淡路市教育情報セキュリティポリシー

制 定 日：平成２８年１２月１２日
施 行 日：平成２９年　４月　１日
一部改定：令和　６年１０月２１日

淡路市教育委員会

目　次

第１章 淡路市教育情報セキュリティポリシーの目的及び構成

１．目的

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いる。一方で、不正アクセス並びにコンピュータウイルス等の新たな攻撃手法による情報資産の漏えい、破壊及び改ざん並びに操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害にも備える必要がある。

淡路市（以下「本市」という。）の各小中学校（以下「学校」という。）は、児童・生徒、保護者等の個人情報及び学校教育の運営上重要な情報を多数取り扱っている。これらの情報資産を様々な脅威から防御することは、児童・生徒、保護者等の権利利益を守るため、また、学校教育の安定的、継続的な運営のために必要不可欠である。

上記のことに鑑み、淡路市教育委員会（以下「教育委員会」という。）は、児童生徒や教職員が安心して ICT を活用できる環境を構築するとともに、学校の情報資産の機密性、完全性及び可用性※1 を維持するための情報セキュリティ対策を講じることを目的として、淡路市教育情報セキュリティポリシー（以下「教育情報セキュリティポリシー」という。）を定めることとする。

※１　国際基準化機構（ISO）が定めるもの（ISO7498-2 : 1989）

- 機密性：情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。
- 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：許可された利用者が必要なときに情報アクセスできることを確実にすること。

２．構成

教育情報セキュリティポリシーは、教育委員会及び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、総合かつ体系的な内容を具体的に取りまとめたものを総称するものである。

教育情報セキュリティポリシーは、学校が保有する情報資産を取り扱う全ての教職員に浸透、普及、定着させるものであり、一定の普遍性を備えた部分としての「基本方針」と、情報資産を取り巻く状況の変化に対応する部分としての「対策基準」から構成する。

（「基本方針」は、教育委員会及び学校が所掌する情報資産においても、淡路市全体の基本方針と共通のものであるとの認識の上に立ち、淡路市の情報セキュリティポリシーにおける基本方針を準用するものとする。）また、教育情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として「淡路市教育情報セキュリティ実施手順」を各学校において策定するものとする。なお、教育情報セキュリティポリシーならびに実施手順に関する情報は、情報漏えい防止の観点から、非公開とする。

淡路市教育情報セキュリティポリシーの構成

文書名		内容
淡路市教育情報セキュリティポリシー	淡路市教育情報セキュリティ基本方針	学校教育に関する情報セキュリティ対策の統一的かつ基本的な方針
	淡路市教育情報セキュリティ対策基準	学校教育に関する情報セキュリティ基本方針を実行に移すため、ネットワーク及び情報システムに共通の情報セキュリティ対策の基準
淡路市教育情報セキュリティ実施手順		情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

第２章 淡路市教育情報セキュリティ基本方針

１．趣旨

この教育情報セキュリティ基本方針は、学校の教育情報セキュリティ対策の基本的な方針を定めるものとする。

２．定義

教育情報セキュリティポリシーにおいて、次に掲げる用語の意義は、それぞれ当該各号に定める。

（１）情報資産

ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体やこれらの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。なお、情報資産には、紙等の有体物に出力された情報も含むものとする。

（２）教育情報システム

ネットワーク及びハードウェア、ソフトウェア（アプリケーションを含む。）、記録媒体で構成され、情報処理を行う仕組みをいう。

（３）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

３．対象範囲

（１）適用範囲

本基本方針が適用される範囲は、淡路市教育委員会事務局並びに淡路市立学校設置条例（平成 17 年 4 月 1 日条例第 224 号）第 1 条により設置する市立学校のうち、同条例第 2 条に規定する別表に掲げる小学校及び中学校（以下「市内小中学校」という。）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。

ア 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

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

ウ 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

４．教育情報セキュリティ管理体制

教育委員会事務局及び市内小中学校における情報資産について、市長部局と連携し、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５．情報資産の分類及び管理

教育委員会事務局及び市内小中学校が保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

６．情報資産への脅威

情報資産に対する脅威を以下に想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、部外者の侵入等による機器又は情報資産の漏えい・破壊・改ざん・消去・盗難、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し及び持ち出しによる紛失、不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、火災等の災害並びに事故、故障等によるサービス及び業務の停止

（４）大規模・広範囲にわたる疾病等による要員不足に伴うシステム運用の機能不全等
（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

７．教育情報セキュリティ対策
　教育情報セキュリティを確保するため、次に掲げる教育情報セキュリティ対策を講ずるものとする。
（１）物理的セキュリティ対策
　情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。
（２）人的セキュリティ対策
　情報セキュリティに関し、教職員等及び外部委託事業者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ずる。
（３）技術及び運用におけるセキュリティ対策
　情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、情報システムの監視、教育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の運用面の対策を講ずる。
（４）障害時におけるセキュリティ対策
　情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画の策定等の対策を講ずる。
（５）外部サービスの利用
　外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。約款による外部サービスを利用する場合には、利用に係る規定を整備し対策を講じる。
　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用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．情報セキュリティ監査及び自己点検の実施
　教育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。

９．教育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、教育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、速やかに教育情報セキュリティポリシーの見直しを実施する。

10．教育情報セキュリティ対策基準の策定
　上記８及び９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等の基準を明らかにする「教育情報セキュリティ対策基準」を定めるものとする。

11．教育情報セキュリティ実施手順の策定
　教育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「教育情報セキュリティ実施手順（以下「実施手順」という。）」を策定するものとする。
　なお、教育情報セキュリティポリシー及び実施手順は、公にすることにより本市の教育行政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３章 淡路市教育情報セキュリティ対策基準

１　趣旨

この教育情報セキュリティ対策基準は、教育情報セキュリティ基本方針において規定する教育情報セキュリティ対策を実行に移すための、淡路市の教育情報セキュリティ対策の基準を定めるものとする。

２　組織体制

市内小中学校の教育情報セキュリティ管理体制については、以下のとおりとする。

（１）最高教育情報セキュリティ責任者(CISO: Chief Information Security Officer、以下「CISO」という。）

ア　CISO は、教育委員会事務局が所管す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。CISO は、教育長をもって充てる。

イ　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する者を最高情報セキュリティアドバイザーとして置くことができる。

（２）統括情報セキュリティ責任者 CIO (CIO:Chief Information Officer、以下「CIO」という）

ア　教育部長を CISO 直属の CIO とし、CISO を補佐しなければならない。

イ　CIO は、市内小中学校の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

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

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

オ　CIO は、市内小中学校の情報資産に対するセキュリティ侵害が発生したとき、又はセキュリティ侵害のおそれがあるとき（以下「緊急時等」という。）には、CISO の指示に従い、又は CISO が不在のときは、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。

カ　CIO は、市内小中学校の共通的なネットワーク、情報システム及び情報資産に関する教育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。

キ　CIO は、緊急時等の円滑な情報共有を図るため、CISO、CIO、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び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。

ク　CIO は、緊急時等において、直ちに CISO 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）情報セキュリティ責任者

ア　教育部学校教育課長を情報セキュリティ責任者とする。

イ　情報セキュリティ責任者は、市内小中学校の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。

ウ　情報セキュリティ責任者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

エ　情報セキュリティ責任者は、所管す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、教育情報セキュリティポリシーの遵守に関する意見の集約、教職員等（常勤教職員、非常勤教職員及び臨時教職員）に対する教育、訓練、助言及び指示を行う。

（４）情報セキュリティ管理者 （学校 CIO：Chief Information Officer、以下「学校 CIO」という。）

ア　学校長を学校 CIO とする。
イ　学校 CIO は、その所管する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。
ウ　学校 CIO は、その所管する学校において、緊急時等には、直ちに情報セキュリティ責任者、CIO 及び CISO に報告を行い、指示を仰がなければならない。

（５）情報システム管理者
ア　教育総務課長を情報システム管理者とする。
イ　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
ウ　情報システム管理者は、所管する情報システムにおける情報セキュリティ対策に関する権限及び責任を有する。
エ　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持管理を行う。

（６）情報システム担当者
ア　教育総務課 ICT 担当を情報システム担当者とする。
イ　情報システム担当者は、情報システム管理者の指示等に従い、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）情報セキュリティ担当者
ア　学校の ICT 担当者等を情報セキュリティ担当者とする。
イ　情報セキュリティ担当者は、学校 CIO の情報セキュリティに関する適正な運用及び管理を補佐するため、学校 CIO に情報セキュリティに必要な情報を提供し、その指示によって学校内の情報セキュリティ対策を推進する。

（８）学校情報セキュリティ委員会
ア　CISO は、市内小中学校の情報セキュリティ対策に関する重要事項を決定し、統一的に対策を講じるため、学校情報セキュリティ委員会（以下「委員会」という。）を設く。
イ　委員会の委員は、CISO、CIO、情報セキュリティ責任者、学校 CIO、情報システム管理者をもって充てる。
ウ　委員会は、リスク情報を共有し、教育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。
エ　委員会は、市内小中学校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。

（９）兼務の禁止
ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
イ　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（１０）情報セキュリティに関する統一的な窓口の設置
ア　CISO は、情報セキュリティに係る事件・事故等（以下「情報セキュリティインシデント」という。）の統一的な窓口の機能を有する組織を教育委員会内に置き、情報セキュリティインシデントについて市内小中学校から報告を受けた場合には、その状況を確認させ、自らへの報告を行わせる。
イ　CISO による情報セキュリティ戦略の意思決定が行われた場合は、その内容を関係部局及び市内小中学校に提供する。
ウ　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・公表の対応を行わなければならない。
エ　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。

３　対象範囲及び用語説明

（１）適応範囲

本対策基準が適用される範囲は、淡路市教育委員会事務局並びに市内小中学校とする。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりである。

ア 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

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

ウ 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

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、教員の個人情報等、学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定とした情報であり、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、保護者への連絡ツ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や作品等、学校が保有する情報資産のうち、それらの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とした情報であり、教員及び児童生徒がアクセスすることを想定する情報
校務用端末	校務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、教員のみが利用可能な端末
校務系システム	校務系ネットワークや校務系サーバ、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、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
教育系システム	学習系ネットワークや学習系サーバ、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、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
学習系ストレージ	学習系情報を取り扱うストレージ
学習系サーバ	学習系情報を取り扱うサーバ

４．情報資産の分類及び管理

（１）情報資産の分類

教育委員会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。また、情報資産の分類における具体的な情報資産は別表（P34～36）に示す。

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（秘密文書相当）
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のある情報
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（児童生徒個々も含む。）のみが知り得る状態を確保する必要のある情報
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（教職員及び児童生徒以外の者が知り得ても支障がない）として作成された情報

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、業務の遂行に支障がある情報
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、業務の遂行に軽微な支障がある情報
完全性 1	完全性 2A又は完全性 2Bの情報資産以外の情報資産	事故があった場合でも業務の遂行に支障がない情報

可用性による情報資産の分類

分類	分類基準	該当する情報資産のイメージ
可用性 2B	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される、又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	必要なとき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、紛失又は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	必要なとき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、紛失又は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

ア 管理責任

（ア） 学校 CIO は、その所管する情報資産について管理責任を有する。

（イ） 学校 CIO は、情報資産が複製又は伝送された場合は、複製等された情報資産も（１）の情報資産の分類に基づき、管理しなければならない。

（ウ） 学校 CIO は、その所管する情報資産について、誤り等を発見した場合には、速やかに、かつ、適切に訂正等を行わなければならない。

イ 情報資産の分類の表示

教職員は、情報資産について「淡路市立小中学校文書分類表」に基づき、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等、適切な管理を行わなければならない。

ウ 情報の作成、複製及び訂正

（ア） 教職員は、業務上必要のない情報を作成してはならない。

（イ） 情報を作成する者は、情報の作成時に（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。

（エ） 教職員は、機密性 2 以上の情報を複製する場合は、学校 CIO の許可を得なければならない。

（オ） 教職員は、情報資産の内容に誤り等を発見した場合には、学校 CIO の指示に従い、速やかに、かつ、適切に訂正等しなければならない。

エ 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は、学校 CIO に判断を仰がなければならない。

オ 情報資産の利用

（ア） 情報資産を利用する者は、校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、適切な取扱いをしなければならない。

（ウ） 情報資産を利用する者は、電磁的記録媒体又は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は、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。

（エ） 学校 CIO は、機密性 2 以上の情報資産のうち特定個人情報等を取り扱う業務を実施する区域を明確にし、物理的な安全措置を講じなければならない。

カ 情報資産の保管

（ア） 学校 CIO 又は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。なお、情報資産の保管場所は、次のとおりとする。

保管場所	保管できる情報資産
教員用ファイルサーバ	全ての情報資産
グループウェア	機密性 2Ｂ以上の情報
デジタルドリル	機密性 2Ａ以下の情報
校務支援システム	機密性 2Ｂ以上の情報
学習支援ソフト	機密性 2Ａ以下の情報（ただし、機微情報を除く。）
学校内補助記憶装置（外付けハードディスク等） ※校外に物理的な持ち出しができない記憶媒体	写真や動画と、機密性 2Ａ以下の情報（ただし、機微情報を除く。）
学校内補助記憶媒体（USB、DVD 等） ※校外に物理的な持ち出しができる記憶媒体	原則として、機密性 2Ａ以下の情報

（イ） 学校 CIO 又は情報システム管理者は、情報資産を記録した USB メモリ等の外部電磁的記録媒体を保管する場合は、外部電磁的記録媒体への書込禁止の措置を講じなければならない。

（ウ） 学校 CIO 又は情報システム管理者は、情報システムのバックアップで取得したデータを記録する電磁的記録媒体を保管する場合は、自然災害の影響を受ける可能性が低い地域又は場所に保管しなければならない。なお、クラウドサービスを利用する場合は、サービスの機能として自然災害対策がなされていることを確認しなければならない。

（エ） 学校 CIO 又は情報システム管理者は、（１）の分類における機密性、完全性及び可用性の 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は、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。

キ 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） 電子メール等により（１）の分類における機密性 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（アクセス制限や暗号化）を行わなければならない。

（イ） 学校 CIO 及び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。

ク 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、学校 CIO に許可を得なければならない。

ケ 情報資産の提供・公表

（ア） 機密性 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、学校 CIO に許可を得なければならない。

（ウ） 学校CIO及び情報システム管理者は、児童生徒、保護者又は市内小中学校関係者に公開する情報資産について、完全性を確保しなければならない。

コ 情報資産の廃棄

（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は、電磁的記録媒体の初期化等、情報を復元できないように措置した上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、学校 CIO の許可を得なければならない。

５．物理的セキュリティ

（１）サーバ等の管理

ア 機器の取付け等

情報システム管理者は、サーバ等の機器の取付けを行うときは、火災、水害、埃（ほこり）、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。

イ サーバの冗長化

（ア） 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は、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。

（イ） 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。

ウ 機器の電源

（ア） 情報システム管理者は、CIO 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） 情報システム管理者は、CIO 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。

エ 通信ケーブル等の配線

（ア） CIO 及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷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） CIO 及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷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） CIO 及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等、適切に管理しなければならない。

（エ） CIO 及び情報システム管理者は、自ら又は情報システム担当者若しくは契約に

より操作を認められた外部委託事業者以外の者が配線の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。

オ 機器の定期保守及び修理

（ア） 情報システム管理者は、可用性2Ａ以上の情報資産を保存するサーバ等の機器の定期保守を実施しなければならない。

（イ） 情報システム管理者は、電磁的記録媒体を内蔵する機器を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、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。

カ 施設外又は学校外への機器の設置

CIO 及び情報システム管理者は、校外にサーバ等の機器を設置するときは、CISO の承認を得なければならない。また、定期的に当該機器の情報セキュリティ対策状況について確認しなければならない。

キ 機器の廃棄等

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は、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

ア 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、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）又は電磁的記録媒体の保管庫をいう。

（イ） CIO 及び情報システム管理者は、施設管理者等と連携し、管理区域から外部に通ずるドアを必要最小限とし、鍵、監視機能、警報装置等によって許可のない者の立入りを防止しなければならない。

（ウ） CIO 及び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。

（エ） CIO 及び情報システム管理者は、施設管理者等と連携し、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

（オ） CIO 及び情報システム管理者は、施設管理者等と連携し、情報システム室内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。

イ 管理区域の入退室管理等

（ア） 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） 教職員及び外部委託事業者等が管理区域に入室する際は、身分証明書等を携帯し、情報システム管理者が身分証明書等の提示を求める場合は、その求めに応じなければならない。

（ウ） 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育委員会事務局職員が付き添うものとし、外見上、当該職員と区別できる措置を講じなければならない。

（エ） 情報システム管理者は、機密性2Ｂ以上の情報資産を扱う情報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、モバイル端末、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。

ウ 機器等の搬入出

（ア） 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） 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、教育委員会事務局職員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

ア CIO は、市内小中学校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。

イ CIO 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。

ウ CIO 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、通信経路上での暗号化を行わなければならない。

エ CIO は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

オ CIO 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。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

（４）教職員等の利用する端末や電磁的記録媒体等の管理

ア 校務用端末及び指導者用端末

（ア） 情報システム管理者は、盗難防止のため、職員室及び教室等で利用する校務用端末並びに指導者用端末の保管庫による管理等、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（イ） 情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

（ウ） 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。また、電磁的記録媒体についてもデータ暗号化機能を備える媒体又は認証パスワード付与機能付きの媒体を使用しなければならない。

イ 学習者用端末

情報システム管理者は、盗難防止のため、教室等で利用する場合は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。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。

６．人的セキュリティ

（１）教職員等における情報セキュリティの徹底

ア 教育情報セキュリティポリシーの遵守

教職員等は、教育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 CIO に相談し、指示を仰がなければならない。

イ 業務以外の目的での使用の禁止

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

ウ モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア） CISO は、機密性 2B、可用性 2B及び完全性 2B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） 教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、学校 CIO の許可を得なければならない。

（ウ） 教職員等は、外部で情報処理業務を行う場合には、学校CIOの許可を得なければならない。

エ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア） 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、学校 CIO の許可を得て利用することができる。ただし、機密性３の情報資産における情報処理を行ってはならない。

（イ） 教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、学校 CIO の許可を得た上で、外部で情報処理作業を行う際に必要な安全管理措置を遵守しなければならない。

オ 持ち出し及び持ち込みの記録

学校 CIO は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

カ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を学校CIOの許可なく変更してはならない。

キ 机上の端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること、又は学校CIOの許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

ク 退職時等の遵守事項

（ア） 教職員等は、異動、退職等により校務を離れるときは、利用していた情報資産を返却しなければならない。

（イ） 教職員等は、異動、退職等により校務を離れた後においても、校務上知り得た情報を漏らしてはならない。

（２）非常勤及び臨時の教職員への対応

ア 教育情報セキュリティポリシー等の遵守

学校 CIO は、非常勤教職員及び臨時教職員（以下「非常勤教職員等」という。）に対し、採用時に教育情報セキュリティポリシー等のうち、非常勤教職員等が守るべき内容を理解させ、実施及び遵守させなければならない。

イ 教育情報セキュリティポリシー等の遵守に対する同意

学校 CIO は、非常勤教職員等の採用の際、必要に応じ、教育情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

ウ インターネット接続及び電子メール使用等の制限

学校 CIO は、非常勤教職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要なときは、これを利用できないよう所要の措置を講じなければならない。

（３）児童生徒への対応

ア 教職員等は、児童生徒に対し、セキュリティを保つために必要な学習用端末やインターネット利用に関する基本的な項目や、異常時の報告について指導しなければならない。

イ 申込書やアンケート、契約書等、書面(電子メール、ホームページへの記入等電磁的方法含む。)により本人から直接個人情報を取得する場合は、児童生徒本人又は保護者に

対してあらかじめ利用目的を明示しなければならない。ただし、下記各号に該当する場合は、この限りでない。

（ア）人の生命、身体又は財産その他の権利利益を保護するため必要な場合

（イ）法令に定める事務の遂行に支障を及ぼすおそれがある場合

（４）教育情報セキュリティポリシー等の掲示

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

（５）外部委託事業者に対する説明

情報システム管理者は、ネットワーク及び情報システムの開発・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て、教育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。

（６）研修・訓練

ア 情報セキュリティ等に関する研修・訓練

学校 CIO は、定期的に情報セキュリティ等に関する研修及び訓練を実施するものとする。

イ 研修計画の策定及び実施

（ア） 学校CIOは、教職員等に対する情報セキュリティ等に関する研修計画の策定及びその実施体制の構築を定期的に行わなければならない。

（イ） 学校CIOは、教職員等が毎年度１回以上の情報セキュリティ研修等を受講できるよう研修計画を策定しなければならない。

（ウ） 新規採用の教職員等を対象とする情報セキュリティ等に関する研修を実施しなければならない。

（エ） 研修は、学校 CIO、情報システム担当者及びその他教職員等に対して、それぞれの役割、情報セキュリティ等に関する理解度等に応じたものにしなければならない。

（オ） 学校CIOは、委員会に対し、教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。

ウ 緊急時対応訓練

学校 CIO は、緊急時等における対応を想定し、訓練実施の体制、範囲等を定めた訓練計画を策定し、定期的に実施しなければならない。

エ 研修・訓練への参加

教職員等は、定められた研修及び訓練に参加しなければならない。

（７）情報セキュリティインシデントの報告

ア 学校内からの情報セキュリティインシデントの報告

（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ときは、直ちに学校CIOに報告しなければならない。

（イ） 教職員等は、学校CIOの指示に従い、情報セキュリティインシデントに対し適切に対処しなければならない。

（ウ） 学校CIOは、遅滞なくCIO、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。

（エ） 情報セキュリティ責任者は、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CIOに報告しなければならない。

イ 保護者等学校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、市内小中学校が利用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情報セキュリティインシデントについて、保護者等学校外部から報告を受けたときは、直ちに学校CIOに報告しなければならない。

（イ） 学校CIOは、遅滞なく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） 情報セキュリティ責任者は、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CIOに報告しなければならない。

（エ） CISO は、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、保護者等外部から報告を受けるための窓口を学校 CIO の所管する学校に設置し、当該窓口への連絡手段を公表しなければならない。

ウ 情報セキュリティインシデント原因の究明・記録、再発防止等

（ア） CIO は、情報セキュリティインシデントについて、学校 CIO、情報システム管理者及び情報ネットワーク保守管理を委託している業者と連携し、これらの情報セキュリティインシデント原因を究明し、その記録を保存しなければならない。

（イ） CIOは、情報セキュリティインシデントの原因究明結果を基に、再発防止策を検討し、CISOに報告しなければならない。

（ウ） CISOは、CIO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ときは、その内容を確認し、必要に応じて委員会に報告するなど、再発防止策を実施するために必要な措置を講じなければならない。

（８）ID及びパスワード等の管理

ア ID及びアカウントの取扱い

教職員等は、自己の管理する ID 及びアカウント(以下「ID 等」という)に関し、次の事項を遵守しなければならない。

（ア） 自己が管理しているID等は、他人に利用させてはならない。

（イ） 共用 ID 等を利用する場合は、共用 ID 等の利用者以外に利用させてはならない。

イ パスワードの取扱い

教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

（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、学校CIO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） 複数の教育情報システムを扱う教職員等は、シングルサインオンを除き、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。

（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。

（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 等に対するパスワードは除くものとする。

７．技術的セキュリティ

（１）コンピュータ及びネットワークの管理

ア 文書サーバの設定等

（ア）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）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）情報システム管理者は、教職員及び児童生徒、保護者に関する個人情報等、特定の教職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当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。

イ バックアップの実施

CIO 及び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かかわらず、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。

ウ 他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合は、その取扱いに関する事項をあらかじめ定め、CIO 及び情報セキュリティ責任者の許可を得なければならない。

エ システム管理記録及び作業の確認

（ア） 情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

（イ） CIO 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、適切に管理しなければならない。

（ウ） CIO、情報システム管理者又は情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２人以上で作業し、互いにその作業を確認しなければならない。

オ 情報システム仕様書等の管理

CIO 及び情報システム管理者は、ネットワーク図、情報システム仕様書等について、記録媒体にかかわらず、校務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

カ ログの取得等

（ア） CIO 及び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（以下「ログ等」という）を取得し、一定の期間保存しなければならない。

（イ） CIO 及び情報システム管理者は、ログ等に関し、取得する項目、保存期間、取扱方法及びログ等が取得できなくなった場合の対処方法等を定め、適切に管理しなければならない。

（ウ） CIO 及び情報システム管理者は、取得したログ等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からの不正侵入、不正操作等の有無について、点検又は分析を実施しなければならない。

キ 障害記録

CIO 及び情報システム管理者は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

ク ネットワークの接続制御、経路制御等

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

ケ 外部の者が利用できるシステムの分離等

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は、重要性が高い情報である機密性２B、可用性２B及び完全性２B以上の情報資産を扱う

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わなければならない。

コ 外部ネットワークとの接続制限等

（ア） 情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとするときは、あらかじめ、CISO 及び CIO の許可を得なければならない。

（イ） 情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、市内小中学校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） 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校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） CIO 及び情報システム管理者は、ウェブサーバ等をインターネットに公開するときは、校内ネットワークへの侵入を防御するため、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

（オ） 情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じるおそれがあるときは、CIO 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。

サ 機微情報に対するインターネットリスクへの対応

（ア） 情報システム管理者は、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメール等のインターネットを介した外部からのリスクの高いシステムと重要性が高い情報を論理的又は物理的に分離をしなければならない。

（イ） 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をネットワーク分離による対策を講じたシステム構成によって通信する場合は、ウイルス感染のない無害化通信等、適切な措置を講じなければならない。

シ 複合機のセキュリティ管理

（ア） CIO 及び情報システム管理者は、複合機を調達するときは、当該複合機が備える機能、設置環境及び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） CIO 及び情報システム管理者は、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） CIO 及び情報システム管理者は、複合機の運用を終了するときは、複合機の持つ電磁的記録媒体の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。

ス 特定用途機器のセキュリティ管理

CIO 及び情報システム管理者は、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ときは、当該機器の特性に応じた措置を講じなければならない。

セ 無線 LAN 及びネットワークの盗聴対策

（ア） CIO は、無線 LAN の利用を認める場合は、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

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

ソ 電子メールのセキュリティ管理

（ア） CIO 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）されることがないよう、電子メールサーバの設定を行わなければならない。

（イ） CIO は、大量のスパムメール等の受信又は送信を検知したときは、必要に応じてメールサーバの運用を停止しなければならない。

（ウ） CIO 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が送受信できないよう、必要な措置を講じなければならない。

（エ） CIO 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） CIO は、添付ファイルの監視等により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外部に持ち出せないよう、システムに必要な措置を講じなければならない。

タ 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は、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 CIO 及び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 CIO の許可なしに使用してはならない。

チ 電子署名・暗号化

教職員等は、４(１)に規定する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ときは、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

ツ 無許可ソフトウェアの導入等の禁止

（ア） 教職員等は、支給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、CIO 及び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、学校 CIO 又は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。

テ 機器構成の変更の制限

（ア） 教職員等は、支給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、支給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は、CIO 及び情報システム管理者の許可を得なければならない。

ト 無許可でのネットワーク接続の禁止

教職員等は、CIO 及び情報システム管理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。

ナ 業務以外の目的でのウェブ閲覧の禁止

（ア） 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。

（イ） CIO 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 CIO 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

ア アクセス制御等

CIO 又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員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） CIO 及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、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、CIO 又は情報システム管理者に通知しなければならない。

（ウ） CIO 及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

ウ 特権を付与された ID の管理等

（ア） CIO 及び情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

（イ） CIO 及び情報システム管理者の特権を代行する者は、CIO 及び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。

（ウ） CISO は、代行者を認めた場合は、速やかに CIO、情報セキュリティ責任者、学校 CIO 及び情報システム管理者に通知しなければならない。

（エ） CIO 及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ） CIO 及び情報システム管理者は、特権を付与された ID 及びパスワードについて、その利用期間に合わせて特権 ID を作成・削除する、又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。

（カ） CIO 及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

（キ） CIO 及び情報システム管理者は、特権を付与された ID のログ監視を行わなければならない。

（３）教職員等による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、CIO 及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

イ CIO 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 CIO は、組織外部からのシステムアクセスを認める場合は、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。

エ CIO 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 CIO 及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を教職員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 教職員等は、持ち込んだ、又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

キ CIO 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。

（４）自動識別の設定

CIO及び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しなければならない。

（５）ログイン時の表示等

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

（６）パスワードに関する情報の管理

ア CIO 又は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。

イ CIO 又は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。

（７）特権による接続時間の制限

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

（８）システム開発、導入、保守等

ア 情報システムの調達

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

（イ） CIO 及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

イ 情報システムの開発

（ア） システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。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及び作業者の ID の管理

① 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。

② 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

（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

① 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。

② 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。

ウ 情報システムの導入

（ア） 開発環境と運用環境の分離及び移行手順の明確化

① 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。

② 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。

③ 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。

④ 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

① 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。

② 情報システム管理者は、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。

③ 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。

④ 情報システム管理者は、開発したシステムについて、受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。

⑤ 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。

エ システム開発・保守に関連する資料等の整備・保管

（ア）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）情報システム管理者は、テスト結果を一定期間保管しなければならない。

（ウ）情報システム管理者は、情報システムに係るソースコードならびに使用したオープンソースのバージョン等を適切な方法で保管しなければならない。

オ 情報システムにおける入出力データの正確性の確保

（ア） 情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

（イ） 情報システム管理者は、故意又は過失により情報が改ざんされる、又は漏えいするおそれがある場合は、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

（ウ） 情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

カ 情報システムの変更管理

情報システム管理者は、情報システムを変更した場合は、プログラム仕様書等の変更履歴を作成しなければならない。

キ 開発・保守用のソフトウェアの更新等

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。

ク システム更新・統合時の検証等

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。

（９）不正プログラム対策

ア CIOの措置事項

CIO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の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止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パソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
（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） 校務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

イ 情報システム管理者の措置事項

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

（ア） 所掌するサーバ及びパソコン等の端末を守るため、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は、コンピュータウイルス等の感染を防止するため、学校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。

ウ 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） 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。
（イ） 外部からデータ又はソフトウェアを取り入れる場合は、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） CIO 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又は感染が疑われる場合は、以下の対応を行わなければならない。

① パソコン等の端末の場合

有線 LAN 接続の場合は、LAN ケーブルの即時取り外し、無線 LAN 接続の場合は、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。

② モバイル端末の場合

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。

エ 専門家の支援体制

CIO 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、外部の専門家の支援を受けられるようにしておかなければならない。

(10) 不正アクセス対策

ア CIO の措置事項

CIO 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及び SSID(アクセスポイントの識別名)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) 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、データの書換えを検出し、CIO 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。

(エ) 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。

(オ) CIO 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。

イ 攻撃の予告

CISO 及び CIO は、サーバ等に攻撃を受けることが明確になった場合は、システムの停止を含む必要な措置を講じなければならない。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。

ウ 記録の保存

CISO 及び CIO 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。

エ 内部からの攻撃

CIO 及び情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の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。

オ 教職員等による不正アクセス

CIO 及び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 CIO に通知し、適切な措置を求めなければならない。

カ サービス不能攻撃

CIO 及び情報システム管理者は、外部からアクセスできる教育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。

キ 標的型攻撃

CIO 及び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、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、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。

(11) セキュリティ情報の収集

ア セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等

CIO 及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

イ 不正プログラム等のセキュリティ情報の収集及び周知

CIO 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。

ウ 情報セキュリティに関する情報の収集及び共有

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

８．運用

（１）情報システムの監視

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

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

ウ　CIO 及び情報システム管理者は、機密性、完全性及び可用性のそれぞれ 2Ｂ以上の情報資産を格納する校務系システムを常時監視しなければならない。

エ　CIO 及び情報システム管理者は、機密性、完全性及び可用性のそれぞれ 2Ａの情報資産を格納する学習系システムを常時監視しなければならない。

（２）教育情報セキュリティポリシーの遵守状況の確認

ア 遵守状況の確認及び対処

（ア）　学校 CIO 及び情報セキュリティ管理者は、教育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、問題を認めた場合は、速やかに CISO 及び CIO に報告しなければならない。

（イ）　CISO 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）　CIO 及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における教育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は、適切かつ速やかに対処しなければならない。

イ パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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、教職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

ウ 教職員等の報告義務

（ア）　教職員等は、教育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 CIO 及び学校 CIO 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 CIO 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

ア 緊急時対応計画の策定

CISO 又は委員会は、情報セキュリティインシデント、教育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、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

イ 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、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

ウ 校務継続計画との整合性確保

CISO 又は委員会は、自然災害及び大規模かつ広範囲にわたる疾病等に備え、教育情報セキュリティポリシーとの整合性を確保した上で、別途校務継続計画を策定しなければならない。

エ 緊急時対応計画の見直し

CISO 又は委員会は、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。

（４）例外措置

ア 例外措置の許可

学校 CIO 及び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は、CISO の許可を得て、例外措置を取ることができる。

イ 緊急時の例外措置

学校 CIO 及び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。

ウ 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、定期的に申請書の実施状況を確認しなければならない。

（５）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、次の法令のほか、関係法令を遵守し、これに従わなければならない。

ア 地方公務員法（昭和２５年法律第２６１号）
イ 著作権法（昭和４５年法律第４８号）
ウ 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）
エ 個人情報の保護に関する法律（平成１５年法律第５７号）
オ 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）
カ 特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編 平成２６年特定個人情報保護委員会告示第６号）
キ サイバーセキュリティ基本法（平成２６年法律第１０４号）

（６）懲戒処分等

ア 懲戒処分

教育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。

イ 違反時の対応

教職員等の教育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は、速やかに次の措置を講じなければならない。

（ア） CIO が違反を確認した場合は、CIO、は当該教職員等が所属する学校の学校 CIO に通知し、適切な措置を求めなければならない。

（イ） 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 CIO 及び当該教職員等が所属する学校の学校 CIO に通知し、適切な

措置を求めなければならない。

（ウ）　学校 CIO の指導によっても改善されない場合は、CIO は、当該教職員等の教育ネットワーク又は教育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。その後速やかに、CIO は、教職員等の権利を停止又は剥奪した旨を CISO 及び当該教職員等が所属する学校の学校 CIO に通知しなければならない。

９．外部サービスの利用

（１）外部委託事業者の選定基準

ア　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。

イ　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、外部委託事業者を選定しなければならない。

ウ　情報システム管理者は、クラウドサービスを利用するときは、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用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ときは、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。

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　外部委託事業者の責任者、委託内容、作業者及び作業場所の特定
ウ　提供されるサービスレベルの保証
エ　外部委託事業者にアクセスを許可する情報の種類及び範囲並びにアクセス方法
オ　外部委託事業者の従業員に対する教育の実施
カ　提供された情報の目的外利用及び受託者以外の者への提供の禁止
キ　業務上知り得た情報の守秘義務
ク　再委託に関する制限事項の遵守
ケ　委託業務終了時の情報資産の返還、廃棄等
コ　委託業務の定期報告及び緊急時報告の義務
サ　教育委員会による監査及び検査
シ　教育委員会による情報セキュリティインシデント発生時の公表
ス　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

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、（２）の契約に基づき措置しなければならない。また、その内容を CIO 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。

10. 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、次の事項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。

（３）ソーシャルメディアサービスの利用

ア　情報セキュリティ管理者は、教育委員会事務局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は、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）　教育委員会事務局のアカウントによる情報発信が、実際に事務局のものであることを明らかにするため、事務局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成り済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　機密性２Ａ以上の情報は、ソーシャルメディアサービスで発信してはならない。

ウ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

11. 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、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、事業者に必ず確認を行わなければならない。

なお、次の項目については、調達時における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るものとする。

（１）個人情報の利用範囲

教育・学校の目的に必要な情報、又は児童生徒・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、児童生徒・保護者に対する広告活動等に個人情報を無断で使用をしないこと。

（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、又は児童生徒・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

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

（８）個人情報の取扱いについての情報開示

個人情報の取扱いについては、契約又はプライバシーポリシーで明確に示すこと。

（９）利用者による個人情報管理

個人情報の登録・変更・削除に関するサービスを利用者に提供すること。

（10）個人情報の適正管理

個人情報に対する不正アクセス又は個人情報の紛失・破壊・改ざん・漏えい・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・買収合併又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。

12. 一人一台端末におけるセキュリティ

学校内外における学習者用端末の安心かつ安全な利用に際し,次に掲げるセキュリティ対策を講ずるものとする。

(1) 学習用端末のセキュリティ対策

ア　学習用端末のセキュリティ対策、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)　情報システム管理者は、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したネットワーク構成を設計しなければならない。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な改修を行わなければならない。

イ　不適切なウェブページの閲覧防止　情報システム管理者は、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対策を講じなければならない。

ウ　マルウェア感染対策　情報システム管理者は、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。

エ　端末を不正利用させないための防止策　情報システム管理者は、端末のセキュリティ状態の監視に加え、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。

オ　セキュリティ設定の一元管理　情報システム管理者は、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なければならない。

カ　端末の盗難・紛失時の情報漏えい対策　情報システム管理者は、児童生徒が端末を紛失しても、遠隔操作でのロックやワイプ(データ消去)により第三者による不正操作や情報漏えいを防ぐ等の安全管理措置を講じなければならない。

キ　運用・連絡体制の整備　情報セキュリティ責任者は、学校内外での端末の運用ルールを制定し、インシデント時の連絡先、対応方法を各学校にて整理しなければならない。

(2) 児童生徒の ID 及びパスワード等の管理

ア　入学及び転入時の ID 登録処理

(ア)　ID は、シンプル・ユニーク(唯一無二)・パーマネント(永続的な識別)な構成要素であることや、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高めるなど適切な措置を講じなければならない。

(イ)　ID 登録やパスワードポリシーは、情報セキュリティ対策として重要な要素であるため、教育委員会で一元的に管理するものとする。

イ　進級及び進学時の ID 関連情報の更新 ID は、進学時に変更し、進級時には属性情報(進級時の組・出席番号など)の更新を行うものとする。

ウ　転出及び卒業等の ID 削除処理 転出及び卒業等した場合は,あらかじめ児童生徒本人によるデータ移行を一定期間設け実施し、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１年以内にしなければならない。ただし、本人同意や個人情報の保護に関する法律に従った適切な管理の下、一部のデータを活用できるものとする。

エ　学習用ツールへのシングルサインオン 学習用ツールの運用効率化や運用負荷の最小化を図ることが適切と判断されたサービスにおいて、シングルサインオンを導入できるものとする。

13. 点検・評価及び見直し

（１）監査

ア 実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、教育ネットワーク及び教育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、毎年度及び必要に応じて監査を行わせなければならない。

イ 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者でなければならない。

ウ 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、監査を行うに当たって、監査実施計画を立案し、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。

エ 外部委託事業者に対する監査

情報セキュリティ監査統括責任者は、外部委託事業者に委託しているときは、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、教育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。

オ 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、委員会に報告する。

カ 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適切に保管しなければならない。

キ 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情報セキュリティ管理者又は学校 CIO 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又は学校 CIO 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。

ク 教育情報セキュリティポリシー及び関係規程等の見直し等への活用

委員会は、監査結果を教育情報セキュリティポリシー及び関係規程等の見直し、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

ア 実施方法

（ア）　CISO 及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度又は必要に応じて自己点検を実施しなければならない。

（イ）　情報セキュリティ責任者は、情報セキュリティ管理者と連携し、所管す

る市内小中学校における教育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、定期的又は必要に応じて自己点検を行わなければならない。

イ 報告

CIO、情報システム管理者及び学校CIOは、自己点検結果と同結果に基づく改善策を取りまとめ、委員会に報告しなければならない。

ウ 自己点検結果の活用

（ア） 教職員等は、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。

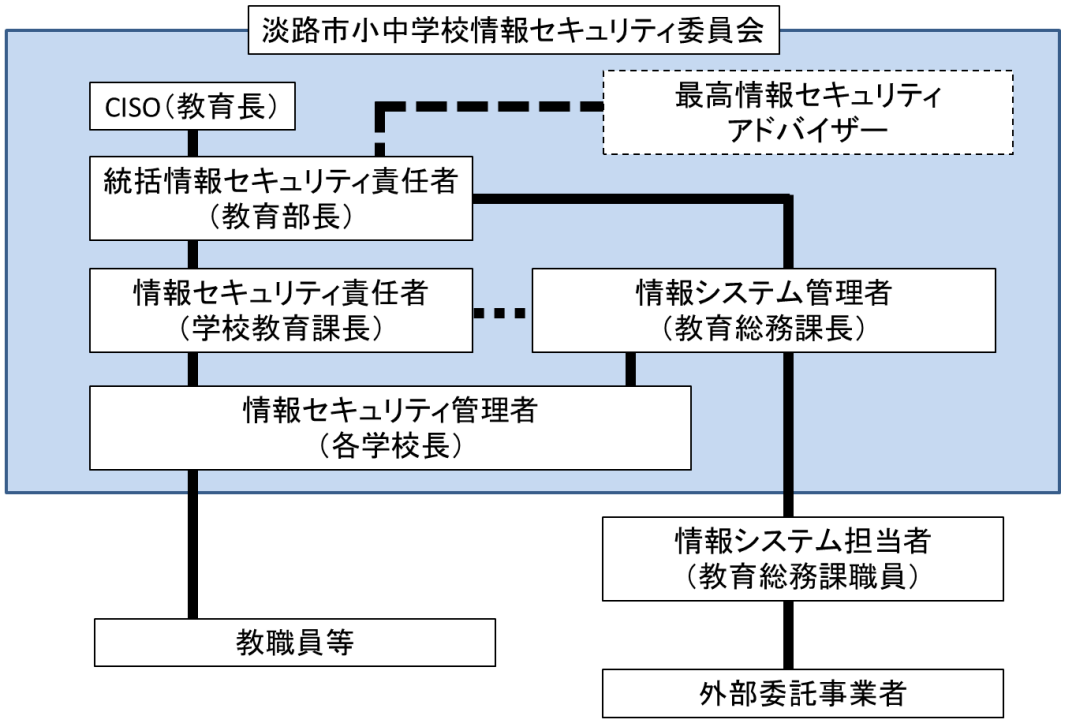
（イ） 委員会は、この点検結果を教育情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（３）セキュリティ対策の見直し・変更

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踏まえ、教育情報セキュリティポリシー及び関係規程等について定期的及び重大な変化が発生した場合に評価を行い、必要があると認めるときは、必要な改善を行うものとする。

（別紙）

淡路市小中学校情報セキュリティ推進組織体制



（別表）情報資産の管理方法及び具体的な内容

重要性	管理方法	校務情報の具体的内容
機密性３	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配布の禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管	生徒等の障がいの状況、事件・事故、指導記録、保護者の収入等の情報等、プライバシー性が高い情報並びに指導要録や成績一覧表等、児童・生徒の情報が高度に集積している帳票や電子データ等 ＜学籍関係＞ 〇指導要録（学籍に関する記録） その写し及び抄本 〇出席簿 〇卒業証書授与台帳 〇転退学受付（整理）簿 〇転入学受付（整理）簿 〇就学児童・生徒異動報告書 〇休学・退学願等受付（整理）簿 〇教科用図書給付児童・生徒名簿 〇要・準要保護児童・生徒認定台帳 〇その他校内就学援助関係書類 ＜成績関係＞ 〇指導要録（指導に関する記録） その写し及び抄本 〇評定一覧表 〇進級・卒業判定会議録・会議資料 〇定期考査素点表 〇成績に関する個票等 ＜生徒指導関係＞ 〇事故報告書・記録簿 〇生徒指導・特別指導等記録簿 〇児童・生徒等の個人写真
機密性３		＜進路関係＞ 〇卒業生進路先一覧等 〇進路希望調査 〇進路指導記録簿 〇入学者選抜に関する表簿 （願書等） ＜教務関係＞ 〇入試関連資料 （合否判定資料等を含む。） ＜健康関係＞ 〇健康診断に関する表簿・歯の検査表 （校医の押印に限り、許可により持ち出し可能とする。） 〇心臓管理等医療情報 〇保健日誌 ＜事務関係＞ 〇住民票・戸籍謄本・抄本など 〇監査調書

		○叙位・叙勲書類 ○卒業生台帳 ○授業料関連書類 ○給与関係書類 ○手当関係書類 （※教育委員会へ提出するものは、例外扱いとする。）
機密性2 完全性2 可用性2	・バックアップ ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管	個別的な情報で、随時・継続的に作成し、蓄積が必要な帳票や電子データ等 ＜学校運営＞ ○不審者対策等マニュアル（2B） ＜学級経営＞ ○学級費会計簿（2B） ＜成績関係＞ ○通知表（2A以上） ○定期考査答案用紙（2A以上） ○児童・生徒作品・作文・レポート等（2A以上） ※校長が一括して、持出許可を行うことができる。管理には要注意。 ＜生徒指導関係＞ ○生徒個人調査票（2B） ○指導カード（児童・生徒等理解カード）（2B） ○教育相談・面接の記録・カード等（2B） ○個別の教育支援計画（2B） ○個別の指導計画（2B） ○自転車等通学生一覧表（2A以上） ＜進路関係＞ ○調査書（2B） ○推薦書（2B） ○受験報告書（2A以上） ＜健康関係＞ ○児童・生徒等健康調査票（2A以上） ○健康保険証の写（2A以上） ＜教科指導関係＞ ○教務手帳（2B） ○週ごとの指導計画（個人情報が含まれるもの）（2B） ＜その他＞ ○児童・生徒等名簿（2A以上） ○住所録（2B）

機密性2 完全性2 可用性2		○緊急連絡先・学級の緊急連絡網（2B） ※校長が行事等で必要な場合には、全学年一括して許可を行うことができる。管理には要注意。 ○職員会議資料（個人情報を含むもの）（2B） ＜事務関係＞ ○各種証明書関係書類（2A 以上） ○収入調定書（2B） ○旅行関係書類（2B） ○運転免許・教員免許状等の写し（2B） ○各種点検報告書（2B） ＜人事管理関係＞ ○休暇欠勤簿等の服務管理関連書類（保護者や地域住民に学校を紹介するために作成された情報資産）（2B） ＜学校運営＞ ○学校要覧（2A 以上） ○PTA 資料（2A 以上） ○ホームページのバックアップデータ（2B） ＜指導関係＞ ○生徒指導計画や生徒指導のしおり等（2A 以上） ＜進路関係＞ ○進路のしおり等（2A 以上） ＜教務関係＞ ○考査問題（2A 以上） ※考査前の考査問題は、担当者が厳重に管理すること。 ＜その他＞ ○学校行事のしおり（2A 以上）（修学旅行・キャンプ・合宿等） ○卒業アルバム・集合写真等（2A 以上）

機密性1 完全性1 可用性1		学校外においても一定程度存在する情報 ＜教材等＞ ○授業用教材 ○教材研究資料 ○宿題プリント ※解答後の取扱いは、重要度2と同様。 ＜その他＞ ○学校紹介パンフレット ○求人一覧