報セキュリティ責任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。

③ 教職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１５）機器構成の変更の制限

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、業務上、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、統括教育情報セキュリティ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。

（１６）無許可でのネットワーク接続の禁止

教職員等は、統括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。

（１７）業務以外の目的でのウェブ閲覧の禁止

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。

（１８）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、教育情報セキュリティ管理者を介して、統括教育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教育情報システム管理者の許可を得なければならない。

② 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、アンチウイルス等を通じて、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。

（１９）児童生徒への指導事項

教職員等は、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。

① 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。

② 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。

③ 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。

④ 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。

⑤ 学習系情報は学習系クラウドに保管

端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して 原則 学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。

⑥ 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。

⑦ 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。

⑧ 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。

⑨ 端末の安全な取り扱い 学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

⑩ 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

（２０）異動・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（紙情報、データの格納された端末、外部記録媒体等）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。

（２１）研修・訓練

①情報セキュリティに関する研修・訓練

（ア） 最高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） 最高情報セキュリティ責任者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

②研修計画の立案及び実施

（ア） 最高情報セキュリティ責任者は、幹部を含めすべての職員等に対する情報セキュリティに関する研修計画を定期的に立案し、情報セキュリティ委員会の承認を得なければならない。

（イ） 新規採用の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） 研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

（エ） 最高情報セキュリティ責任者は、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

③情報セキュリティポリシーの遵守

教育情報セキュリティ管理者は、教職員等が常に学校情報セキュリティポリシーを閲覧できるように掲示しなければならない。

④委託事業者に対する説明

教育情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、学校

情報セキュリティポリシーのうち、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。

⑤緊急時対応訓練

最高情報セキュリティ責任者は、緊急時対応を想定した訓練を必要に応じて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。

⑥研修・訓練への参加

幹部を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

（２２）事故、欠陥等の報告

①職場内からの事故等の報告

（ア） 職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかに情報セキュリティ管理者に報告の上、必要な指示を仰がなければならない。

（イ） 報告を受けた情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。

（ウ） 情報セキュリティ管理者は、報告のあった事故等について、必要に応じて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。

（エ） 情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

②住民等外部からの事故等の報告

（ア） 職員等は、斜里町が管理するネットワーク及び情報システム等の情報資産に関する事故欠陥について、住民等外部から報告を受けた場合、情報セキュリティ管理者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、速やかに統括教育情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

（ウ） 教育情報セキュリティ管理者は、当該事故等について、必要に応じて最高情報セキュリティ責任者及び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。

（エ） 最高情報セキュリティ責任者は、情報システム等の情報資産に関する事故、欠陥について、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。

（オ） 統括教育情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

③事故等の原因の究明・記録、再発防止等

（ア） 情報セキュリティ委員会は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

（イ） 情報セキュリティ委員会は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告しなければならない。

（ウ） 情報セキュリティ委員会は、情報セキュリティインシデントに関係する教育情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

（エ） 情報セキュリティ委員会は、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、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。

（オ） 最高情報セキュリティ責任者は、情報セキュリティ委員会から、事故等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に必要な措置を指示しなければならない。

６．技術的セキュリティ

６－１　コンピュータ及びネットワークの設定管理

（１）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、特定の教職員等しか取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、個人情報などを含む重要性が高い情報を保管する場合に限る）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、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。

（２）バックアップの実施

統括教育情報セキュリティ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、次の①及び②に基づきバックアップを実施するものとする。

① 校務系情報及び校務外部接続系情報については、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。

② 学習系情報については、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。

（３）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、統括教育情報セキュリティ責任者及び教育情報セキュリティ責任者の許可を得なければならない。

（4）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。

② 統括教育情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システムの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切に管理しなければならない。

③ 統括教育情報セキュリティ責任者、情報システム管理者また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。

（5）情報システム仕様書等の管理

統括教育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、適切に管理しなければならない。

（6）ログの取得等

① 統括教育情報セキュリティ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 統括教育情報セキュリティ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 統括教育情報セキュリティ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。

（７）障害記録

統括教育情報セキュリティ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。

（８）ネットワークの接続制御、経路制御

① 統括教育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、ルーター等の通信ソフトウェア等を設定しなければならない。

② 統括教育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。

（９）外部の者が利用できるシステムの分離

教育情報システム管理者は、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、特に情報資産重要性分類２Ｂ（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情報資産）以上を扱うシステムとの論理的又は物理的な分離、も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。

（１０）外部ネットワークとの接続制限

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、CISO及び統括教育情報セキュリティ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資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。

④ 統括教育情報セキュリティ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、統括教育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。

（１１）複合機のセキュリティ管理

① 統括教育情報セキュリティ責任者は、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 統括教育情報セキュリティ責任者は、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 統括教育情報セキュリティ責任者は、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。

（１２）IoT 機器を含む特定用途機器のセキュリティ管理

統括教育情報セキュリティ責任者は、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。

（１３）無線ＬＡＮ及びネットワークの盗聴対策

① 統括教育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づけなければならない。

② 統括教育情報セキュリティ責任者は、機密性の高い情報を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。

（１４）電子メールのセキュリティ管理

① 教職員等は、電子メールの送受信にあたっては、教育情報システム管理者が指定した電子メールソフトウェアを利用しなければならない。

② 教職員等は、教育情報システム管理者の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。

③ 統括教育情報セキュリティ責任者は、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、電子メールサーバの設定を行わなければならない。

④ 統括教育情報セキュリティ責任者は、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。

⑤ 統括教育情報セキュリティ責任者は、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。

⑥ 統括教育情報セキュリティ責任者は、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。

⑦ 統括教育情報セキュリティ責任者は、システム開発や運用、保守等のため施設内に常駐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。

⑧ 教職員等は、重要情報（パスワード、個人情報等）は、原則として電子メールを用いて送信してはならない。

⑨ 統括教育情報セキュリティ責任者は、教職員等が電子メールの送信等により情報資産を無断で職場外に持ち出すことが不可能となるように、添付ファイルの監視等によりシステム上措置しなければならない。

（１５）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・転送してはならない。

③ 教職員等は、電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上、送信しなければならない。

④ 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が分からないようにしなければならない。

⑤ 教職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

⑥ 教職員等は、必要がある場合を除き、ウェブで利用できるフリーメール、ネットワークストレージ等を使用してはならない。

（１６）電子署名・暗号化

① 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、最高情報セキュリティ責任者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

② 教職員等は、暗号化を行う場合に最高情報セキュリティ責任者が定める以外の方法を用いてはならない。また、最高情報セキュリティ責任者が定めた方法で暗号のための鍵を管理しなければならない。

③ 最高情報セキュリティ責任者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（１７）無許可ソフトウェアの導入等の禁止

① 教職員等は、パソコン等の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、統括教育情報セキュリティ責任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の管理、セキュリティ上の問題点が解決済みであるかの確認、供給者の連絡先及び更新情報が明確であるかの確認を行わなければならない。

③　教職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１８）機器構成の変更の制限

①　教職員等は、パソコン等の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、業務上、パソコン等の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、統括教育情報セキュリティ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。

（１９）無許可でのネットワーク接続の禁止

教職員等は、統括教育情報セキュリティ責任者の許可なくパソコン等の端末をネットワークに接続してはならない。

（２０）業務以外の目的でのウェブ閲覧の禁止

①　教職員等は、ウェブブラウザの利用にあたって、情報システム管理者が指定したウェブブラウザの設定を施さなければならない。

②　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。

③　教職員等は、業務上不必要なバナー広告はクリックしてはならない。

④　教職員等は、業務上不必要なファイルやソフトウェア、不審なファイル等をダウンロードしてはならない。

⑤　統括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。

（２１）Web 会議サービスの利用時の対策

①　統括教育情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めるよう努めなければならない。

②　教職員等は、斜里町の定める利用手順に従い、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。

③　教職員等は、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講ずること。

④　教職員等は、外部から Web 会議に招待される場合は、斜里町の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

（２２）ソーシャルメディアサービスの利用

①　教育情報セキュリティ管理者は、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）本町のアカウントによる情報発信が、実際の本町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 Web 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（ハードディスク、USB メモリ、紙等）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 機密性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 アカウント乗っ取りを確認した場合には、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。

⑤ 可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、斜里町の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

６－２　アクセス制御

（１）アクセス制御等

① アクセス制御

統括教育情報セキュリティ責任者又は教育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。

② 利用者ＩＤ・パスワードの取扱い

（ア）統括教育情報セキュリティ責任者及び教育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、教職員等の異動、出向、退職者に伴う利用者ＩＤ・パスワードの取扱い等の方法を定め、ＩＤ・パスワードが登録されている教職員等の情報を記録し、維持しなければならない。

（イ）教職員等は、業務で使用する端末は、ユーザＩＤとパスワードで保護しなければならない。

（ウ）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、統括教育情報セキュリティ責任者又は教育情報システム管理者に通知しなければならない。

（エ）統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用されていないＩＤ・パスワードが放置されないよう、定期的に点検しなければならない。

（オ）統括教育情報セキュリティ責任者及び教育情報システム管理者は、異動等により、庁内システムや端末を使用しなくなった教職員等、又は退職した教職員等のユーザＩＤとパスワードは直ちに削除しなければならない。

③ 特権を付与されたＩＤの管理等

（ア）統括教育情報セキュリティ責任者及び教育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。

（イ）統括教育情報セキュリティ責任者及び教育情報システム管理者の特権を代行する者は、統括教育情報セキュリティ責任者及び教育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。

（ウ）最高情報セキュリティ責任者は、代行者を認めた場合、速やかに統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、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に通知しなければならない。

（エ）統括教育情報セキュリティ責任者及び教育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。

（オ）統括教育情報セキュリティ責任者及び教育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、教職員等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。

（カ）統括教育情報セキュリティ責任者及び教育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。

（２）教職員等による職場外からのアクセス等の制限

① 教職員等が職場外からネットワーク又は情報システムにアクセスする場合は、統括教育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教育情報システム管理者の許可を得なければならない。

② 統括教育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職場外からのアクセスを認める場合、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 統括教育情報セキュリティ責任者は、職場外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 統括教育情報セキュリティ責任者は、職場外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 職員等は、職場外から持ち帰ったパソコン等の端末を庁内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。

⑥ 統括教育情報セキュリティ責任者は、外部から教育ネットワークに接続することを許可する場合は、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、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）自動識別の設定

統括教育情報セキュリティ責任者及び教育情報システム管理者は、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よう努めなければならない。

（4）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及びログイン試行回数の制限、アクセスタイムアウトの設定、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。

（5）パスワードに関する情報の管理

① 統括教育情報セキュリティ責任者又は教育情報システム管理者は、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。

② 統括教育情報セキュリティ責任者又は教育情報システム管理者は、本人であることを確認の上、教職員等に対してパスワードを発行する。

（6）特権による接続時間の制限

教育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。

６－３システム開発、導入、保守等

（１）情報システムの調達

① 統括教育情報セキュリティ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 統括教育情報セキュリティ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。

（２）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

（ア）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。

（イ）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

（ア）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。

（イ）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。

（３）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

(ア)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とシステム運用環境を分離しなければならない。

(イ)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環境への移行について、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。

(ウ)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。

(エ)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

(ア)教育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。

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

(ウ)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。

(エ)教育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。

(オ)教育情報システム管理者は、運用環境への移行に先立ち、システムの脆弱性テストを行い、その結果を確認しなければならない。

（4）システム開発・保守に関連する資料等の整備・保管

① 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。

② 教育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。

③ 教育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ならびに使用したオープンソースのバージョン（リポジトリ）を適切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

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。

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。

（6）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。

（7）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。

（８）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。

６－４不正プログラム対策

（１）統括教育情報セキュリティ責任者の措置事項

統括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などにおいてコンピュータウィ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 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などにおいてコンピュータウィ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 コンピュータウィ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、コンピュータウィ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の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 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦ 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。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しなければならない。

（２）教育情報システム管理者の措置事項

教育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。

① 教育情報システム管理者は、その所掌するサーバ及びパソコン等の端末を守るため、コンピュータウイルス等の不正プログラムへの対策を講じなければならない。

② 不正プログラム対策は、常に最新の状態に保たなければならない。

③ 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う場合、コンピュータウイルス等の感染を防止するために、市が管理している電磁的記録媒体以外を教職員等に利用させてはならない。また、不正プログラムの感染、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）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 パソコン等の端末において、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。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しなければならない。

⑥ 統括教育情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦ 情報システム管理者の指示に従い、当該ソフトウェアのバージョンアップ及びセキュリティパッチの適用を行わなければならない。

⑧ 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は、ＬＡＮケーブルの即時取り外しを行い、完全に駆除が終了するまでＬＡＮケーブルの再接続と該当する端末での作業を行ってはならない。

（４）専門家の支援体制

統括教育情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、専門家等の支援体制を講じるものとする。

６－５不正アクセス対策

（１）統括教育情報セキュリティ責任者の措置事項

統括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を閉鎖しなければならない。

② 不要なサービスについて、機能を削除又は停止しなければならない。

③ 情報システムへアクセス可能な機器は、必要最小限にし、不必要な機器は接続してはならない。

④ 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、統括教育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、設定しなければならない。

⑤ セキュリティホールを最小限に抑えるため、情報システムに、使用しないソフトウェアを搭載してはならない。

⑥ 不正アクセスを発見した場合、不正アクセスの被害の拡大及び再発防止のため、原因を分析し、再発防止対策を講じなければならない。

⑦ 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。

⑧ 統括教育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しなければならない。

⑨ 本町が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

⑩ クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

⑪ パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本町が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認しなければならない。

（２）攻撃の予告

最高情報セキュリティ責任者及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む措置を講じなければならない。また、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。

（３）記録の保存

最高情報セキュリティ責任者及び統括教育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。

（４）内部からの攻撃

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等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校内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。

（５）教職員等による不正アクセス

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等による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の教育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。

（６）サービス不能攻撃

統括教育情報セキュリティ責任者及び教育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。

（７）標的型攻撃

統括教育情報セキュリティ責任者及び教育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、教育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。

６－６セキュリティ情報の収集

（１）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

① 統括教育情報セキュリティ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、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、ソフトウェア更新等の対策を実施しなければならない。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本町の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

（２）不正プログラム等のセキュリティ情報の収集・周知

統括教育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、職員等に周知しなければならない。

（３）情報セキュリティに関する情報の収集及び共有

統括教育情報セキュリティ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国及び関係団体、民間事業者等から適宜収集し、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、セキュリティ侵害等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

７－１情報システムの監視

（１） 統括教育情報セキュリティ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。

（２） 統括教育情報セキュリティ責任者及び教育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。

（３） 統括教育情報セキュリティ責任者及び教育情報システム管理者は、機密性 2B 以上、完全性 2B 以上、可用性 2B 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。

７－２情報セキュリティポリシーの遵守状況の確認

（１）遵守状況の確認及び対処

① 教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、学校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統括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 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。

③ 統括教育情報セキュリティ責任者及び教育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学校情報セキュリティ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。

（２）端末及び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及び最高情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、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）教職員等の報告義務

① 教職員等は、学校情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括教育情報セキュリティ責任者及び教育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。

② 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統括教育情報セキュリティ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。

７－３侵害時の対応

（１）緊急対応計画の策定

最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティに関する事故、学校情報セキュリティポリシーの違反等により情報資産への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、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。

（２）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 再発防止措置の策定

（３）業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（４）緊急時対応計画の見直し

最高情報セキュリティ責任者又は情報セキュリティ委員会は、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。

7－4 例外措置

（1）例外措置の許可

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、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、最高情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

（2）緊急時の例外措置

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、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。

7－5 法令遵守

（1）教職員等は、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。

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 1 月 12 日法律第 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 斜里町個人情報保護条例（令和 5 年　条例第 2 号）
⑦ 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）
⑧ サイバーセキュリティ基本法（平成 26 年法律第 104 号）

（2）統括教育情報セキュリティ責任者及び教育情報システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

７－６懲戒処分等

（１）懲戒処分

学校情報セキュリティポリシーに違反した教職員等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、地方公務員法による懲戒処分の対象とする。

（２）違反時の対応

教職員等の学校情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

① 統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員等が所属する学校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。

② 教育情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括教育情報セキュリティ責任者及び当該教職員等が所属する学校の教育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。

③ 教育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、統括教育情報セキュリティ責任者は、当該教職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括教育情報セキュリティ責任者は、教職員等の権利を停止あるいは剥奪した旨を最高情報セキュリティ責任者及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知しなければならない。

７－７　児童生徒における ID 及びパスワード等の管理

（１）ID 登録・変更・削除

① 入学／転入時の ID 登録処理

ID についてはシンプル・ユニーク（唯一無二）・パーマネント／パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じなければならない。

② 進級／進学時の ID 関連情報の更新

ID については原則として進級／進学にも変更不要とすることが望ましい。そのため ID を変えることなく ID の属性情報（進級時の組・出席番号、進学先学校名など）の変更を行っておくことで、MDM による各種ポリシーや使用アプリケーションの変更を効率的に行うことが可能となる。さらに、統合型校務支援システム等における児童生徒の氏名と連動した ID 管理を行うことで、校務側で管理している属性情報と一体となった ID を含んだマスター管理の一元化が望ましい。

③ 転出／卒業／退学時の ID 削除処理

ユニークなID は、個人を識別できる可能性があるため、個人情報保護の観点から、サービス提供期間を超えて個人を特定する情報を保持しないようにする必要がある。転出や卒業／退学時に学習用ツールのサービス利用期間内に実施し、ID の利用停止後、最終的にはID 及び関連するデータの完全削除を行うこと。ただし、本人同意や個人情報保護条例に従った適切な管理の下、一部のデータを活用することは可能である。

（2）多要素認証によるなりすまし対策

成績評価につながるCBT（Computer Based Testing：試験における工程を全てコンピュータ上で行うこと）など、本人確認を厳格に行う必要がある場合においては、児童生徒のID／パスワードに加えて多要素認証を設定することが望ましい。

（3）学習用ツールへのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度ID／パスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定期間は各種サービスにアクセスが行えるシングルサインオンの導入を行うことが望ましい。

８．業務委託と外部サービスの利用

（1）業務委託

①委託事業者の選定基準

（ア） 教育情報セキュリティ管理者は、委託事業者の選定にあたり、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） 教育情報セキュリティ管理者は、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、委託事業者を選定しなければならない。

②契約項目

重要な情報資産を取扱う業務を委託する場合には、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。

・学校情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・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
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従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委託事業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義務
・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
・学校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

教育情報セキュリティ管理者は、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、②の契約に基づき措置を実施しなければならない。また、その内容を統括教育情報セキュリティ責任者に報告するとともに、その重要度に応じ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。

（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、機密性の高い情報の取り扱いには十分に留意する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
・利用手続き及び運用手順

（３）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。

９．評価・見直し

（１）監査

①実施方法

情報セキュリティ委員会は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム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、必要に応じて監査を行わせなければならない。

②監査を行う者の要件

（ア） 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

（イ） 監査を行う者は、監査及び情報セキュリティに関する専門知識を有するものでなければならない。

③監査実施計画の立案及び実施への協力

（ア）　情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

（イ）　被監査部門は、監査の実施に協力しなければならない。

④委託事業者に対する監査

（ア）　委託事業者に委託している場合、情報セキュリティ監査統括責任者は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、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（イ）　クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

⑤報告

情報セキュリティ監査統括責任者は、監査報告書を作成し、情報セキュリティ委員会に報告する。

⑥保管

情報セキュリティ監査統括責任者は、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を、紛失等が発生しないように適切に保管しなければならない。

⑦監査結果への対応

最高情報セキュリティ責任者は、監査結果により発見された問題点について、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、指摘事項の対処は、各課等で直ちに実行されなければならない。

⑧情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（２）自己点検

①実施方法

（ア）　統括教育情報セキュリティ責任者及び教育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、必要に応じて自己点検を実施しなければならない。

（イ）　教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する部局における学校情報セキュリティ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。

②報告

統括教育情報セキュリティ責任者、教育情報システム管理者及び教育情報セキュリティ責任者は、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、情報セキュリティ委員会に報告しなければならない。

③自己点検結果の活用

（ア） 教職員等は、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） 情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（3）学校情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティポリシーについて情報セキュリティ監査及び自己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ふまえ、必要があると認めた場合、改善を行うものとする。

第３章 斜里町学校情報セキュリティ実施手順

この実施手順は、斜里町立学校情報セキュリティポリシー（以下「ポリシー」という。）に基づいて、教職員等が教育情報セキュリティ対策を行うための具体的な手順を定めたものである。

１． 情報資産の管理

斜里町が保有する情報資産については、斜里町学校情報セキュリティポリシー対策基準（以下「対策基準」という。）によって定められた分類により重要度を分類し、適正に管理を行うこと。

（１）情報資産の管理方法

① 機密性３（秘情報）

職務上必要な限定された関係者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必ず実施するとともに、次のとおり必要な対策を取ること。

・外部ネットワークから分離したファイルサーバに保存するなど、職務上必要な者のみにアクセス権限を設定するよう努めなければならない。

・データもしくはフォルダにセキュリティ対策を設定するか、ファイルを暗号化する。

・その存在の有無についても、職務上必要な最低限の者以外に漏れないよう、厳格に扱う。

② 機密性２Ａ及び２Ｂ（関係者外秘情報）

関係者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必要に応じて実施するとともに、次のとおり必要な対策を取ること。

・外部ネットワークから分離したファイルサーバに保存するなど、関係者のみにアクセス権限を設定するよう努めなければならない。

・ファイル自身に適切なパスワードを設定するか、ファイルを暗号化する。

③ 機密性１（その他情報）

教職員等がアクセス可能であるため、情報の改ざんや偽情報の流布の防止のために、必要な対策を取ること。

（２）情報資産の複製、持ち出し及びメール送信

情報資産を複製、持ち出し及びメール送信する場合も、情報資産の分類に応じて、必要な対策を取ること。

① 機密性３（秘情報）

・職務上必要な限定された関係者のみにアクセス制限したフォルダに保存し、原則として、保管場所からの複製、持ち出し、及びメール送信はしない。

・やむを得ず保管場所以外に複製、持ち出し及びメール送信する場合は、教育情報セキ

ュリティ管理者の承認を事前に得るとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。

・情報資産の持ち出し時には、肌身離さず所持し、盗難、紛失等に十分注意する。

・複製、持ち出し及びメール送信した情報資産は、不要になり次第速やかに削除し、情報の漏えいを防ぐ。

② 機密性２Ａ及び２Ｂ（関係者外秘情報）

・関係者のみにアクセスできるファイルサーバに保管し、原則として、保管場所からの複製及び持ち出しはしない。

・やむを得ず保管場所以外に複製、持ち出す場合は、教育情報セキュリティ管理者の承認を事前に得るとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。

・情報資産の持ち出し時には、盗難、紛失等に十分注意する。

③ 機密性１（その他情報）

・外部ネットワークから分離したファイルサーバに保存し、原則として、保管場所からの複製及び持ち出しはしない。

・保管場所以外に複製及び持ち出す場合は、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。

・情報資産の持ち出し時には、盗難、紛失等に十分注意する。

（３）情報処理機器の廃棄について

情報処理機器の廃棄をする際には、情報資産の分類に関係なく、データの消去等を確実に行い、情報の漏えい防止のために、次のとおり必要な対策を取ること。

・データの消去には、破砕処理や、磁気によるデータの消去等を施し、データの復元ができないようにする。

・情報機器の記憶媒体を保守契約により交換する場合又はリース機器の撤去を行う場合は、撤去後の記憶媒体の処理方法についても保守業者に確認を取り、データ消去を確実にする。

・データの消去を外部に委託する際には、データ消去証明書等の提出を義務付ける。

２．セキュリティの確保

教職員等は、本町が保有する情報資産を守るため、当該情報資産を管理している教育情報セキュリティ管理者の指示の下、対策基準によって定められたセキュリティ対策を実施する。

（１）物理的セキュリティ

① 情報システムのセキュリティ対策

パソコン等の情報システムについては、次のとおり必要な対策を取ること。

・機器に適切なパスワードを設定し、不要なアクセスを防ぐ。

・パソコンを離れる際には、ロック画面（スクリーンセーバー）にするなど、他人にパソコンを閲覧されないようにする。
・外部記憶装置は、セキュリティ機能付きのものを使用する。
・私物の外部記憶装置を接続しない。

② 入室の制限

サーバ室のように重要な情報機器が設置してある部屋の管理については、次のとおり必要な対策を取ること。

・施錠管理し、不正な入室を防ぎ、入退室については入退室記録簿を備え管理を行うなどして対策を行う。
・入室できる者を制限する。また、入室を予定していない者が入室を行う際には、入室権限を持つ者が同行する又は部屋の管理者に事前に許可を得る。
・不正な入室が行われないように厳重に管理する。

③ 盗難の防止

情報システム及び情報資産（以下「情報資産等」という。）の盗難を防ぐために、次のとおり必要な対策を取ること。

・情報処理機器は、施錠管理できる部屋等に管理し、盗難防止の対策を取る。
・情報資産を管理するキャビネット等は、施錠管理を行うなど対策を講じる。

④ 災害対策

サーバ機器のような重要な情報処理機器のシステム停止を可能な限り防ぐために、次のとおり必要な対策を取ること。

・情報処理機器の備え付けにあたっては、耐震対策を十分に考慮する。
・災害により情報システムが停止しないように、構築時に冗長化を行う。
・災害等によりデータが消失することがないように、サーバ機器は定期的にバックアップを取る。
・停電等による不測のシステム停止によりハードウェア障害が起きないように、無停電電源装置等を用いて、電源断時に自動で終了処理を行う。

（２）人的セキュリティ

① 情報資産の管理

各学校は、教育情報セキュリティ管理者の指示の下、情報資産の重要度を適切に分類し、情報資産の管理を行うこと。

・情報資産の重要度を適切に設定する。
・機密性３及び機密性２Ａ及び２Ｂの権限範囲が適切であるか定期的に確認する。
・情報資産台帳等を作成し、守るべき情報資産を整理する。

② 情報セキュリティポリシーの徹底

教職員等は、ポリシーを遵守しなければならない。

・定期的にポリシーが遵守されているか確認する。

・情報セキュリティに関する研修に参加する。
・教育情報システム担当者から通知されるセキュリティ情報を確認し、セキュリティ対策を実施する。

③ パスワードの設定管理

教職員等は、パスワードの設定を行う際には、次のとおり設定すること。

・８文字以上のパスワードにするなど、推測しにくいパスワードを設定する。
・英字、数字、記号を組み合わせる。
・初期に設定されているパスワードは使用せず、必ず変更する。
・定期的にパスワードを変更する。
・パスワードをメモしたものを人目に付くところに置かない。
・パスワードを他人に教えない。
・複数のシステムに同じパスワードを設定しない。

④ 電子メールのセキュリティ対策

電子メールの利用の際には、次のとおり必要な対策を取ること。

・電子メール内に記載されている URL は、不用意にリンク先にアクセスすると、ウィルス感染、フィッシング詐欺等の危険があることから、URL に間違いがないか、信頼のおける URL であるかなど、十分に注意する。
・身に覚えのない送信主からのメールに添付ファイルがある場合、コンピュータウィルス感染しているファイルの可能性があるため、不用意に開封しない。開封する場合は、ウィルスチェックを行ってから開封する。
・電子メールの送信者のアドレスが正しいことを確認する。
・身に覚えのない送信主からのメール、明らかに不自然な内容のメール等は不用意に応答せず、必要に応じて情報システム担当者に相談する。
・送り先のメールアドレス入力の際には、間違いの無いように再チェックし送信する。
・添付ファイルを送信するときには、添付ファイルにパスワードを設定する。

（３） 技術的セキュリティ

① 情報システムのセキュリティ対策

パソコン等の情報システムについては、次のとおり必要な対策を取ること。

・導入しているウィルス対策ソフトをインストールし、リアルタイム検索を有効化すること。また、定期的にウィルス感染チェックを行うこと。
・OS 又はインストールされているソフトウェア等で、セキュリティの脆弱性が発覚した場合には、速やかにセキュリティアップデートを行う。
・不正なアクセスや攻撃を防ぐために、不要な常駐プログラム等を停止する。
・アカウントの管理者は、アカウントの整理を定期的に実施し、不要なアカウントは削除する。

・機器の利用は IP アドレス等で、利用可能な範囲を制限する。
・管理用途で遠隔から機器にアクセスする際は、IP アドレス制限やパスワード等でアクセスを制限し、不特定多数のアクセスを禁止する。
・不正なアクセスを防ぐため、不要なサービスは停止する。
・パスワード等の設定を行い、アクセスできる者を制限する。
・IP アドレスでの利用制限の設定を行い、不要なアクセスを防ぐ。
・登録された MAC アドレスやサブネット、IP アドレス以外から接続できないように設定する。
・校舎内ネットワーク接続パソコンからインターネット接続のため無線 LAN への接続は原則禁止とする。
・SNMP の設定をする場合は、IP アドレスによる接続制限やコミュニティ名を標準設定から変更するなど、不特定多数の読み書きができないようにする。

② ネットワークへの不正接続対策

ネットワークの接続口が不特定の者によって接続されないよう、次のとおり必要な対策をとること。

・不特定多数が出入りする部屋では、ケーブルを接続するだけで校舎内ネットワーク及びインターネットが利用できるようになる DHCP サーバの設置は行わない。
・ルータモードを持つ機器は校舎内ネットワークに設置しない。

３．禁止事項

本町の情報資産等を利用するにあたり、以下の行為はしてはならない。

（１） 法令に違反する行為

・閲覧権限及び利用権限のない情報資産等へ不正にアクセスする。
・情報資産等を破壊及び改ざんする。
・コンピュータウィルスを配布する。
・他人の写真や音声を当人に無断でホームページ等に公開する。
・他人の作成した文書、写真等を無断でホームページ等に公開する。
・有償ソフトウェアを無断でコピーして使用する。
・ファイル共有ソフト等を用いて、著作権のあるソフトウェア、音楽ファイル、動画ファイル等を入手したり、入手した情報を公開して提供したりする。
・その他、法令に違反するとみなされる行為。

（２）公序良俗に反する行為

・他人になりすまして、ネットワーク上で発言する。
・事実と異なる情報を意図的に流す。
・猥褻とみなされる文章や画像をホームページ等で公開する。
・人権、性別、思想信条などに基づく差別的な文章等をホームページ等で公開する。

・メーリングリスト等に他人を無断で登録する。
・他人のファイル等を当人に無断で参照する。
・その他、公序良俗に違反するとみなされる行為。

（3）本町の行政運営及び学校運営等に反する行為
・ネットワークを意図的に混雑させる。
・教育情報セキュリティ管理者や教育情報システム担当者の指示に従わない。
・データ量の多いファイル等をメールで大量に送る。
・アカウントの貸し借りを行う。
・業務上必要のないソフトウェアをダウンロードして利用する。
・その他、本町の行政運営及び学校運営に反するとみなされる行為。

4．インシデントに対する対応と報告

インシデントが発生した場合には、その被害を最小限に抑えるため、以下のとおり対応しなければならない。

（1）重要度の区分

インシデントが発生した場合には、その事象から、以下のように重要度を区分する。

区分	事象
重要度高	・本町（学校）の信用や利益を大きく損なうもの ・本町（学校）の業務・運営に支障があるもの ・違反行為の内容が法律等に違反するもの ・事象が重大で解決に時間を要するもの ・その他、重要度が高いと認められるもの
重要度低	・本町（学校）の信用や利益を損なう可能性がないもの ・本町（学校）の業務・運営に支障が少ないもの ・事象が軽微ですぐに対応が可能なもの

（2）インシデントに対する対応

① 教職員等は、インシデントを発見した場合には、「様式１インシデント報告書」にて、速やかに教育情報セキュリティ管理者に連絡をしなければならない。また、教育情報システム担当者にも同様に連絡をすること。

② 教育情報セキュリティ管理者は、インシデントが発生した場合には、速やかに事実関係の確認、問題の解決に努めるとともに、再発防止策の検討及び実施をしなければならない。

③ 教育情報セキュリティ管理者は、発生したインシデントの重要度に関わらず、統括教育情報セキュリティ責任者にインシデントの内容や対応状況、再発防止策等について報告しなければならない。この場合、統括教育情報セキュリティ責任者は、当該事象の重要度区分について判断する。

（3）「重要度高」と判断されたインシデントへの対応

① 報告

（ア）当該事象が発生した場合、教育情報セキュリティ管理者は、「インシデント報告書」を作成し、統括教育情報セキュリティ責任者へ提出しなければならない。

（イ）統括教育情報セキュリティ責任者は、教育情報セキュリティ管理者からインシデントの報告を受けた後、最高情報セキュリティ責任者へ報告しなければならない。

（ウ）統括教育情報セキュリティ責任者は、教育情報セキュリティ管理者からインシデントの報告を受けた後、情報化推進委員会を開催し、報告を行わなければならない。

② 調査等

（ア）情報化推進委員会は、インシデントが発生した場合、ポリシーの遵守等に問題がなかったか調査を行う。

（イ）統括教育情報セキュリティ責任者は、情報化推進委員会の調査結果に基づき、対応を行う。

・原因が、当該事象が発生した部署（学校）にある場合
当該教育情報セキュリティ管理者に対して、ポリシーの遵守を徹底させる。

・原因が、対策基準及び実施手順の不備にある場合
最高情報セキュリティ責任者に対して、対策基準及び実施手順の見直しを進言する。

５．見直し

最高情報セキュリティ責任者は、対策基準及び実施手順に課題及び問題点が認められる場合又は統括教育情報セキュリティ責任者からポリシー見直しの進言があった場合は、見直しを行うものとする。

様式１

令和　　年　　月　　日

インシデント報告書

統括教育情報セキュリティ責任者　様

（学校名）
教育情報セキュリティ管理者
校長　○○　○○

情報資産に関する障害及び事故について、次のとおり報告します。

１　障害及び事故の区分	・ コンピュータウイルス感染　　・ パソコンや外部記録媒体の紛失等 ・ 情報システムへの不正アクセス　・ その他（　　）
２　発生日時	年　　月　　日　　時　　分頃
３　事案内容	
４　原因	
５　被害状況	
６　現在行っている対応	
７　その他特記事項	