岩出市教育情報セキュリティポリシー

（令和８年４月版）

岩出市教育委員会

平成３１年４月１日　策定

岩出市教育情報セキュリティ基本方針

１　目的

本基本方針は、本市教育委員会が保有する情報資産の重要性を維持するため、本市教育委員会が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。なお、本基本方針は、岩出市情報セキュリティポリシー（令和８年３月１日策定）に準拠するものとする。

２　定義

本基本方針及び岩出市教育情報セキュリティ対策基準において次に掲げる用語の意義は、当該各号に定めるところによる。また、その他の用語については、岩出市情報セキュリティポリシーにおいて使用する用語の例によるものとする。

（１）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及びその構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

コンピュータ、ネットワーク及び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

情報資産の重要性及び可用性を維持することをいう。

（４）情報セキュリティポリシー

本基本方針及び岩出市教育情報セキュリティ対策基準をいう。

（５）機密性

情報にアクセスすることを認められた者のみが、情報にアクセスできる状態を確保することをいう。

（６）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。

（７）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。

（８）クラウドサービス

クラウドコンピューティングを利用したサービスをいう。クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能にするモデルであり、最小限の利用手続またはクラウド事業者とのやりとりで速やかに割当てられ提供されるものである。

（９）重要性

情報資産の漏えい、滅失、毀損又は利用不能等の事態が発生した際に、児童生徒等の生命・財産、プライバシー、及び学習活動や校務運営に及ぼす支障の大きさに応じた区分をいう。

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）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、プログラム上の欠陥、操作ミス、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　適用範囲

（１）対象機関の範囲

情報セキュリティポリシーが適用される機関等は、教育委員会、教育部内の各組織及び市立小中学校（以下「教育委員会」という。）とする。

ただし、市長部局が管理するネットワーク等については、岩出市情報セキュリティポリシーを適用するものとする。

（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

5　職員等の遵守義務

職員（非常勤職員及び会計年度任用職員等を含む全ての職員）及び外部受託者（教育委員会の業務に従事する派遣会社社員、協力会社社員及び業務受託会社社員等）（以下「職員等」という。）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

教育委員会の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２）情報資産の分類と管理

教育委員会の保有する情報資産を重要性に応じて分類し、該当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、情報システム室等、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な対策を講じる。

（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の確保等、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、緊急時対応計画を策定する。

7　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ポリシー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を定める情報セキュリティ対策基準を策定する。

なお、情報セキュリティ対策基準は、公にすることにより教育委員会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。

１０　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教育委員会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。

１１　違反に対する対応

情報セキュリティポリシーに違反した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、地方公務員法の規定による懲戒処分の対象とする。

岩出市教育情報セキュリティ対策基準

第１　趣旨

この基準は、岩出市教育情報セキュリティ基本方針（以下「基本方針」という。）　に基づき、岩出市教育委員会（「基本方針」４（１）の適用範囲をいう。以降同じ。）における情報セキュリティ対策等を実施するために共通の基準として具体的な遵守事項及び判断基準を定めたものである。

第２　組織体制

基本方針で定めた情報セキュリティ対策を推進する組織体制については次のとおりとする。

１　最高情報セキュリティ責任者

副市長を、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、教育委員会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　統括教育情報セキュリティ責任者

(1) 教育長を最高情報セキュリティ責任者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、最高情報セキュリティ責任者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、教育委員会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、教育委員会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。

(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及び情報システム担当者に対し、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、教育委員会の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合は、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、教育委員会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・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、最高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、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、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。

(8) 統括教育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、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、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、教育委員会において所有している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、教育委員会において所有している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職員等に対する教育、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)教育部内の各組織においては課長または各組織の長を、学校その他の教育機関においては各施設の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、その所管する各組織または学校その他の教育機関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、その所管する各組織または学校その他の教育機関において、情報資産に対する侵害が発生した場合又は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。
(4) 教育情報セキュリティ管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
(5) 教育情報セキュリティ管理者は、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・管理を行う。

5　情報セキュリティ担当者

(1) 情報セキュリティ担当者は、教育情報セキュリティ管理者の指示等に従い、その所属する課室及び施設等の情報セキュリティに関する対策の向上を図らなければならない。
(2) 情報セキュリティ担当者は、学校においては教頭をもって充てるものとする。

6　教育情報化推進本部

教育委員会の情報セキュリティ対策を統一的に行うため、教育情報化推進本部において、情報セキュリティポリシー等の情報セキュリティに関する重要な事項を決定する。

7　兼務の禁止

(1) 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。
(2) 点検を受ける者とその点検を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

第３　情報資産の分類と管理方法

1　情報資産の分類

学校における情報資産は、重要性に応じて４段階に分類する。なお、教育委員会のその他の組織等においては、岩出市情報セキュリティポリシーに準拠して分類するものとする。

重要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
重要性Ⅰ	生命・財産・プライバシーに甚大な影響を及ぼす情報。原則として外部持ち出し禁止。強固な暗号化が必須。	指導要録原本、人事情報等
重要性Ⅱ	学校運営・教育活動に重大な影響を及ぼす情報。パブリッククラウド利用時は多要素認証（MFA）を含む強固なアクセス制御を適用。	通知表、調査書、健康診断票、ID・パスワード台帳等
重要性Ⅲ	教育活動に影響を及ぼす（不利益を被る）情報。教育情報セキュリティ管理者の包括的承認により持ち出し可。	出席簿、教材、学習記録（ワークシート・作品等）等
重要性Ⅳ	公開を前提とした情報。特段の利用制限なし。	学校要覧、HP 掲載情報等

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第３の１の分類に基づき管理しなければならない。

(2) 情報の作成

ア　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、情報の作成時に第３の１の分類に基づき、当該情報の分類をしなければならない。

ウ　情報を作成する者は、作成途中の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途中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。

(3) 情報資産の入手

ア　組織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扱いをしなければならない。

イ　組織外の者が作成した情報資産を入手した者は、第３の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、入手した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。

(4) 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、情報資産の第３の１分類に応じ、適切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、記録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、当該記録媒体を取り扱わなければならない。

(5) 情報資産の保管

ア　教育情報セキュリティ管理者は、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は、情報資産を記録した外部記録媒体を長期保管する場合は、書込み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は、重要性Ⅱ以上の情報を記録した外部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。

(6) 情報の送信

電子メール等により重要性Ⅲ以上の情報を送信する者は、必要に応じて暗号化又はパスワード設定を行わなければならない。

(7) 情報資産の運搬

ア　重要性Ⅲ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。

イ　重要性Ⅲ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、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。

(8) 情報資産の提供・公表

ア　重要性Ⅲ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。

イ　重要性Ⅲ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

ウ　教育情報セキュリティ管理者は、住民に公開する情報資産について、重要性を確保しなければならない。

(9) 情報資産の廃棄

ア　重要性Ⅲ以上の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。
イ　重要性Ⅲ以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合は、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上で廃棄しなければならない。
ウ　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。

第４　物理的セキュリティ

１　情報システム（サーバ等）の管理

(1) 機器の取付け

教育情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

(2) 機器の電源

ア　教育情報セキュリティ管理者は、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、所管する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るよう努めなければならない。
イ　教育情報セキュリティ管理者は、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、所管するサーバ等の機器を保護するための措置を講じるよう努めなければならない。

(3) 通信ケーブル等の配線

ア　教育情報セキュリティ管理者は、施設管理部門と連携し、所管する通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。
イ　教育情報セキュリティ管理者は、所管する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は、連携して対応しなければならない。
ウ　教育情報セキュリティ管理者は、所管する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、適切に管理するよう努めなければならない。
エ　教育情報セキュリティ管理者は、自ら又は操作を認めた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施さなければならない。

(4) 機器の定期保守及び修理

ア　教育情報セキュリティ管理者は、所管する重要性Ⅱ以上のサーバ等の機器の定期保守を必要に応じて実施しなければならない。
イ　教育情報セキュリティ管理者は、記憶媒体を内蔵する機器を外部の事業者に修理させる場合は、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は、外部の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、秘密保持体制の確認などを行わなければならない。

(5) 敷地外への機器の設置

教育情報セキュリティ管理者は、管理する施設の敷地外にサーバ等の機器を設置する場合は、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。

(6) 機器の廃棄等

教育情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合は、機器内部の記憶装置から、すべ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

(1) 統括教育情報セキュリティ責任者は、施設管理部門と連携し、施設内の通信回線及び通信回線装置を、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。
(3) 統括教育情報セキュリティ責任者は、重要性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は、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、送受信される情報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、伝送途中に情報が破壊、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　職員等のパソコン等の管理
(1) 教育情報セキュリティ管理者は、執務室、職員室及び教室等のパソコン等の端末について、盗難防止の対策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。

第５　人的セキュリティ

１　職員等の遵守事項

(1) 職員等の遵守事項

ア　情報セキュリティポリシー等の遵守

職員等は、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報告し、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

職員等は、業務以外の目的で情報資産を使用してはならない。

ウ　パソコン等の端末の持ち出し及び外部における情報処理作業の制限

(ｱ) 最高情報セキュリティ責任者は、重要性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。

(ｲ) 職員等は、教育委員会のパソコン等の端末、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。

(ｳ) 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。

エ　パソコン等の端末等の持込

職員等は､私物のパソコンを施設内に持ち込んではならない。

オ　職員等は、支給以外のパソコン及び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、安全管理措置を遵守しなければならない。

カ　持ち出しの記録

教育情報セキュリティ管理者は、情報資産等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。

キ　パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、情報システムに関するセキュリティ機能の設定を統括教育情報セキュリティ責任者の許可なく変更してはならない。

ク　机上の端末等の管理

職員等は、離席する際には、パソコン等の端末や記録媒体、情報が印刷された文書等について、教育情報セキュリティ管理者の許可なく情報を閲覧、利用又は盗難されることがないように、適切な措置を講じなければならない。

ケ　退職時等の遵守事項

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。

(2) 非常勤及び会計年度任用職員等への対応

ア　情報セキュリティポリシー等の遵守

教育情報セキュリティ管理者は、非常勤及び会計年度任用職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び会計年度任用職員等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

教育情報セキュリティ管理者は、非常勤及び会計年度任用職員等にパソコン等の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及び電子メールの使用等が不要である場合は、これを利用できないようにしなければならない。

(3) 外部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・保守等を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含め、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。

(4) 児童生徒への指導

学習用端末を使用する児童生徒に対して、端末の扱い方、ID・パスワードの秘匿管理、SNS 利用のルール、情報モラルについて児童生徒の発達段階に応じて指導しなければならない。

(5) 生成 AI の利用

教育情報セキュリティ管理者が指定した、入力データが学習に利用されない設定（オプトアウトや API 利用等）が施されたツールに限り、本方針および別途定める『生成 AI 利活用推進方針』に従って利用できる。生成 AI の出力結果をそのまま利用したことにより発生した情報漏えい、権利侵害等の事故については、当該利用者の責任とする。詳細については、別途定める『岩出市立学校における生成 AI 利活用推進方針』に従うものとする。

2　研修・訓練

(1) 情報セキュリティに関する研修・訓練

最高情報セキュリティ責任者は、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。

(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、管理職を含め、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立案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、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、情報システム担当者及びその他職員等に対し、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、教育情報化推進本部に対し、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) 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実施しなければならない。また、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、効果的に実施できるようにしなければならない。

(4) 研修・訓練への参加

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　事故、欠陥等の報告及び対処

(1) 事故、欠陥等の報告及び対処

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又は住民等外部から報告を受けた場合は、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。

イ　教育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、緊急時対応計画に従い、適切に対処しなければならない。

(2) 事故、欠陥等の分析及び記録の保存

統括教育情報セキュリティ責任者は、事故、欠陥等を分析し、再発防止のための情報資産として体系的に記録し、活用できるよう記録を保存しなければならない。

4　ＩＤ及びパスワード等の管理

(1) ＩＣカード等の取扱い

教育情報セキュリティ管理者及び職員等は、ＩＣカード等について関係実施手順に基づき適正に取り扱わなければならない。

(2) ＩＤの取り扱い

職員等は、自己が管理又は利用しているＩＤを他人に利用させてはならない。また、共有ＩＤを管理又は利用する場合は、共有ＩＤの利用者以外に利用させてはならない。

(3) パスワードの取り扱い

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。

ア　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。

イ　パスワードを記載したメモを作成してはならない。

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、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。

オ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

カ　仮のパスワードは、最初のログイン時点で変更しなければならない。

キ　パソコン等の端末のパスワード記憶機能を利用してはならない。

ク　職員等間でパスワードを共有してはならない。

第６　技術的セキュリティ

1　情報システム及びネットワークの管理

(1) 情報システムの設定等

ア　教育情報セキュリティ管理者は、情報システムを設置する場合は、許可していない職員等が情報資産を閲覧及び使用できないように、アクセス制御の設定をしなければならない。

イ　教育情報セキュリティ管理者は、特定の職員のみ取り扱う情報資産がある場合は、別領域を作成しアクセス制御の措置を講じ、同一組織等であっても、担当職員以外の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。

(2) バックアップの実施

教育情報セキュリティ管理者は、必要に応じて情報資産の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

教育情報セキュリティ管理者は、他の団体と情報システム及び情報資産を交換する場合は、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の許可を得なければならない。

(4) 情報システム管理記録及び作業の確認

ア　教育情報セキュリティ管理者は、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　教育情報セキュリティ管理者は、所管する情報システムにおいて、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、窃取、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。

ウ　教育情報セキュリティ管理者は所管する情報システムにおいて、システム変更等の作業を行う場合は、必要に応じて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

教育情報セキュリティ管理者は、所管する情報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、紛失等がないよう、適切に管理しなければならない。

(6) アクセス記録の取得等

ア　教育情報セキュリティ管理者は、所管する情報システムの各種アクセス記録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　教育情報セキュリティ管理者は、所管する情報システムのアクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。

(7) ネットワークの接続制御、経路制御等

ア　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、ネットワークを設定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、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。

(8) 外部の者が利用できるシステムの分離等

教育情報セキュリティ管理者は、所管する情報システムにおいて、外部の者が利用できるシステムについて、必要に応じて他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(9) 外部ネットワークとの接続制限等

ア　教育情報セキュリティ管理者は、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の許可を得なければならない。

イ　教育情報セキュリティ管理者は、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、庁内及び学校等のすべてのネットワーク、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。

ウ　教育情報セキュリティ管理者は、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、必要に応じて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　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は、ウェブサーバ等の情報システムをインターネットに公開する場合は、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うえで接続しなければならない。

オ　教育情報セキュリティ管理者は、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。

(10) ネットワークの分離

ア　教育情報セキュリティ管理者は、校務系システム及び学習系システム間の通信経路の物理的又は理論的な分離をするとともに、校務系システム及び校務外部接続系システム間の通信経路を物理的又は理論的に分離し、それぞれ適切な安全管理措置を講じるよう努めなければならない。

イ　教育情報セキュリティ管理者は、校務系システムと校務外部接続系システム及び学習系システム間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図るよう努めなければならない。

(11) 無線ＬＡＮ及びネットワークの盗聴対策

統括教育情報セキュリティ責任者は、無線ＬＡＮを利用する場合は、解読が困難な暗号化及び認証技術の使用を義務付けしなければならない。

(12)電子メールのセキュリティ管理

ア　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。

イ　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。

ウ　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。

エ　統括教育情報セキュリティ責任者は、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職員等に周知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、情報システムの開発や運用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、委託先との間で利用方法を取り決めなければならない。

(13)電子メールの利用制限

ア　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。

イ　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。

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

エ　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。

オ　職員等は、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サービス等を使用してはならない。

(14)電子署名・暗号化

ア　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重要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。

イ　職員等は、暗号化を行う場合は、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。

(15)無許可ソフトウェアの導入等の禁止

ア　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。

イ　職員等は、業務上の必要がある場合は、当該情報システムを所管する統括教育情報セキュリティ責任者の許可を得て、ソフトウェアを導入することができる。

ウ　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。

(16)機器構成の変更の制限

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。ただし、業務上の必要がある場合には、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。

(17)無許可でのネットワーク接続の禁止

職員等は、統括教育情報セキュリティ責任者の許可なく情報システムをネットワークに接続してはならない。

(18)業務以外の目的でのウェブの閲覧の禁止

ア　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。

イ　統括教育情報セキュリティ責任者は、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。

２　アクセス制御

(1) アクセス制御

ア　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セキュリティ管理者は、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

(ｱ) 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は、所管する情報システムに係る利用者の登録、変更、抹消等の情報管理、職員等の異動、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。

(ｲ) 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、当該情報システムを所管する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。

(ｳ) 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は、所管する情報システムについて利用されていないＩＤ等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

(ｱ) 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は、所管する情報システムに係る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)管理者権限等の特権を付与されたＩＤ等を利用する者は、教育情報セキュリティ管理者が指名し、統括教育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)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は、管理者権限等の特権を付与されたＩＤ等の変更について、外部委託事業者に行わせてはならない。

(2) 職員等による外部からのアクセス等の制限

ア　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、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所管する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。

イ　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。

ウ　統括教育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は、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　統括教育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は、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　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は、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合は、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　職員等は、外部から持ち帰ったパソコン等の端末を内部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。

(3) パスワードに関する情報の管理

統括教育情報セキュリティ責任者又は情報システムを所管する教育情報セキュリティ管理者は、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。

(4) 特権による接続時間の制限

教育情報セキュリティ管理者は、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　情報システムの開発、導入、保守等

(1) 情報システムの調達

ア　統括教育情報セキュリティ責任者及び情報システムを所管する教育情報セキュリティ管理者は、情報システムの開発、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　統括教育情報セキュリティ責任者及び情報システムを所管する教育情報セキュリティ管理者は、情報システム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

ア　情報システムの開発における責任者及び作業者の特定

情報システムを所管する教育情報セキュリティ管理者は、情報システムの開発の責任者及び作業者を特定しなければならない。

イ　情報システム開発における責任者、作業者のＩＤの管理

(ｱ) 情報システムを所管する教育情報セキュリティ管理者は、情報システムの開発の責任者及び作業者が使用するＩＤを管理し、開発完了後に開発用ＩＤを削除しなければならない。

(ｲ) 情報システムを所管する教育情報セキュリティ管理者は、情報システムの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　情報システムの開発に用いるハードウエア及びソフトウェアの管理

(ｱ) 情報システムを所管する教育情報セキュリティ管理者は、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ェアを特定しなければならない。

(ｲ) 情報システムを所管する教育情報セキュリティ管理者は、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は、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

ア　開発環境と運用環境の分離及び移行手順の明確化

(ｱ) 情報システムを所管する教育情報セキュリティ管理者は、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。

(ｲ) 情報システムを所管する教育情報セキュリティ管理者は、移行の際に、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。

イ　テスト

(ｱ) 情報システムを所管する教育情報セキュリティ管理者は、新たに情報システムを導入する場合は、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) 情報システムを所管する教育情報セキュリティ管理者は、運用テストを行う場合は、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) 情報システムを所管する教育情報セキュリティ管理者は、個人情報及び重要性の高いデータを、テストデータに使用してはならない。

(4) 情報システムの開発・保守に関連する資料等の保管

ア　情報システムを所管する教育情報セキュリティ管理者は、システム開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

イ　情報システムを所管する教育情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

(5) 情報システムにおける入出力データの正確性の確保

ア　情報システムを所管する教育情報セキュリティ管理者は、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　情報システムを所管する教育情報セキュリティ管理者は、故意又は過失により情報が改ざん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　情報システムを所管する教育情報セキュリティ管理者は、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

情報システムを所管する教育情報セキュリティ管理者は、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

情報システムを所管する教育情報セキュリティ管理者は、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は、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。

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。

ア　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、不正プログラムの情報システムへの侵入を防止しなければならない。

イ　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。

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、必要に応じ職員等に対して注意喚起しなければならない。

エ　所管する情報システムに、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。

オ　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。

カ　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。

(2) 教育情報セキュリティ管理者の措置事項

情報システムを所管する教育情報セキュリティ管理者は、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　所管する情報システムに、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システムに常駐させなければならない。

イ　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。

ウ　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。

エ　インターネットに接続していない情報システムにおいて、記録媒体を使う場合は、コンピュータウイルス等の感染を防止するために、教育情報セキュリティ管理者が認めた媒体以外を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又は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) 職員等の遵守事項

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。

ア　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。

イ　外部から情報資産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。

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は、速やかに削除しなければならない。

エ　不正プログラム対策ソフトウェアによる端末のチェックを定期的に実施しなければならない。

オ　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によるチェックを行わなければならない。

カ　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。

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は、ＬＡＮケーブルの即時取り外し又は機器の電源遮断を行わなければならない。

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、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しなければならない。

イ　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教育情報セキュリティ管理者へ通報するよう、設定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、情報システムに攻撃を受けることが明確になった場合は、情報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、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、情報システムに攻撃を受け、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セキュリティ管理者は、職員等及び外部委託事業が使用しているパソコン等の端末からの施設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) 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は、職員等による不正アクセスを発見した場合は、当該職員等が所属する組織または学校その他の教育機関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　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

統括教育情報セキュリティ責任者及び情報システムを所管する教育情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じて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、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) 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、必要に応じて対応方法について、職員等に周知しなければならない。

第7　運用

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セキュリティ管理者は、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セキュリティ管理者は、重要なアクセス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。

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

ア　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、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。

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　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は、情報システムの設定等における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、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) 職員等の報告義務

ア　職員等は、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は、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。

イ　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。

3　侵害時の対応等

(1) 緊急時対応計画の策定

教育情報化推進本部は、情報セキュリティに関する事故、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、あらかじめ緊急時対応計画を定め、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、次の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

(3) 事業継続計画との整合性確保

教育情報化推進本部は、自然災害等に備えた事業継続計画を策定する場合には、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

教育情報化推進本部は、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を考慮し、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

(1) 例外措置の許可

教育情報セキュリティ管理者は、情報セキュリティポリシーを遵守することが困難な状況で、学校事務及び教育活動等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は、学校事務及び教育活動等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。

(3) 例外措置の申請書の管理

最高情報セキュリティ責任者は、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。

5　法令等遵守

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１２月１３日法律第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5月３０日法律第５７号）
(6) 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）
(7) 岩出市個人情報の保護に関する法律施行条例（令和４年１２月２２日条例第１８号）

6　懲戒処分等

(1) 懲戒処分

情報セキュリティポリシーに違反した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) 違反に対する対応

職員等の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。

ア　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職員等が所属する組織または学校その他の教育機関の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。

イ　情報セキュリティ担当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。

ウ　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は、統括教育情報セキュリティ責任者は当該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又は剥奪することができる。その後、統括教育情報セキュリティ責任者は、職員等の権利を停止又は剥奪した旨を最高情報セキュリティ責任者及び当該職員等が所属する組織または学校その他の教育機関の教育情報セキュリティ管理者に速やかに通知しなければならない。

第８　外部委託

(1) 外部委託先の選定基準

教育情報セキュリティ責任者は、外部委託先の選定に当たり、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。

(2) 契約項目

情報システムの運用等を外部委託する場合には、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。

ア　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
イ　委託先の責任者、委託内容、作業者、作業場所の特定
ウ　提供されるサービスレベルの保証
エ　従業員に対する教育の実施
オ　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
カ　業務上知り得た情報の守秘義務
キ　再委託に関する制限事項の遵守
ク　委託業務終了時の情報資産の返還、廃棄等
ケ　委託業務の定期報告及び緊急時報告義務
コ　市による監査及び検査

サ　市による事故時等の公表
シ　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、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、必要に応じて契約に基づき措置しなければならない。

第９　クラウドサービスの利用

１　クラウドサービスの利用における情報セキュリティ対策

(1) 利用者認証

ア　教育委員会は、クラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意サービス提供定款や契約書面上で確認または合意しなければならない。

イ　教育委員会は、当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

ウ　教育委員会側の管理者権限を有する者の ID の管理について、第６の２（１）ウを遵守しなければならない。

(2) アクセス制御

ア　教育委員会は、当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　教育委員会は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可された職員のみがアクセスできる環境を設定しなければならない。

(3) クラウドに保管するデータの暗号化

教育委員会は、当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じられていることを、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。

(4) マルチテナント環境におけるテナント間の安全な管理

教育委員会は、複数のクラウド利用者がクラウドリソースを共用する環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策が講じられていることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(5) クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策

ア　教育委員会は、当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知することを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　教育委員会は、当該クラウドサービスを提供する情報システムのインターネット接続境界において、教育委員会以外による不正な通信侵入を防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講ずることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(6) 情報の通信経路のセキュリティ確保

ア　教育委員会は、教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）をクラウド事業者に求め、合意のうえ、利用しなければならない。

イ　教育委員会は、クラウド事業者が保守運用等を遠隔で行う場合の、保守運用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するため必要な措置（情報交換の実施基準･手順等の整

備、通信の暗号化等）をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(7) クラウドサービスを提供する情報システムの物理的セキュリティ対策

教育委員会は、当該クラウドサービスのサーバ等の管理条件について、第４の１に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(8) クラウドサービスを提供する情報システムの運用管理

ア　教育委員会は、当該クラウドサービスにおけるデータバックアップについて、第６の１（２）に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　教育委員会は、当該クラウドサービスにおける情報セキュリティの確保や点検に必要なアクセス記録等について、第６の１（６）に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(9) クラウドサービスを提供する情報システムのマルウェア対策

ア　教育委員会は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　教育委員会は、内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(10) 教育委員会側のセキュリティ確保

ア　教育委員会は、クラウドサービスにアクセスする利用者側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じなければならない。

イ　教育委員会は、標的型攻撃による外部からの脅威の侵入を防止するために、職員への教育や入口対策を講じなければならない。

(11) クラウド事業者従業員の人的セキュリティ対策

ア　教育委員会は、クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　教育委員会は、クラウドサービスに関わるクラウド事業者従業員に対して、業務に用いる ID 及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

ウ　教育委員会は、クラウドサービスに関わらない従業員等が教育委員会のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

エ　教育委員会は、教育委員会のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、教育委員会の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(12) データの廃棄等について

ア　教育委員会は、サービス利用終了時等において、教育委員会のデータが不用意に残置されないよう、適切に破棄するための流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。

イ　教育委員会は、サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。

２　パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

(1) 守秘義務、目的外利用及び第三者への提供の禁止

教育委員会は、クラウド事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなければならない。クラウドサービス事業者がコンテンツにアクセスできるかどうかを確認し、サービスに係る情報及び受託した情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項について、サービス提供に係る契約に含めなければならない。契約には、当該条項に違反したクラウドサービス事業者に対する損害賠償規定を含める。

(2) 準拠する法令、情報セキュリティポリシー等の確認

教育委員会は、クラウド事業者がどのような規範に基づいてサービス提供するか開示を求め、教育委員会の準拠する法令、情報セキュリティポリシー等を確認し、それらとの整合を確認しなければならない。

(3) クラウド事業者の管理体制

ア　教育委員会は、クラウド事業者に対して、情報セキュリティポリシー等の遵守を担保する管理体制が整備されているか、クラウド事業者の組織体制に関する以下の項目を確認し、合意しなければならない。

(ｱ) サービスの提供についての管理責任を有する責任者の設置

(ｲ) 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理 者）の設置

(ｳ) サービスの提供に係る情報システムの運用に関する事務を統括する責任者の設置

(4) クラウド事業者従業員への教育

ア　教育委員会は、クラウド事業者に、従業員に対して個人情報保護等の関係法令、守秘義務等、業務遂行に必要な知識、意識向上のための適切な教育及び訓練を実施し、充分な知識とセキュリティ意識を醸成することを求めなければならない。

イ　教育委員会は、クラウド事業者に、従業員への上記育成計画、教育実績等の情報を提示させ、自らデータを管理する場合と同様の教育・訓練を実施しているかを確認しなければならない。

(5) 情報セキュリティに関する役割の範囲、責任分界点

ア　教育委員会は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点について開示するよう求めなければならない。

イ　教育委員会は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点が教育委員会側で講ずる情報セキュリティ対策の役割の範囲と整合することを確認し、合意しなければならない。

(6) 監査

ア　教育委員会は、クラウドサービスの監査状況、範囲・条件、内容等についてクラウド事業者に開示するよう求めなければならない。

イ　教育委員会は、クラウド事業者によるクラウドサービスに関する監査レポート等を根拠にして、自らの関係法令、情報セキュリティポリシーと照らし合わせ、安全性が確保されているかについて確認しなければならない 。

(7) 情報インシデント管理及び対応フローの合意

ア　教育委員会は、情報セキュリティインシデント管理に関する責任範囲及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めなければならない。

イ　教育委員会は情報セキュリティインシデント管理に関する責任範囲及びインシデント対応フローを検証しなければならない。

(8) クラウドサービスの提供水準及び品質保証

教育委員会は、クラウドサービスの提供水準（サービス 内容、提供範囲等）と品質保証（サービス稼働率、故障等の復旧時間等）を確認するとともに、それらの水準・品質が、業務遂行に求められる要求水準を満たすことを確認し、合意しなければならない。

(9) クラウド事業者の再委託先等との合意事項

ア　教育委員会は、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策について、クラウド事業者自らが実施する内容と、再委託先等に委託する内容も含め

て提示することをクラウド事業者に求めなければならない。また、サプライチェーンリスク対策が適切に講じられていることをクラウド事業者に求めなければならない。

イ　教育委員会は、アの提示内容が、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策と整合していることを確認しなければならない。

(10) その他留意事項

ア　教育委員会は、クラウド事業者がサービスを安定して提供可能な企業・団体であるかについて考慮しなければならない。

イ　教育委員会は、クラウド事業者間でのデータ形成の互換性が必ずしも保証されている訳ではないことから、事業者を変更する際のデータ移行の方法などについて、クラウド事業 者にサービス提供定款や契約書面上で確認または合意しなければならない。

ウ　教育委員会は、クラウド事業者に対して、クラウドサービスにおいて扱う情報資産や情報システム等について、日本の法令が適用されること及び係争等における管轄裁判所が日本国内であることを確認すること。

3　約款による外部サービスの利用

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。

4　ソーシャルメディアサービスの利用

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

(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適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　重要性Ⅱ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。

第１０　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っては、事業者における個人情報の適切な管理が行われていることが必須であることから、教育委員会は、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、以下の項目を参考として、事業者に確認を行うものとする。

1　個人情報の利用範囲

教育・学校の目的に必要な情報、または児童生徒・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、無断提供をしないこと。

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

教育・学校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・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禁止

教育・学校の目的を達成するため、または児童生徒・保護者によって許可された場合を除き、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定義

サービス提供期間（利用者と合意した期間）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、および保持するのは、教育機関、教師、また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、契約また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、管理するものとすること。

12　合併/買収

合併または他社による買収を伴う場合、後継企業が以前に収集し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。

第１１　評価・見直し

１　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セキュリティ管理者は、所管するネットワーク及び情報システムについて、定期的又は必要に応じ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、所管する部局における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、毎年度又は必要に応じた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、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、教育情報化推進本部に報告しなければならない。

(3) 自己点検結果の活用

ア　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　教育情報化推進本部は、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。

２　情報セキュリティポリシー及び関係規程等の見直し

教育情報化推進本部は、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踏まえ、必要があると認めた場合は、情報セキュリティポリシー及び関係規程等の見直しを行うものとする。