令和７年２月１日

○周南市立学校情報セキュリティ対策基準

周南市立学校情報セキュリティ対策基準（平成２８年１月１日制定）の一部を改正する。

周南市立学校情報セキュリティ対策基準

目次

第１章　はじめに

１ 目的

この対策基準は、周南市立学校情報セキュリティ基本方針に係る要領（令和６年２月１日制定。以下「基本方針」という。）第６条の規定に基づき、本市の学校教育に係る情報資産の適切な保護、管理、運用等に関し必要な事項を定めたものである。

２ 定義

この対策基準における定義は、基本方針第２条に規定するところによる。

３ 適用範囲

この対策基準が適用される範囲は、基本方針第４条に規定するところによる。

第２章　組織体制

１ 最高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（ＣＩＳＯ: Chief Information Security Officer、以下「ＣＩＳＯ」という。）とする。ＣＩＳＯは、本市における全ての学校ネットワーク、学校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) ＣＩＳＯ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 学校情報セキュリティ統括責任者

(1) 教育部長を、ＣＩＳＯ直属の学校情報セキュリティ統括責任者とする。学校情報セキュリティ統括責任者はＣＩＳＯを補佐しなければならない。

(2) 学校情報セキュリティ統括責任者は、本市の全ての学校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) 学校情報セキュリティ統括責任者は、本市の全ての学校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) 学校情報セキュリティ統括責任者は、学校情報セキュリティ責任者、学校情報セキュリティ管理者、学校情報システム管理者及び学校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) 学校情報セキュリティ統括責任者は、本市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) 学校情報セキュリティ統括責任者は、本市の共通的な学校ネットワーク、学校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) 学校情報セキュリティ統括責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、学校情報セキュリティ統括責任者、学校情報セキュリティ責任者、学校情報セキュリティ管理者、学校情報システム管理者、学校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) 学校情報セキュリティ統括責任者は、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 学校情報セキュリティ責任者

(1) 学校教育課長を学校情報セキュリティ責任者とする。

(2) 学校情報セキュリティ責任者は、本市の学校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) 学校情報セキュリティ責任者は、本市において所有している学校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) 学校情報セキュリティ責任者は、本市において所有している学校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、学校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に対する教育、訓練、助言及び指示を行う。

4 学校情報セキュリティ管理者

(1) 学校長及び所属長(周南市教育支援センター所長、周南市教育研究センター所長、学校教育課長)を、学校情報セキュリティ管理者とする。

(2) 学校情報セキュリティ管理者は当該学校等の情報セキュリティ対策に関する権限及び責任を有する。

(3) 学校情報セキュリティ管理者は、当該学校等において、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、学校情報セキュリティ責任者、学校情報セキュリティ統括責任者及び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 学校情報システム管理者

(1) 本市教育委員会が所管する学校情報システムの担当室課長及び個別の学校情報システムを保有する学校の学校長を、学校情報システムに関する学校情報システム管理者とする。

(2) 学校情報システム管理者は、所管する学校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) 学校情報システム管理者は、所管する学校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) 学校情報システム管理者は、所管する学校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 学校情報システム担当者

学校情報システム管理者は、所管する学校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学校情報システム担当者を適宜選任する。

7 学校情報セキュリティ委員会

(1) 本市の学校情報セキュリティ対策を統一的に行うため、以下の委員で構成される学校情報セキュリティ委員会を設置する。

ア ＣＩＳＯ
イ 学校情報セキュリティ統括責任者
ウ 学校情報セキュリティ責任者
エ 学校情報セキュリティ管理者のうち小学校校長会長及び中学校校長会がそれぞれ選任した者
オ 周南市情報セキュリティ担当部長
カ 必要に応じＣＩＳＯが別途選任した者

(2) 学校情報セキュリティ委員会は、学校情報セキュリティポリシーの周知及び遵守状況の確認評価・見直し等、情報セキュリティに関する重要な事項を決定する。

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

9 情報セキュリティに関する統一的な窓口の設置

(1) ＣＩＳＯは、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

(2) ＣＩＳＯよる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

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

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

１０ 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、所属する学校の学校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。

１１ 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、所属する組織の学校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。

第３章　情報資産の分類と管理方法

１ 情報資産の分類

本市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。

(1) 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概要
機密性３	学校等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	特定の教職員等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	学校等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	教職員等のみが知り得る状態を確保する必要がある情報資産（教職員等のうち特定の教職員等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	学校等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	教職員等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（教職員等及び児童生徒のうち特定の教職員等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（教職員等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）

(2) 完全性による情報資産の分類

分類	分類基準	該当する情報資産の概要
完全性２Ｂ	学校等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	学校等で取り扱う情報資産のうち、改ざん、誤びゅう又は破損に	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

	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	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

(3) 可用性による情報資産の分類

分類	分類基準	該当する情報資産の概要
可用性２Ｂ	学校等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	学校等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

２ 情報資産の管理

(1) 管理責任

ア 学校情報セキュリティ統括責任者は、学校情報システムとその運用管理を定めた学校情報セキュリティ対策基準を策定しなければならない。

イ 学校情報セキュリティ管理者は、自校の所管する情報資産について管理責任を有する。

ウ 学校情報セキュリティ管理者は、自校で所管する情報資産を確認し、情報資産台帳（以下「台帳」という。）を整備しなければならない。

エ 学校情報セキュリティ管理者は、教職員等の情報資産の取扱いに際し、台帳及び実施手順に基づいた運用管理を指導しなければならない。

オ 教職員等は、台帳及び実施手順に基づき、適切に情報資産を取り扱わなければならない。

(2) 情報資産の取扱い

ア 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。（情報資産の分類の表示先：ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等）

イ 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、情報の作成時に当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

(ｳ) 情報を作成する教職員等は、作成途上の情報についても、取扱いを許可されていないものの閲覧や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。

ウ 情報資産の入手

(ｱ) 本市教職員等が作成した情報資産を入手した教職員等は、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) 本市教職員等以外の者が作成した情報資産を入手した教職員等は、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

(ｳ) 情報資産を入手した教職員等は、その情報資産の分類が不明な場合、学校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。

エ 情報資産の利用

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

(3) 情報資産の保管

ア 学校情報セキュリティ管理者及び学校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 学校情報セキュリティ管理者又は学校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しなければならな

い。

ウ 教職員等は、学校情報セキュリティ管理者が指定した保管先にのみ情報資産を保管しなければならない。

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

(4) 情報資産の外部持ち出し

ア 分類に応じた情報資産の外部持ち出し制限

(ｱ) 教職員等は、機密性２Ｂ以上の情報資産を外部持ち出しする場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者の個別許可を得なければならない。また、持ち出し持ち帰りの記録をつけなければならない。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

(ｲ) 機密性２Ａ及び機密性１の情報資産については、教職員等の外部持ち出しについて、教育情報セキュリティ管理者の判断で包括的許可を可とする。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合は必要に応じ用いなければならない。

イ 電子メール、外部ストレージサービスによる情報の送信

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、外部ストレージサービスにより機密性２Ａ以上の情報を外部送信する教職員等は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。

(ｲ) 利用する電子メール、外部ストレージサービスは、学校情報セキュリティ統括責任者が許可するサービスのみを利用し、私的に契約したサービスを利用してはならない。

ウ 外部電磁的記録媒体を用いた情報の外部持ち出し

USBメモリ等の物理的な媒体による情報の外部持ち出しでは、教育委員会又は学校から支給された公的な媒体のみ利用すること。

エ FAXによる情報の送信

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

オ 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の安全対策を講じ、宛名・差出名を明記して、厳重に封印しなければならない。

(ｲ) 機密性２Ａ以上の情報資産を運搬する教職員等は、学校情報セキュリティ管理

者に許可を得なければならない。

カ 情報資産の公表

(ｱ) 学校情報セキュリティ管理者は、公開する情報が正しい内容であることを事前に確認し、誤公開を防がなければならない。

(ｲ) 学校情報セキュリティ管理者は、公開する情報資産について、改ざんや消去されないように定期的に確認しなければならない。

(5) 情報資産の廃棄

ア 情報資産を廃棄する教職員は、機密性２Ａ以上の情報資産が記載された紙媒体の書類を廃棄する場合には、内容を復元できないように細断、熔解またはこれに準ずる方法にて廃棄しなければならない。

イ 情報を記録している電磁的記憶媒体を利用しなくなった場合、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 機密性２Ａ以上の情報資産の廃棄・リース返却を行う教職員等は、学校情報セキュリティ管理者の許可を得て、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。

エ 機密性２Ａ以上の情報資産の廃棄を外部委託事業者に委託する場合、廃棄する情報資産を業者が引き取る際、教職員等が立ち会わなければならない。

第４章　物理的セキュリティ

１ サーバ等の管理

(1) サーバ等の管理

ア 学校情報システム管理者は、サーバ等の機器の管理に関する実施体制と管理責任を明確にしなければならない。

イ 学校情報システム管理者は、サーバ等の機器の所在を確認し、管理外の機器が設置されていないことを確認しなければならない。

(2) 機器の取付け

ア 学校情報システム管理者は、サーバ等の機器の設置は職務上必要なものに限定し、その使用目的を明確にしなければならない。

イ 学校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、必要な措置を講じなければならない。

(3) 機器の電源

ア 学校情報システム管理者は、学校情報セキュリティ統括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。

イ 学校情報システム管理者は、学校情報セキュリティ統括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

ア 学校情報セキュリティ統括責任者及び学校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な措置を講じなければならない。

イ 学校情報セキュリティ統括責任者及び学校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。

ウ 学校情報セキュリティ統括責任者及び学校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。

エ 学校情報セキュリティ統括責任者、学校情報システム管理者は、自ら又は学校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

ア 学校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保守を実施しなければならない。

イ 学校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、学校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

学校情報セキュリティ統括責任者及び学校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

学校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。

２ 管理区域（情報システム室等）の管理

(1) 管理区域の構造等

ア 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。

イ 学校情報セキュリティ統括責任者及び学校情報システム管理者は、管理区域を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。

ウ 学校情報セキュリティ統括責任者及び学校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。

エ 学校情報セキュリティ統括責任者及び学校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、防水措置等を講じなければならない。

オ 学校情報セキュリティ統括責任者及び学校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

ア 学校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し、ICカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなけ

ればならない。

イ 管理区域に入室を許可する場合、入退室を許可された者に身分証明書等を携帯させ、必要に応じ、その提示を求めなければならない。

ウ 学校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者が付き添うものとし、外見上区別できる措置を講じなければならない。

エ 学校情報システム管理者は、機密性２Ｂ以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

(3) 機器等の搬入出

ア 学校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。

イ 学校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、入退室を許可された者を立ち会わせなければならない。

3 通信回線及び通信回線装置の管理

(1) 学校情報セキュリティ統括責任者は、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) 学校情報セキュリティ統括責任者は、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) 学校情報セキュリティ統括責任者は、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) 学校情報セキュリティ統括責任者は、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) 学校情報セキュリティ統括責任者は、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。

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) 学校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) 学校情報システム管理者は、校務系システム、学校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) 学校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。

(4) 学校情報システム管理者は、端末の学校外での業務利用の際は、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。

(5) 学校情報システム管理者は、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ウェアの導入等の対策を講じなければならない。

(6) 学校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、教職員等の端末に対して不適切なウェブページのＷｅｂフィルタリング等の閲覧を防止する対策を講じなければならない。

第５章　人的セキュリティ

１ 学校情報セキュリティ管理者の措置事項

(1) 情報資産の管理

ア 情報資産の持ち出し及び持ち込みの記録管理

学校情報セキュリティ管理者は、教職員等による情報資産の外部持ち出しについて、記録管理しなければならない。

イ 情報資産の廃棄管理

(ｱ) 学校情報セキュリティ管理者は、廃棄処理を外部に委託する場合は、学校の外に委託業者が持ち出す行為に教職員等が立ち合うように指示し、誤廃棄を予防しなければならない。

(ｲ) 教育情報セキュリティ管理者は、廃棄した情報資産を記録管理しなければならない。

(2) 端末等の持ち出し及び持ち込みの記録

学校情報セキュリティ管理者は、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。

(3) 教職員等への情報セキュリティポリシー等の遵守指導

学校情報セキュリティ管理者は、教職員等に対し、学校情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

(4) 新規ソフトウェア及びコンテンツの導入・利用判断

学校情報セキュリティ管理者は、教職員等から、導入したソフトウェア・コンテンツの制限解除や、業務上新たなソフトウェア・コンテンツの導入について、事前に相談があった場合は、学校情報システム管理者に上申して、判断を仰がなければならない。

(5) インターネット接続及び電子メール利用の制限

ア 学校情報セキュリティ管理者は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導しなければならない。

イ Ｗｅｂフィルタリングの設定について、教職員等から相談があった場合は、学校情報システム管理者に上申して、判断を仰がなければならない。

(6) 校内での管理

学校情報セキュリティ管理者は、教職員等と協力して下記を管理しなければならない。

ア 来校者の氏名及び入退時刻を記録しなければならない。

イ 来校者には名札などを着用させ、第三者であることが識別できるようにしなければ

ならない。

ウ 地域住民、保護者などに校内施設を開放する場合、職員室等開放していない施設へは入場できないよう制限を設けなければならない。

2 教職員等の遵守事項

教職員等は、教育情報セキュリティ管理者の指導の下、以下の規定を遵守しなければならない。また、教育委員会事務局職員についても、教育ネットワーク及び同ネットワークに帰属する情報資産を取扱う範囲においては、以下の該当する規定を準用するものとする。

(1) 学校情報セキュリティポリシー等の遵守

教職員等は、学校情報セキュリティ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

ア 執務室の施錠管理

職員室等にて教職員等が不在となる場合には、職員室等を施錠しなければならない。

イ 来校者等への対応

来校者等を職員室等に入れる場合には、教育情報セキュリティ管理者または学校情報セキュリティ担当者の許可を求めなければならない。

ウ 机上の書類・端末等の管理

教職員等は、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、離席時の端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

(3) 支給端末の取扱い

ア 教職員等は、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。

(ｱ) セキュリティ機能に関する設定変更

(ｲ) メモリ増設等の改造

エ 教職員等は、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) 支給以外の端末及び電磁的記録媒体等の業務利用

ア 教職員等は、支給以外の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、「支給以外のパソコン等情報機器の使用承認申請書」（別記第２号様式）により学校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。

イ 教職員等は、支給以外の端末及び電磁的記録媒体等を用いる場合には、学校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) 端末や電磁的記録媒体等の持ち出し及び教育委員会及び学校が構築・管理している環境の外部における情報処理作業の制限

ア 教職員等は、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 教職員等は、外部で情報処理業務を行う場合には、学校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。

ア 教職員個人に割り当てられているＩＤは、他人に利用させてはならない。

イ 共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

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学校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。

ア パスワードは、他者に知られないように管理しなければならない。

イ パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ パスワードは十分な長さとし、文字列は他者に容易に推測されな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、学校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 複数の学校情報システムを扱う教職員等は、原則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。）

カ 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。

キ サーバ、ネットワーク機器及び端末において、原則パスワードを記憶させてはならない。

ク 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。）

ケ 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。

コ 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。

(8) 外部電磁的記録媒体の取扱い

ア 利用するUSBメモリ等の外部電磁的記憶媒体は、教育委員会又は学校から支給された公的な媒体のみ利用すること。

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

(9) 電子メールの利用制限

ア 教職員等は、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 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。

ウ 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。

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

オ 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学校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。

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

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

ク 差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合には、添付ファイルの閲覧やリンク先（URL）にアクセスせずに、学校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。

(10) クラウドサービス・ソーシャルメディアサービス利用制限

ア 機密性２Ｂ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。

イ 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。

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

(11) 不正プログラム対策に関する教職員等の遵守事項

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。

ア 端末に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及び不正プログラム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。

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

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でチェックを行わなければならない。

カ 学校情報セキュリティ責任者が提供するセキュリティ対策に関する情報を、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又は感染が疑われる場合は、すみやかに学校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。

(12) 電子署名・暗号化

ア 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、学校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等、セキュリティを考慮して、送信しなければならない。

イ 教職員等は、暗号化を行う場合に学校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、学校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。

ウ 学校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。

(13) 無許可ソフトウェアの導入等の禁止

ア 教職員等は、端末に無断でソフトウェアを導入してはならない。

イ 教職員等は、業務上の必要がある場合は、学校情報セキュリティ責任者及び学校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、学校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。

ウ 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。

(14) 機器構成の変更の制限

ア 教職員等は、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。

イ 教職員等は、業務上、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、学校情報セキュリティ責任者及び学校システム管理者の許可を得なければならない。

(15) 無許可でのネットワーク接続の禁止

教職員等は、学校情報セキュリティ責任者の許可なく情報機器をネットワークに接続してはならない。

(16) 業務以外の目的でのウェブ閲覧の禁止

教職員等は、業務以外の目的でウェブを閲覧してはならない。

(17) 外部からのアクセス等の制限

ア 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、学校情報セキュリティ管理者を介して、学校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学校情報システム管理者の許可を得なければならない。

イ 教職員等は、持ち込んだ又は外部から持ち帰った端末を施設内のネットワークに接続する前に、不正プログラム対策ソフトウェア等を通じて、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。

(18) 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

ア 学習用途の利用限定

学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

イ 利用者認証情報の秘匿管理

ＩＤ及びパスワードは他の人に知られないようにすること。

ウ 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。

エ 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。

オ 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。

カ 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。

キ 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。

ク 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。

ケ 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。

(19) 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。

3 研修・訓練

(1) 情報セキュリティに関する研修・訓練

学校情報セキュリティ統括責任者は、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。

(2) 研修計画の策定及び実施

学校情報セキュリティ統括責任者は、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、ＣＩＳＯの承認を得なければならない。

(3) 緊急時対応訓練

学校情報セキュリティ統括責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、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。

(4) 研修・訓練への参加

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。

4 情報セキュリティインシデントの連絡体制の整備

(1) 学校内からの情報セキュリティインシデントの報告

ア 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 報告を受けた学校情報セキュリティ管理者は、速やかに学校情報セキュリティ統括責任者、学校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に報告しなければならない。

ウ 学校情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてＣＩＳＯ及び学校情報セキュリティ責任者に報告しなければな

らない。

(2) 教職員等の報告義務

ア 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、直ちに学校情報セキュリティ責任者又は学校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学校情報セキュリティ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。

(3) 市民等外部からの情報セキュリティインシデントの報告

ア 教職員等は、管理対象のネットワーク及び学校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、市民等外部から報告を受けた場合、学校情報セキュリティ管理者に報告しなければならない。

イ 報告を受けた学校情報セキュリティ管理者は、速やかに学校情報セキュリティ統括責任者、学校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に報告しなければならない。

ウ 学校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、必要に応じてＣＩＳＯ及び学校情報セキュリティ責任者に報告しなければならない。

(4) 情報セキュリティインシデント原因の究明・記録、再発防止等

ア 学校情報セキュリティ統括責任者は、情報セキュリティインシデントについて、学校情報セキュリティ管理者、学校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、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、ＣＩＳＯに報告しなければならない。

イ ＣＩＳＯは、学校情報セキュリティ統括責任者から、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に必要な措置を指示しなければならない。

第６章　技術的セキュリティ

１ コンピュータ及びネットワークの設定管理

(1) ファイルサーバ及び端末の設定等

ア 学校情報システム管理者は、教職員等が使用できるファイル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。

イ 学校情報システム管理者は、ファイル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。

ウ 学校情報システム管理者は、機密性による情報資産の分類に応じて、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。

(2) バックアップの実施

学校情報セキュリティ統括責任者及び学校情報システム管理者は、ファイルサーバ等に記録された校務系情報及び学習系情報について、サーバの冗長化対策に関わらず、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) ログの取得等

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

イ 学校情報セキュリティ統括責任者及び学校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。

ウ 学校情報セキュリティ統括責任者及び学校情報システム管理者は、取得したログを必要に応じて点検又は分析する機能を設け、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。

(4) ネットワークの接続制御、経路制御等

ア 学校情報セキュリティ統括責任者は、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、所管するネットワークの内部におけるファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

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

(5) 外部の者が利用できるシステムの分離等

学校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 機密性２Ｂ以上を扱うシステムとの論理的又は物理的な分離、若しくは各システムにおけるアクセス権管理の徹底を行うこと。

(6) 外部ネットワークとの接続制限等

ア 学校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及び学校情報セキュリティ統括責任者の許可を得なければならない。

イ 学校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、学校等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。

ウ 学校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。

エ 学校情報セキュリティ統括責任者及び学校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、学校ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

オ 学校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、学校情報セキュリティ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。

(7) 重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクへの対応

学校情報システム管理者は、校務系システムと学習系システムとの間で通信する場合には、各システムにおけるアクセス権管理の徹底を行う等の適切な措置を図らなければならない。

(8) 複合機のセキュリティ管理

ア 学校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、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、適切なセキュリティ要件を策定しなければならない。

イ 学校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切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。

ウ 学校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。

(9) 特定用途機器のセキュリティ管理

学校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

に応じた対策を実施しなければならない。

(10) 無線ＬＡＮ及びネットワークの盗聴対策

ア 学校情報セキュリティ統括責任者は、無線ＬＡＮの利用を認める場合、解読が困難な通信経路の暗号化及び認証技術の使用を義務付けなければならない。

イ 学校情報セキュリティ統括責任者は、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、通信経路の暗号化等の措置を講じなければならない。

(11) 電子メールのセキュリティ管理

ア 学校情報セキュリティ統括責任者は、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 学校情報セキュリティ統括責任者は、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。

ウ 学校情報セキュリティ統括責任者は、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。

エ 学校情報セキュリティ統括責任者は、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。

オ 学校情報セキュリティ統括責任者は、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。

２ アクセス制御

(1) アクセス制御等

ア 学校情報セキュリティ統括責任者又は学校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。

イ 強固なアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、多要素認証等のアクセスの真正性に関する要素技術を取り入れ、当該システムの認証強度の向上とアクセス権管理を徹底すること。

(ｱ)

(2) 外部からのアクセス等の制限

ア 学校情報セキュリティ統括責任者は、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。

イ 学校情報セキュリティ統括責任者は、民間事業者等の外部組織からのシステムアク

セスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る等の措置を講じなければならない。

ウ 学校情報セキュリティ統括責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために通信経路の暗号化等の措置を講じなければならない。

エ 学校情報セキュリティ統括責任者及び学校情報システム管理者は、外部からのアクセスに利用する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。

オ 学校情報セキュリティ統括責任者は、外部から学校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

学校情報セキュリティ統括責任者及び学校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接続の可否が自動的に識別される仕組みを設けなければならない。

(4) ログイン時の表示等

学校情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員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しなければならない。

(5) 特権による接続時間の制限

学校情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

3 システム開発、導入、保守等

(1) 情報システムの調達

ア 学校情報セキュリティ統括責任者及び学校情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ 学校情報セキュリティ統括責任者及び学校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

ア システム開発における責任者及び作業者の特定

学校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。

イ システム開発における責任者、作業者のＩＤの管理

(ｱ) 学校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) 学校情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

ウ システム開発に用いるハードウェア及びソフトウェアの管理

(ｱ) 学校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) 学校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

ア 開発環境と運用環境の分離及び移行手順の明確化

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

イ テスト

(ｱ) 学校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) 学校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) 学校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) 学校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) 学校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

ア 学校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。

イ 学校情報システム管理者は、テスト結果を一定期間保管しなければならない。
ウ 学校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並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
ア 学校情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。
イ 学校情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。
ウ 学校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
学校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
学校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
学校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

(1) 学校情報セキュリティ統括責任者の措置事項
学校情報セキュリティ統括責任者は、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などにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止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など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、必要に応じ教職員等に対して注意喚起しなければならない。
エ 所掌するサーバ及び端末に、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。

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。

キ 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。

(2) 学校情報システム管理者の措置事項

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

ア 学校情報システム管理者は、その所掌するサーバ及び端末を守るため、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。

イ 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。

ウ 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。

5 不正アクセス対策

(1) 学校情報セキュリティ統括責任者の措置事項

学校情報セキュリティ統括責任者は、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。

ア 使用されていないポート及びＳＳＩＤ（無線ＬＡＮネットワーク名）を閉鎖しなければならない。

イ 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。

ウ 学校情報セキュリティ統括責任者は、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。

(2) 攻撃への対処

ＣＩＳＯ及び学校情報セキュリティ統括責任者は、サーバ等に攻撃を受けた場合、又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) サービス不能攻撃

学校情報セキュリティ統括責任者及び学校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。

(4) 標的型攻撃

学校情報セキュリティ統括責任者及び学校情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

6 セキュリティ情報の収集

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

学校情報セキュリティ統括責任者及び学校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) 不正プログラム等のセキュリティ情報の収集及び周知

学校情報セキュリティ統括責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員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

学校情報セキュリティ統括責任者及び学校情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第７章　運用

１ 情報システムの監視

(1) 学校情報セキュリティ統括責任者及び学校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) 学校情報セキュリティ統括責任者及び学校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) 内部からの攻撃監視

学校情報セキュリティ統括責任者及び学校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端末からの所管するネットワーク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。

２ ドキュメントの管理

(1) システム管理記録及び作業の確認

ア 学校情報システム管理者は、所管する学校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 学校情報セキュリティ統括責任者及び学校情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

ウ 学校情報セキュリティ統括責任者、学校情報システム管理者又は学校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、学校情報システム担当者が作業内容を事前に確認しなければならない。

(2) 情報システム仕様書等の管理

学校情報セキュリティ統括責任者及び学校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。

(3) 障害記録の管理

学校情報セキュリティ統括責任者及び学校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。

(4) 記録の保存

ＣＩＳＯ及び学校情報セキュリティ統括責任者は、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。

3 教職員等のＩＤ及びパスワードの管理

(1) 利用者ＩＤの取扱い

ア 学校情報セキュリティ統括責任者及び学校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の取扱い等の方法を定めなければならない。

イ 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、学校情報セキュリティ統括責任者又は学校情報システム管理者に通知しなければならない。

(2) パスワードに関する情報の管理

ア 学校情報セキュリティ統括責任者又は学校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。

4 学校情報セキュリティ統括責任者又は学校情報システム管理者は、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。特権を付与されたＩＤの管理等

(1) 学校情報セキュリティ統括責任者及び学校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。

(2) 学校情報セキュリティ統括責任者及び学校情報システム管理者の特権を代行する者は、学校情報セキュリティ統括責任者及び学校情報システム管理者が指名し、ＣＩＳＯが認めた者でなければならない。

(3) ＣＩＳＯは、代行者を認めた場合、速やかに学校情報セキュリティ統括責任者、学校情報セキュリティ責任者、学校情報セキュリティ管理者及び学校情報システム管理者に通知しなければならない。

(4) 学校情報セキュリティ統括責任者及び学校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、外部委託事業者に行わせてはならない。

(5) 学校情報セキュリティ統括責任者及び学校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、その利用期間に合わせて特権ＩＤを作成・削除する、若しくは、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。

(6) 学校情報セキュリティ統括責任者及び学校情報システム管理者は、特権を付与されたＩＤのパスワードを初期設定以外のものに変更しなければならない。

5 学校情報セキュリティポリシーの遵守状況の確認及び管理

(1) 遵守状況の確認及び対処

ア 学校情報セキュリティ責任者及び学校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、速やかに学校情報セキュリティ委員会に報告しなければならない。

イ 学校情報セキュリティ委員会は、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 学校情報セキュリティ統括責任者及び学校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) 端末及び電磁的記録媒体等の利用状況調査

ＣＩＳＯ及びＣＩＳＯ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端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(3) 業務以外の目的でのウェブ閲覧の禁止

学校情報セキュリティ統括責任者は、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、学校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。

(4) 教職員等による不正アクセスの管理

学校情報セキュリティ統括責任者及び学校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等の学校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 他団体との情報システムに関する情報等の交換

学校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、学校情報セキュリティ統括責任者及び学校情報セキュリティ責任者の許可を得なければならない。

7 侵害時の対応等

(1) 緊急時対応計画の策定

ＣＩＳＯ又は学校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、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。

(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。

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) 業務継続計画との整合性確保

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、学校情報セキュリティ委員会は当該計画と学校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

ＣＩＳＯ又は学校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。

8 例外措置

(1) 例外措置の許可

学校情報セキュリティ管理者及び学校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、ＣＩＳＯ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

学校情報セキュリティ管理者及び学校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ＣＩＳＯに報告しなければならない。

(3) 例外措置の申請書の管理

ＣＩＳＯは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

9 法令等遵守

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) 教育公務員特例法（昭和24年法律第1号）

(3) 著作権法（昭和45年法律第48号）

(4) 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）

(5) 個人情報の保護に関する法律（平成15年法律第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) サイバーセキュリティ基本法（平成26年法律第104号）

(8) 周南市個人情報の保護に関する法律施行条例（令和4年条例第41号）

１０ 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) 学校情報セキュリティ統括責任者又は学校情報セキュリティ責任者が違反を確認した場合、学校情報セキュリティ統括責任者は、当該教職員等が所属する学校等の学校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) 学校情報システム管理者等が違反を確認した場合、違反を確認した者は、速やかに学校情報セキュリティ統括責任者及び当該教職員等が所属する学校等の学校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。

第８章　外部委託

１ 外部委託事業者の選定基準

(1) 学校情報システム管理者は、外部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。

(2) 学校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。

(1) 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の遵守

(2) 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

(3) 提供されるサービスレベルの保証

(4) 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

(5) 外部委託事業者の従業員に対する教育の実施

(6) 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

(7) 業務上知り得た情報の守秘義務

(8) 再委託に関する制限事項の遵守

(9) 委託業務終了時の情報資産の返還、廃棄等

(10) 委託業務の定期報告及び緊急時報告義務

(11) 市による監査、検査

(12) 市による情報セキュリティインシデント発生時の公表

(13) 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

学校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、必要に応じ契約に基づき措置しなければならない。また、その内容を学校情報セキュリティ統括責任者に報告するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

4 外部委託事業者に対する説明

学校情報システム管理者は、ネットワーク及び情報システムの開発・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、学校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。

第９章　ＳａａＳ型パブリック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) クラウドサービスでの情報資産の取り扱い

機密性２Ｂ以上の情報資産をクラウドサービスで取り扱ってはならない。ただし、十分なセキュリティ対策が講じられていると学校情報セキュリティ統括管理者が認める場合は、この限りでない。

(2) 利用者認証

ア 学校情報システム管理者は、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若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又は合意しなければならない。

イ 学校情報システム管理者は、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又は合意しなければならない。

ウ 学校情報システム管理者は、管理者権限を有する者のＩＤの管理について、「第７章　４　特権を付与されたＩＤの管理等」を遵守しなければならない。

エ クラウドサービス利用時は、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) アクセス制御

ア 学校情報システム管理者は、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又は合意しなければならない。

イ 学校情報システム管理者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産ごとに、許可されたクラウドを利用する教職員等及び児童生徒のみがアクセスできる環境を設定しなければならない。

(4) クラウドに保管するデータの暗号化

学校情報システム管理者は、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又は合意しなければならない。

(5) マルチテナント環境におけるテナント間の安全な管理

学校情報システム管理者は、複数の情報システム管理者がクラウドリソースを共用する環境において、特定の情報システム管理者に対して発生したセキュリティ侵害が、他の情報システム管理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又は合意しなければならな

い。

(6) 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 学校情報システム管理者は、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又は合意しなければならない。

イ 学校情報システム管理者は、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、学校情報システム管理者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又は合意しなければならない。

(7) 情報の通信経路のセキュリティ確保

ア 学校情報システム管理者は、学校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 学校情報システム管理者は、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、サービス提供定款や契約書面上で確認又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物理的セキュリティ対策

ア 学校情報システム管理者は、当該クラウドサービスのサーバ等の管理条件を「第４章　１　サーバ等の管理」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又は合意しなければならない。

イ 学校情報システム管理者は、クラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理において、「第４章　２　管理区域(情報システム室等)の管理」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又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運用管理

ア 学校情報システム管理者は、当該クラウドサービスにおけるサーバの冗長化について、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又は合意しなければならない。

イ 学校情報システム管理者は、当該クラウドサービスにおけるデータバックアップ及び復旧手順について、「第６章　１(2)　バックアップの実施」に準じた対策をク

ラウド事業者に求め、サービス提供約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 学校情報システム管理者は、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監査に必要なログの取得について、「第６章　１(3)　ログの取得等」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又は合意しなければならない。

(10) 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 学校情報システム管理者は、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又は合意しなければならない。

イ 学校情報システム管理者は、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又は合意しなければならない。

(11) 情報システム管理者側のセキュリティ確保

ア 学校情報システム管理者は、クラウドサービスにアクセスする教職員等及び児童生徒の端末について、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 学校情報システム管理者は、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、クラウドを利用する教職員等及び児童生徒への教育や入口対策を講じなければならない。

(12) クラウド事業者従業員の人的セキュリティ対策

ア 学校情報システム管理者は、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要領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又は合意しなければならない。

イ 学校情報システム管理者は、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又は合意しなければならない。

ウ 学校情報システム管理者は、クラウドサービスに関わらない従業員等が学校情報システム管理者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又は合意しなければならない。

エ 学校情報システム管理者は、情報システム管理者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、学校情報システム管理者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又は合意しなければならない。

オ 学校情報システム管理者は、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、マルウェアを侵入させないよう、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又は合意しなければならない。

(13) サービス終了時のデータの廃棄及び利用者アカウントの抹消について

ア 学校情報システム管理者は、サービス利用終了時等において、クラウドを利用する教職員等及び児童生徒のデータ及び利用者アカウント情報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又は合意しておかなければならない。

イ 学校情報システム管理者は、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又は合意しておかなければならない。

ウ 学校情報システム管理者は、クラウドサービスで利用する全ての情報資産について、サービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

(14) クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

学校情報システム管理者は、利用するクラウドサービスの要件規準を確認し、要件規準を満たすネットワークを設計しなければならない。

２ ＳａａＳ型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

学校情報システム管理者は、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

学校情報システム管理者は、クラウド事業者がどのような規範（クラウド事業者の準拠する認証制度、個人情報保護指針、プライバシーポリシー、情報セキュリティに関する基本方針及び対策基準、保守運用管理要領等）に基づいてサービス提供するか開示を求め、情報システム管理者の準拠する法令、情報セキュリティポリシーを確認し、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

学校情報システム管理者は、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等について確認し、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 学校情報システム管理者は、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 学校情報システム管理者は、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 学校情報システム管理者は、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 学校情報システム管理者は、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情報システム管理者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 学校情報システム管理者は、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 学校情報システム管理者は、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、学校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 学校情報システム管理者は、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 学校情報システム管理者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と及びインシデント対応フローを検証し、インシデントに備えた組織体制を整備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

学校情報システム管理者は、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 学校情報システム管理者は、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 学校情報システム管理者は、前項の提示内容が、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 学校情報システム管理者は、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 学校情報システム管理者は、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又は合意しなければならない。

ウ 学校情報システム管理者は、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。

エ 学校情報システム管理者は、クラウド事業者において個人情報の適切な管理が行われているか確認するとともに、確認した項目については、調達時においてサービスの過剰な排除にならないよう留意した上で、契約要件等として定めなければならない。

３ ＳａａＳ型パブリッククラウドサービス利用における教職員等の留意点

(1) ＩＤ・パスワード等の秘匿

ア 教職員等は、ＩＤ・パスワードについて秘匿管理を行わなければならない。

イ 教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。もし該当要素が流出等したと考えられる場合には、速やかに学校情報セキュリティ管理者に報告しなければならない。

(2) ＳａａＳ型パブリッククラウドサービスを利用する端末の管理

教職員等は、クラウドサービスにアクセスする際に活用する端末について、紛失・盗難を避けるよう、適切に管理しなければならない。

(3) 情報分類に基づく情報管理

学校情報セキュリティ統括管理者が認めるパブリッククラウド上で機密性２Ｂ以上の情報資産を取扱う場合には、多要素認証を含む強固なアクセス制御による対策を講じる必要がある。

(4) 学校外からのＳａａＳ型パブリッククラウドサービス利用

ア 教職員等は、学校外からクラウドサービスを利用する際、情報資産の取扱いを当該クラウドサービス上のみで行うことを原則とする。

イ クラウドサービスから端末にファイルをダウンロードする際は、情報資産の外部持ち出しに基づく安全管理措置として、端末の安全性を事前に確認するとともに、作業が終わり次第当該端末から情報資産をすみやかに消去しなければならない。

(5) ＳａａＳ型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

教職員等は、クラウドサービスを学習用途と校務用途で適切に使い分けるよう、共有先やダウンロード方法等の運用ルールについてあらかじめ確認し、適切に運用しなければならない。

4 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

学校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。

ア 約款によるサービスを利用してよい範囲

イ 業務により利用する約款による外部サービス

ウ 利用手続及び運用手順

(2) 約款による外部サービスの利用における対策の実施

教職員等は、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

(1) 学校情報システム管理者は、本市教育委員会又は学校等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 学校等のアカウントによる情報発信が、実際の学校等のものであることを明らかにするために、学校等が自己管理するホームページ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。

(2) 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。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章　１人１台学習者用端末におけるセキュリティ

１ 学習者用端末のセキュリティ対策

(1) 授業に支障のないネットワーク構成の選択（帯域や同時接続数など）

学校情報セキュリティ統括責任者は、１人１台学習者用端末の授業等での一斉利用などを考慮し、十分な帯域や同時接続数を確保した適切なネットワーク構成を設計すること。また、運用状況を定期的に検証・評価し、必要に応じて改修計画を策定しなければならない。

(2) 不適切なウェブページの閲覧防止

学校情報セキュリティ統括責任者は、児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止するため、以下の対策等を講じなければならない。

ア フィルタリングソフトウェア

イ 検索エンジンのセーフサーチ

ウ セーフブラウジング

(3) マルウェア感染対策

学校情報セキュリティ統括責任者は、学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

(4) 端末を不正利用させないための防止策

学校情報セキュリティ統括責任者は、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が安心して利用できる状態を維持しなければならない。

(5) セキュリティ設定の一元管理

学校情報セキュリティ統括責任者は、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仕組みを設けなければならない。

(6) 端末の盗難・紛失時の情報漏洩対策

学校情報セキュリティ統括責任者は、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。また、児童生徒が端末を紛失した場合、遠隔操作でロックをかける、又はワイプ（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。

(7) 運用・連絡体制の整備

学校情報セキュリティ管理者は、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等にて整理しなければならない。

２ 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

ア 入学・転入時のＩＤ登録処理

ＩＤについては同一組織内で重複せず、シンプルかつ識別可能なものを設定するものとし、また、児童生徒によるサービス毎のＩＤ・パスワード等の認証情報の入力や、アカウント情報管理を簡素化するため、学校情報システム管理者は、シングルサインオンの導入に努めなければならない。

イ 転出・卒業・退学時のＩＤ削除処理

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てはならない。転出や卒業・退学時に学習用ツールのサービス利用期間が終了する場合、あらかじめ児童生徒本人によるデータ移行を必要に応じサービス利用期間内に実施し、ＩＤの利用停止後、ＩＤ及び関連するデータの完全削除を行わなければならない。

第１１章　評価・見直し

１ 監査

(1) 実施方法

学校情報セキュリティ責任者は、学校等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 学校情報セキュリティ責任者は、監査を実施する場合には、監査対象の学校等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者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 学校情報セキュリティ責任者は、監査を行うに当たって、監査実施計画を立案し、学校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 監査対象の学校等は、監査の実施に協力しなければならない。

(4) 外部委託事業者に対する監査

監査の実施を外部委託事業者に委託している場合、学校情報セキュリティ責任者は、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、学校情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。

(5) 報告

学校情報セキュリティ責任者は、監査結果を取りまとめ、学校情報セキュリティ委員会に報告する。

(6) 保管

学校情報セキュリティ責任者は、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

ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する学校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学校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。

(8) 学校情報セキュリティポリシー及び関係要領等の見直し等への活用

学校情報セキュリティ委員会は、監査結果を学校情報セキュリティポリシー及び関係要領等の見直し、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 学校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 学校情報セキュリティ責任者は、学校情報セキュリティ管理者と連携して、所管する学校等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

学校情報セキュリティ統括責任者、学校情報システム管理者及び学校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、学校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 学校情報セキュリティ委員会は、この点検結果を学校情報セキュリティポリシー及び関係要領等の見直し、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及び関係規定等の見直し

学校情報セキュリティ委員会は、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、学校情報セキュリティポリシー及び関係要領等について見直しを行うものとする。

附　則

この対策基準は、平成２０年６月３０日から施行する。

附　則

この対策基準は、平成２８年１月１日から施行する。

附　則

この対策基準は、令和６年２月１日から施行する。

附　則

この対策基準は、令和７年２月１日から施行する。