# 吹田市教育情報セキュリティポリシー

平成３０年１月３１日制定
平成３０年４月　１日改定

この情報セキュリティポリシー（以下「セキュリティポリシー」という。）は、吹田市電子計算組織の管理運営に関する規程（平成 13 年吹田市訓令第 14 号）第 4 条に基づき、情報セキュリティ対策について総合的かつ具体的に取りまとめたものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

# Ⅰ　情報セキュリティ基本方針

## 1　目的

本基本方針は、本市が保有する情報資産の情報セキュリティを維持するため、本市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。

## 2　定義

（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、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、ネットワーク及び電磁的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。

（4）　機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

（5）　完全性

情報資産が破壊、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。

（6）　可用性

情報資産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、情報資産にアクセスできる状態を確保することをいう。

## 3　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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、重要情報の詐取、内部不正等の意図的な要因による脅威

（2）　プログラム上の欠陥、操作、設定ミス、機器故障等の非意図的要因による脅威

（3）　地震、落雷、火災、停電等の災害によるサービス、業務停止等の脅威

## 4　対象範囲

（1）　実施機関の範囲

本基本方針が対象とする実施機関は、吹田市個人情報保護条例（平成 14 年条例第 7 号）第 2 条第 1 項第 4 号に規定する実施機関とする。

（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
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

5　職員等の順守義務

吹田市職員、常勤嘱託員、非常勤職員及び臨時雇用員（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セキュリティポリシー、情報セキュリティに関連する規定等を順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、次の情報セキュリティ対策を実施する。

（1）　組織体制

情報セキュリティ対策を強力に推進するため、その責任及び権限を明確にした全庁的な管理体制を確立するものとする。

（2）　情報資産の分類と管理

本市の保有する情報資産を機密性、完全性、可用性の３つの側面から分析し、重要性に応じた分類に基づき情報セキュリティ対策を実施する。

（3）　物理的なセキュリティ対策

情報処理機器、通信回線及びそれらを設置している施設等の管理について、物理的な対策を実施する。

（4）　人的なセキュリティ対策

情報セキュリティに関する権限及び責任を明確にし、職員等が順守すべき事項を定めるとともに、セキュリティポリシーの意義を全ての職員等が理解できるように教育及び啓発に努める。

（5）　技術的なセキュリティ対策

ネットワーク管理、外部及び内部からのアクセス制御、ウイルス対策等の技術面での対策を実施する。

（6）　運用面におけるセキュリティ対策

情報システムの監視、セキュリティポリシーの順守状況の確認、外部委託を行う際のセキュリティ確保等、セキュリティポリシーの運用面の対策を実施する。また、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。

7　情報セキュリティ監査及び自己点検の実施

セキュリティポリシーの順守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8　評価及び見直し

情報セキュリティ監査及び自己点検による評価の結果、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、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

上記６、７及び８に規定する対策等を実施するために、具体的な順守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

なお、情報セキュリティ対策基準は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから、原則として非公開とする。

10　情報セキュリティ実施手順

セキュリティポリシーに基づき情報セキュリティ対策を実施するため、具体的な順守事項を明記した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。

なお、実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから、原則として非公開とする。

## Ⅱ 情報セキュリティ対策基準

### 1　対象範囲及び用語説明

（1）実施機関の範囲

本対策基準が対象とする実施機関は、市長及び教育委員会とする。

（2）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

ア　教育ネットワーク、教育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　教育ネットワーク及び教育情報システムで取り扱う情報（以下「情報」という。）

ウ　教育情報システムの仕様書、ネットワーク図等のシステム関連文書

（3）実施機関の範囲の例外

実施機関の範囲外であっても、本対策基準の対象となる情報システムを利用する場合にあっては、本対策基準の対象範囲とする。

（4）用語説明

本対策基準における用語は、以下のとおりとする。

| 用語 | 定義 |
|---|---|
| 校務系情報 | 児童･生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教職員の個人情報など、学校等が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導、進路指導等に活用することを想定しており、かつ、当該情報に児童・生徒がアクセスすることが想定されていない情報 |
| 学習系情報 | 学校等が保有する情報資産のうち、保護者メールやホームページ等インターネット接続を前提とした情報、及び児童・生徒のワークシート、作品など、学校等が保有する情報資産のうち、学校における授業などにおいて活用することを想定しており、かつ当該情報に教職員及び児童・生徒がアクセスすることが想定されている情報 |
| 校務系システム | 校務系ネットワーク、校務系サーバ、校務系サーバと通信を行っている端末及びソフトウェアで構成される校務系情報を取り扱うシステム |
| 学習系システム | 学習系ネットワーク、学習系サーバ、学習系サーバと通信を行っている端末及びソフトウェアで構成される学習系情報を取り扱うシステム |
| 教育情報システム | 校務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 |
| 学習系サーバ | 学習系情報を取り扱うサーバ |

### 2　組織

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

ア　市長が指定する副市長を、CISO とする。CISO は、本市における全ての教育ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

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した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

（2）統括教育情報セキュリティ責任者

ア　教育長を、CISO 直属の統括教育情報セキュリティ責任者とする。統括教育情報セキュリティ責任者は CISO を補佐するものとする。

イ　統括教育情報セキュリティ責任者は、本市の全ての教育ネットワーク、教育情報システム等における開発、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　統括教育情報セキュリティ責任者は、本市の全ての教育ネットワーク、教育情報システム等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。

（3）教育情報責任者

ア　教育監を教育情報責任者とする。

イ　教育情報責任者は、本市の教育情報セキュリティ対策に関する統括的な権限及び責任を有する。

ウ　教育情報責任者は、本市において所有している教育情報システムにおける開発、設定の変更、運用、見直し等を行う際の情報セキュリティに関する統括的な権限及び責任を有する。

エ　教育情報責任者は、本市において所有している教育情報システムについて、セキュリティポリシーの順守に関する意見の集約並びに教職員及び臨時的任用教職員（以下「教職員等」という。）に対する教育、訓練、助言及び指示を行う。

オ　教育情報責任者は、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 及び統括教育情報セキュリティ責任者の指示に従い、両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。

カ　教育情報責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括教育情報セキュリティ責任者、教育情報責任者、統括教育情報セキュリティ管理者、統括教育情報システム管理者、教育情報管理者、教育情報システム管理者、教育情報システム担当者及び教育情報学校等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。

キ　教育情報責任者は、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。

（4）統括教育情報セキュリティ管理者

ア　学校教育部指導室長を統括教育情報セキュリティ管理者とする。

イ　統括教育情報セキュリティ管理者は、教育情報管理者に対して、情報セキュリ

ティに関する指導及び助言を行う権限を有する。

（5）統括教育情報システム管理者

ア　学校教育部教育センター所長を統括教育情報システム管理者とする。

イ　統括教育情報システム管理者は、教育情報システム管理者、教育情報システム担当者及び教育情報学校等担当者に対して、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。

ウ　統括教育情報システム管理者は、本市の共通的な教育ネットワーク、教育情報システム等に関する実施手順の維持及び管理を行う権限及び責任を有する。

（6）教育情報管理者

ア　学校・園、室課（以下「学校等」という。）の長を、教育情報管理者とする。

イ　教育情報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。

ウ　教育情報管理者は、当該学校等において、セキュリティポリシーの順守に関する教職員等に対する教育、訓練、助言及び指示を行う。

エ　教育情報管理者は、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、CISO、統括教育情報セキュリティ責任者、教育情報責任者及び統括教育情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

（7）教育情報システム管理者

ア　教育委員会の情報システム担当室課の長を、教育情報システムに関する教育情報システム管理者とする。

イ　教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ　教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。

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

（8）教育情報システム担当者

ア　教育情報システム管理者が指定する職員を、教育情報システム担当者とする。

イ　教育情報システム担当者は、教育情報システム管理者の指示等に従い、教育情報システムの開発、設定の変更、運用、更新、システム利用のための申請手続き等の作業を行う。

（9）教育情報学校等担当者

ア　教育情報管理者が指定する教職員等を、教育情報学校等担当者とする。

イ　教育情報学校等担当者は、教育情報システム管理者の指示等に従い、当該学校等における教育情報システムの導入、管理、運用、システム利用のための申請手続き等の作業を行う。

（10）PMO

本市の情報セキュリティ対策を統一的に実施するため、吹田市情報化推進本部設置要領（平成 17 年 4 月 1 日制定）第 6 条に定める PMO において、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。

3　情報資産の分類及び管理

（1）情報資産の分類

情報資産を機密性、完全性、可用性の３つの側面から分析し、重要性に応じ次のとおり分類する。

| 重要性区分 | 内容 | 例 |
|---|---|---|
| Ⅰ | セキュリティ侵害が、教職員又は児童・生徒の生命、財産、プライバシー等へ重大な影響を及ぼす情報資産 | ・児童･生徒の重要な情報が一元的に収められている情報<br>・情報が正確・完全な状態である必要があり、かつ、特定の教職員のみが知り得る状態を確保する必要のある情報で機密性を要する情報 |
| Ⅱ | セキュリティ侵害が、学校等の事務及び教育活動の実施に重大な影響を及ぼす情報資産 | ・情報が正確・完全な状態である必要があり、秘密文書に相当する機密性は要しないが、教職員のみが知り得る状態を確保する必要がある情報 |
| Ⅲ | セキュリティ侵害が、学校等の事務及び教育活動の実施に軽微な影響を及ぼす情報資産 | ・児童・生徒がアクセスすることを想定している情報<br>・教職員及び児童･生徒が学習活動で使用する情報のうち、重要性区分Ⅰ又はⅡに分類されない情報 |
| Ⅳ | 上記以外の情報資産 | ・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 |

（2）情報資産の管理方法

ア　管理責任

（ア）教育情報管理者は、その所管する情報資産について管理責任を有する。

（イ）教育情報管理者は、その所管する情報資産について（1）の分類に応じた取扱制限を定めなければならない。

（ウ）情報資産が複製された場合には、複製された情報資産も（1）の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

教職員等は、情報資産について、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、文書の隅等に、情報資産の重要性区分を表示し、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

（ア）教職員等は、業務上必要のない情報を作成してはならない。
（イ）情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の重要性区分とアクセス権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　情報資産の入手

（ア）教職員等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重要性区分に基づいた取り扱いをしなければならない。
（イ）教職員等でない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、当該情報資産の重要性区分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重要性区分が不明な場合、教育情報管理者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、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、情報資産の重要性区分に応じ、適切な取り扱いをしなければならない。
（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の重要性区分が異なる情報が複数記録されている場合、記録されている情報のうち重要性区分が最も高いものの分類に従って、当該電磁的記録媒体を取り扱わなければならない。

カ　情報資産の保管

（ア）教育情報管理者又は教育情報システム管理者は、情報資産の重要性区分に従って、情報資産を適切に保管しなければならない。
（イ）教育情報管理者又は教育情報システム管理者は、情報を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を実施しなければならない。
（ウ）教育情報管理者又は教育情報システム管理者は、重要性区分Ⅰ又はⅡの情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を施し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

重要性区分Ⅰ又はⅡの情報を外部へ送信する場合は、重要性区分Ⅰの情報については教育情報責任者、重要性区分Ⅱの情報については教育情報管理者の許可を得た上で、暗号化又はパスワード設定を行わなければならない。

ク　情報資産の運搬

（ア）車両等により重要性区分Ⅰ又はⅡ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実施しなければならない。
（イ）重要性区分Ⅰ又はⅡの情報資産（複製を含む。）の保管場所からの移動及び庁舎外又は学校・園外への持出し業務が必要となったときは、移動については

教育情報管理者、持出しについては法令等の定めがある場合を除き、教育情報責任者の許可を得なければならない。

ケ　情報資産の提供・公表

（ア）重要性区分Ⅰ又はⅡ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。

（イ）重要性区分Ⅰ又はⅡの情報資産を外部に提供する者は、教育情報管理者に許可を得なければならない。

（ウ）教育情報管理者及び教育情報システム管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

コ　情報資産の廃棄

（ア）重要性区分Ⅰ又はⅡの情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体を初期化し、乱数を書込む等適切な措置を施した上で廃棄しなければならない。

（イ）重要性区分Ⅰ又はⅡの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）重要性区分Ⅰ又はⅡの情報資産の廃棄を行う者は、教育情報管理者の許可を得なければならない。

4　物理的なセキュリティ対策

（1）サーバ等の管理

ア　機器の取付け

教育情報システム管理者は、サーバの設置に際しては、温度、湿度等の環境条件を十分留意した場所に設置するものとし、サーバラックへの固定等、地震にも耐えられるような対策を実施しなければならない。また、盗難防止のワイヤーを設置する等、盗難防止対策を実施しなければならない。

イ　サーバの冗長化

（ア）教育情報システム管理者は、校務系サーバその他の校務系情報を格納しているサーバについては、必要に応じデータを二重化する等障害時に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）教育情報システム管理者は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを必要に応じ冗長化しなければならない。

ウ　機器の電源

（ア）教育情報システム管理者は、統括教育情報システム管理者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適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）教育情報システム管理者は、統括教育情報システム管理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

置を実施しなければならない。

エ　通信ケーブル等の配線

（ア）統括教育情報システム管理者及び教育情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等、必要な措置を実施しなければならない。

（イ）統括教育情報システム管理者及び教育情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

（ウ）統括教育情報システム管理者及び教育情報システム管理者は、ネットワーク接続口（ハブのポート等）を教職員等でない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）統括教育情報システム管理者及び教育情報システム管理者は、自ら又は教育情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、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）教育情報システム管理者は重要性区分Ⅰ又はⅡ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）教育情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、設置場所で行わせなければならない。設置場所から持ち出す場合、教育情報システム管理者は、外部の事業者に故障を修理させるに当たり、当該事業者との間で、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。

カ　庁舎外又は学校・園外への機器の設置

統括教育情報システム管理者及び教育情報システム管理者は、庁舎外又は学校・園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。

キ　機器の廃棄等

教育情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を実施しなければならない。

（２）管理区域（サーバ室等）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、当該機器等の管理並びに運用を行うための部屋（以下「サーバ室」という。）や電磁的記録媒体の保管庫が設定された部屋をいう。

（イ）統括教育情報システム管理者及び教育情報システム管理者は、管理区域を原則として地階又は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

きないようにしなければならない。

（ウ）統括教育情報システム管理者及び教育情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、電子錠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）統括教育情報システム管理者及び教育情報システム管理者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を実施しなければならない。

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

イ　管理区域の入退室管理等

（ア）教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、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）職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

（ウ）教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、名札の着用等を求め、必要に応じて立入区域を制限した上で、管理区域への入退室を許可された吹田市職員を付き添わせなければならない。

（エ）教育情報システム管理者は、重要性区分Ⅰ又はⅡの情報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、電磁的記録媒体等の持ち込みを管理しなければならない。

ウ　機器等の搬入出

教育情報システム管理者は、管理区域内で機器等を搬入出する場合は、その安全性について確認し、吹田市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　統括教育情報システム管理者は、庁舎内又は学校・園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。

イ　統括教育情報システム管理者は、外部へのネットワーク接続を必要最小限に限定し、できる限り接続ポイントを減らさなければならない。

ウ　統括教育情報システム管理者は、重要性区分Ⅰ又はⅡの情報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、送受信される情報の暗号化を行わなければならない。

エ　統括教育情報システム管理者は、通信回線について、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　統括教育情報システム管理者は、重要性区分Ⅰ又はⅡの情報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実施しなければならない。

（4）パソコン等の管理

ア　教育情報管理者は、盗難防止のため、職員室及びパソコン教室等で利用する端末の保管庫による管理又はワイヤーによる固定、モバイル端末の使用時以外の施錠管理等、使用する目的に応じた適切な物理的措置を実施しなければならない。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　教育情報システム管理者は、情報システムへのログイン時に認証情報の入力を必要とするように設定しなければならない。

ウ　教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の二要素認証を併用しなければならない。

5　人的なセキュリティ対策

（1）教職員等の順守事項

ア　教職員等の順守事項

（ア）セキュリティポリシー等の順守

教職員等は、セキュリティポリシー及び実施手順を順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、順守することが困難な点等がある場合は、速やかに教育情報管理者に相談し、指示を仰がなければならない。

（イ）業務以外の目的での使用の禁止

a　教職員等は、業務以外の目的で情報資産の使用、情報システムへのアクセス、電子メール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。

b　統括教育情報システム管理者は、電子メール又はインターネットへのアクセスに関するログを保存し、異常がないか定期的に確認しなければならない。

c　統括教育情報システム管理者は、情報システム等の業務以外の目的での使用を発見したときは、直ちに教育情報管理者に通知し、適切な措置を求めなければならない。この場合において、改善されないときは、アクセス権を停止することができる。

（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

a　CISO は、重要性区分Ⅰ又はⅡ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。

b　教職員等は、学校等のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報管理者の許可を得なければな

らない。

c　外部における情報処理作業の制限

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

（エ）支給以外のパソコン、モバイル端末、電磁的記録媒体等の業務利用

a　教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報管理者の許可を得て利用することができる。

b　教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、教育情報管理者の許可を得た上で、外部で情報処理作業を行う際の安全管理措置を順守しなければならない。

（オ）持ち出し及び持ち込みの記録

教育情報管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

（カ）パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を教育情報システム管理者の許可なく変更してはならない。

（キ）机上の端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体、情報が印刷された文書等について、第三者に使用されること又は教育情報管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の機密性の高い場所への保管等、適切な措置を実施しなければならない。

（ク）退職時等の順守事項

教職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、業務を離れた後も、業務上知り得た情報を漏らしてはならない。

イ　非常勤及び臨時の教職員への対応

（ア）セキュリティポリシー等の順守

教育情報管理者は、非常勤及び臨時の教職員（以下「臨時的任用職員」という。）に対し、着任時にセキュリティポリシー等のうち、臨時的任用職員が守るべき内容を理解させ、また、実施及び順守させなければならない。

（イ）パソコンやモバイル端末の利用制限

教育情報管理者は、臨時的任用職員にパソコンやモバイル端末による作業を行わせる場合は、統括教育情報システム管理者に申請しなければならない。

ウ　セキュリティポリシー等の管理

教育情報管理者は、教職員等が常に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しなければならない。

（２）情報セキュリティに関する研修及び訓練

CISO は、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。また、全ての教職員等は、定められた研修及び訓練に参加しなければならない。

ア　研修計画の策定及び実施

（ア）CISO 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を策定しなければならない。

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

（ウ）研修計画において、新規採用の教職員等を対象とする情報セキュリティに関する研修を実施するようにしなければならない。

（エ）CISO は、毎年度１回、教職員等の情報セキュリティ研修の実施状況について確認しなければならない。

イ　緊急時対応訓練

CISO 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。

（３）情報セキュリティインシデントの報告

ア　学校等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、速やかに教育情報管理者に報告しなければならない。

（イ）報告を受けた教育情報管理者は、速やかに統括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。また、必要に応じて CISO、統括教育情報セキュリティ責任者、教育情報責任者及び統括教育情報システム管理者にも報告しなければならない。

イ　住民等外部からの情報セキュリティインシデントの報告

（ア）教職員等は、全ての教育ネットワーク、教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、速やかに教育情報管理者に報告しなければならない。

（イ）報告を受けた教育情報管理者は、速やかに統括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。また、必要に応じて CISO、統括教育情報セキュリティ責任者、教育情報責任者及び統括教育情報システム管理者にも報告しなければならない。

（ウ）CISO は、教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

ウ　情報セキュリティインシデント原因の究明、記録、再発防止等

（ア）教育情報責任者は、情報セキュリティインシデントについて、教育情報管理

者、統括教育情報セキュリティ管理者及び教育情報システム管理者と連携し、これらの情報セキュリティインシデントの原因を究明し、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結果から、再発防止策を検討し、必要に応じて CISO 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）CISO 及び統括教育情報セキュリティ責任者 は、教育情報責任者から、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。

（4）ID 及びパスワード等の管理

ア　IC カード等の取り扱い

教職員等は、認証に用いるカード類を厳格に管理しなければならない。紛失したときは、速やかに教育情報管理者及び教育情報システム管理者に報告しなければならない。

イ　ID の取り扱い

（ア）教職員等は、自己の管理する ID を、他者に利用させてはならない。

（イ）教職員等は、複数の利用者が共通で利用できる ID（以下、「共通 ID」という。）を利用する場合は、共通 ID の利用許可者以外に利用させてはならない。

ウ　パスワードの取り扱い

教職員等は、自己の管理するパスワードに関し、次の事項を順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、教育情報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）パスワードは定期的に変更し、古いパスワードを再利用してはならない。

（カ）複数の教育情報システムを扱う教職員等は、同一のパスワードを異なるシステム間で用いてはならない。

（キ）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。

（ク）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。

（ケ）教職員等間でパスワードを共有してはならない。

6　技術的なセキュリティ対策

（1）コンピュータ及びネットワークの管理

ア　共有フォルダの設定等

（ア）教育情報システム管理者は、教職員等が使用できる共有フォルダの容量を設定し、教職員等に周知しなければならない。

（イ）教育情報システム管理者は、共有フォルダを原則として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）教育情報システム管理者は、住民の個人情報、人事記録等、特定の教職員等しか取り扱えないデータについて、別途フォルダを作成する等の措置を実施し、同一学校等であっても、担当者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。

（エ）その他共有フォルダに関する事項は、実施手順に定める。

イ　バックアップの実施

教育情報システム管理者は、サーバ等に記録された情報について、サーバの冗長化対策に関わらず、定期的にバックアップを実施しなければならない。

ウ　他団体との情報システムに関する情報等の交換

教育情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取り扱いに関する事項をあらかじめ定め、教育情報責任者の許可を得なければならない。また、統括教育情報セキュリティ責任者にその旨を報告しなければならない。

エ　システム管理記録及び作業の確認

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

（イ）教育情報システム管理者は、所管する情報システムの変更等に関する処理について、その記録を適切に管理しなければならない。

（ウ）教育情報システム管理者、教育情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、2 名以上で作業する等、作業ミスをしないように努めなければならない。

オ　情報システム仕様書等の管理

教育情報システム管理者は、ネットワーク構成図及び情報システム仕様書について、記録媒体の種類に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

カ　ログの取得等

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

（イ）教育情報システム管理者は、ログとして取得する項目、保存期間、取扱方法等について定め、消去又は改ざんされることがないように適切にログを管理しなければならない。

（ウ）教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

キ　障害記録

教育情報システム管理者は、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、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）教育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、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）教育情報システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

ケ　外部ネットワークとの接続制限等

（ア）教育情報システム管理者は、所管するネットワーク及びシステムを外部ネットワークと接続しようとする場合には、CISO の許可を得なければならない。

（イ）教育情報システム管理者は、接続しようとする外部ネットワークに関す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・園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）教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理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）教育情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、教育ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

（オ）教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括教育情報システム管理者の判断に従い、速やかに当該外部ネットワークを遮断しなければならない。

コ　ネットワークの分離

（ア）統括教育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を物理的又は論理的に分離し、それぞれで適切な安全管理措置を講じなければならない。

（イ）統括教育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間で通信する場合には、ウイルス感染の防止などの適切な措置を図らなければならない。

サ　ネットワークに接続するその他機器

（ア）教育情報システム管理者は、複合機、プリンタ、ファクシミリ、テレビ会議システム、ネットワークカメラシステム等（以下「複合機等」という。）を調達する場合、当該複合機等が備える機能、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対策を実施しなければなければ

ならない。

（イ）教育情報システム管理者は、複合機等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等に対する情報セキュリティインシデントへの対策を実施しなければならない。

（ウ）教育情報システム管理者は、複合機等の運用を終了する場合、複合機等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実施しなければならない。

（エ）教育情報システム管理者は、複合機等について、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。

シ　無線 LAN 及びネットワークの盗聴対策

（ア）教育情報システム管理者は、無線 LAN を利用する場合、解読が困難な暗号化及び認証技術を使用しなければならない。

（イ）教育情報システム管理者は、重要性区分Ⅰ又はⅡの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、必要に応じて暗号化等の措置を実施しなければならない。

ス　電子メールのセキュリティ管理

（ア）統括教育情報システム管理者は、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）が行われることのないよう、電子メールサーバの設定を行わなければならない。

（イ）統括教育情報システム管理者は、スパムメール等の受信対策を適切に実施しなければならない。また、庁内から大量のスパムメールの送信を検知した場合は、メールサーバの運用を停止する等適切に対処しなければならない。

（ウ）統括教育情報システム管理者は、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制限しなければならない。

（エ）統括教育情報システム管理者は、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について教職員等に指示しなければならない。

（オ）統括教育情報システム管理者は、システム開発や運用、保守等のため庁舎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。

（カ）統括教育情報システム管理者は、教職員等によるメールの送受信を教育情報管理者が確認できるような対策を実施しなければならない。

（キ）教育情報管理者は、情報資産の外部への送信が適切であることを確認するため、教職員等が送付するメールを管理しなければならない。

（ク）その他メールサーバの運用に関する事項は、実施手順に定める。

セ　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、教育情報管理者に報告しなければならない。
（オ）教職員等は、許可されていないメールサービス、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。

ソ　電子署名及び暗号化

（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、電子署名、暗号化、パスワード設定等の適切なセキュリティ対策を実施して送信しなければならない。
（イ）教育情報責任者は、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。

タ　無許可ソフトウェアの導入等の禁止

（ア）教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
（イ）教職員等は、業務上の必要がある場合は、教育情報管理者及び統括教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育情報管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。
（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。
（エ）統括教育情報システム管理者は、アプリケーションソフト等の端末へのインストールが許可なく行われたことを発見した場合は、そのアプリケーションソフト等の使用を停止することができる。

チ　機器構成の変更の制限

（ア）教職員等は、パソコン、モバイル端末及びネットワーク機器に対し機器の改造、増設及び交換を行ってはならない。
（イ）教職員等は、業務上、パソコン、モバイル端末及びネットワーク機器の改造、増設及び交換を行う必要がある場合には、統括教育情報システム管理者の許可を得なければならない。
（ウ）統括教育情報システム管理者は、パソコン、モバイル端末及びネットワーク機器の改造、増設及び交換が許可なく行われたことを発見したときは、その使用を停止することができる。

ツ　無許可でのネットワーク接続の禁止

（ア）教職員等は、許可なくネットワーク環境の変更を行ってはならない。業務上、ネットワーク機器の増設等の必要が生じたときは、統括教育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、統括教育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。

（ウ）統括教育情報システム管理者は、ネットワーク環境の変更やネットワーク機器の増設が許可なく行われたことを発見したときは、その使用を停止することができる。

（２）　アクセス制御

ア　アクセス制御等

（ア）アクセス制御

a　教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないようにシステム上制限しなければならない。

b　教育情報システム管理者は、所管する情報システム等を新たに接続するとき若しくは変更又は廃止するときは、統括教育情報システム管理者に申請しなければならない。

（イ）利用者 ID の取り扱い

a　教育情報管理者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、退職に伴う利用者 ID について、適切に取り扱わなければならない。

b　システムを所管する教育情報システム管理者は、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、当該教職員等が所属する学校等の教育情報管理者に通知しなければならない。

c　教育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

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

b　教育情報システム管理者の特権を代行する者は、教育情報システム管理者が指定する。

c　教育情報システム管理者は、特権を付与された ID 及びパスワードについて、一般の利用者 ID よりも定期変更、入力回数制限等のセキュリティ機能を強化するよう努めなければならない。

d　教育情報システム管理者は、特権を付与された ID を初期設定以外のものに変更するように努めなければならない。

e　教育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。

（エ）特権による接続時間の制限

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

（オ）共通 ID の管理等

a　教育情報システム管理者は、業務上利用者を区別する必要がない場合、共通 ID を登録することができる。

b　教育情報システム管理者は、共通 ID を利用する場合、利用者 ID の取り扱いに準じ、適切に取り扱わなければならない。

c　教育情報システム管理者は、共通 ID の利用は必要最小限とし、重要性区分Ⅰ又はⅡの情報資産を取り扱うシステムでは利用してはならない。

イ　教職員等による外部からのアクセス等の制限

（ア）統括教育情報システム管理者及び教育情報システム管理者は、外部から本市のネットワークにアクセスさせるときは、原則として外部に公開されているサーバに対してのみ行わせるものとし、直接内部ネットワークにアクセスすることを許可してはならない。

（イ）統括教育情報システム管理者及び教育情報システム管理者は、公衆通信回線（公衆無線 LAN 等）を教育ネットワークに接続することを許可してはならない。

（ウ）教職員等は、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。

ウ　自動識別の設定

統括教育情報システム管理者及び教育情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

エ　ログイン時の表示等

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

オ　パスワードに関する情報の管理

（ア）教育情報システム管理者は、教職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

（イ）統括教育情報システム管理者又は教育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。

（3）システム開発、導入、保守等

ア　情報システムの調達

（ア）教育情報システム管理者は、情報システム開発、導入、保守等の調達に当た

っては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

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

（ウ）教育情報システム管理者は、アプリケーションソフトの購入、バージョンアップ等に関しては、統括教育情報システム管理者の許可を得なければならない。

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

教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、プロジェクト計画書等、システム開発のための手順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

a　教育情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

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

（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

a　教育情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

b　教育情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

ウ　情報システムの導入

（ア）開発環境と運用環境の分離及び移行手順の明確化

a　教育情報システム管理者は、原則としてシステム開発、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。

b　教育情報システム管理者は、システム開発、保守及びテスト環境からシステム運用環境への移行について、システム開発及び保守に関する計画の策定時に手順を明確にしなければならない。

c　教育情報システム管理者は、移行の際、情報システムに記録されている情報の保存を確実に行い、移行に伴う情報システム運用環境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。

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

（イ）テスト

a　教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを行わなければならな

い。

b　教育情報システム管理者は、運用テストを行う場合、原則としてあらかじめテスト環境による操作確認を行わなければならない。

c　教育情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

d　教育情報システム管理者は、開発したシステムについて受入テストを行う場合、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。

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

（ウ）システム開発及び保守に関連する資料等の整備及び保管

a　教育情報システム管理者は、システム開発及び保守に関連する資料並びにシステム関連文書を適切に整備及び保管しなければならない。

b　教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

c　教育情報システム管理者は、情報システムに関するソースコードを適切な方法で保管しなければならない。

（エ）情報システムにおける入出力データの正確性の確保

a　教育情報システム管理者は、情報システムに入力されるデータについて、必要に応じて範囲、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。

b　教育情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出する仕組みを構築しなければならない。

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

（オ）情報システムの変更管理

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

（カ）開発及び保守用のソフトウェアの更新等

教育情報システム管理者は、開発及び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。

（キ）システム更新時の検証等

教育情報システム管理者は、システム更新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後の業務フローの検証を行わなければならない。

（４）不正プログラム対策

ア　教育情報システム管理者の措置事項

教育情報システム管理者は、不正プログラム対策として、次のとおり取り扱わなければならない。

（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）所管するサーバ、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ソフトウェアのバージョンは、常に最新の状態に保たなければならない。

（キ）インターネットに接続していないシステムにおいても、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、本市が管理している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。

（ク）業務で利用するソフトウェアは、原則として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ものを利用してはならない。

イ　教職員等の順守事項

教職員等は、不正プログラム対策に関し、次のとおり取り扱わなければならない。

（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な添付ファイルを受信した場合は速やかに統括教育情報システム管理者に報告し、その指示に従い処理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）統括教育情報システム管理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又は感染が疑われる場合は、次の対応を行った上、統括教育情報システム管理者及び教育情報システム管理者に報告し、その指示に従わなければならない。

a　パソコン等の端末の場合

LAN ケーブルの即時取外しを行わなければならない。

b　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。

ウ　専門家の支援体制

統括教育情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（5）不正アクセス対策

ア　教育情報システム管理者の措置事項

教育情報システム管理者は、不正アクセス対策として、次のとおり取り扱わなければならない。

（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）ネットワークの基幹部分及び重要なシステムの設定に関するファイル等については、定期的に調査し、改ざんされていないかを確認しなければならない。

（エ）統括教育情報システム管理者と連携し、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 及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を実施しなければならない。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 及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

エ　内部からの攻撃

教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の端末から庁内のサーバ等又は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

システムを所管する教育情報システム管理者は、教職員等による不正アクセス

を発見した場合は、当該教職員等が所属する学校等の教育情報管理者に通知し、適切な処置を求めるとともに、統括教育情報システム管理者に報告しなければならない。

カ　サービス不能攻撃

教育情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を実施しなければならない。

キ　標的型攻撃

統括教育情報システム管理者及び教育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、教育等の人的対策や自動再生無効化等の入口対策を実施しなければならない。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実施しなければならない。

（6）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、ソフトウェアの更新等

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

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

統括教育情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、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

統括教育情報システム管理者及び教育情報システム管理者は、情報セキュリティ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実施しなければならない。

7　運用面におけるセキュリティ対策

（1）情報システムの監視

ア　教育情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを障害検知機能等により常時監視しなければならない。

イ　統括教育情報システム管理者及び教育情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を実施しなければならない。

ウ　統括教育情報システム管理者は、外部と常時接続するシステムをファイアウォ

ール、不正侵入検知装置等により、常時監視しなければならない。

（2）セキュリティポリシーの順守状況の確認

ア　順守状況の確認及び対処

（ア）教育情報管理者は、セキュリティポリシーの順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 CISO 、統括教育情報セキュリティ責任者、教育情報責任者及び統括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）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）統括教育情報システム管理者及び教育情報システム管理者は、ネットワーク、サーバ等のシステム設定等におけるセキュリティポリシーの順守状況について、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。

イ　パソコン、モバイル端末、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パソコン、モバイル端末、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、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、直ちに教育情報管理者に報告しなければならない。教育情報管理者は、必要に応じて統括教育情報セキュリティ責任者、教育情報責任者及び統括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）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、適切かつ速やかに対処しなければならない。

（3）侵害時の対応等

教育ネットワーク及び教育情報システムにおいて、セキュリティ上の重大な事故が発生し、情報資産が侵害されたときは、被害の拡大防止、迅速な復旧、証拠保全及び再発防止を図るため、次に掲げる対策を実施する。

ア　連絡及び報告

（ア）事故を発見した者は、実施手順に定める連絡系統に基づき直ちに連絡しなければならない。

（イ）事故を発見した者は、事故内容、考え得る事故原因、被害内容、被害範囲等について速やかに教育情報システム管理者に報告しなければならない。

（ウ）教育情報システム管理者は、必要に応じて統括教育情報セキュリティ責任者、教育情報責任者及び統括教育情報システム管理者に報告しなければならない。

イ　調査

統括教育情報システム管理者及び教育情報システム管理者は、報告に基づき詳

細な調査を実施し、CISO、統括教育情報セキュリティ責任者及び教育情報責任者に報告しなければならない。

ウ　対策

（ア）統括教育情報システム管理者は、次に掲げる本市の情報資産が脅威にさらされた状況が発生したときは、それらを保護するためネットワークを切断することができる。

a　ポートスキャン等の異常なアクセスが継続しているとき

b　不正アクセスが発見されたとき

c　サービス不能攻撃等によりシステムの運用に支障をきたすとき

d　コンピュータウイルス等の不正プログラムが増殖しているとき

e　その他情報資産に重大な被害を与える可能性があるとき

（イ）教育情報システム管理者は、次に掲げる状況が発生した場合は所管の教育情報システムを停止しなければならない。

a　コンピュータウイルス等の不正プログラムが増殖し、さらに被害が拡大する可能性があるとき

b　災害等により長時間の停電が発生する可能性があるとき

c　その他情報資産に重大な被害を与える可能性があるとき

（ウ）統括教育情報システム管理者及び教育情報システム管理者は、復旧に際しては証拠保全措置を施し、再発防止の暫定対策を検討し、実施しなければならない。

（エ）統括教育情報システム管理者及び教育情報システム管理者は、実施した対策等についてログも含めその記録を適切に保存しなければならない。

エ　再発防止

統括教育情報システム管理者及び教育情報システム管理者は、発生した事故についてのリスク分析を実施し、再発防止に向け関連する実施手順を改正するとともに、必要に応じてセキュリティポリシーの改正を検討の上、PMO に提案しなければならない。

（4）例外措置

ア　例外措置の許可

教育情報管理者及び教育情報システム管理者は、セキュリティポリシー及び関係規定等を順守することが困難な状況で、学校等の事務及び教育活動の適正な遂行を継続するため、順守事項とは異なる方法を採用し又は順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。

イ　緊急時の例外措置

教育情報管理者及び教育情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISO、統括教育情報セキュリティ責任者、教育情報責任者及び統括教育情報シ

ステム管理者に報告しなければならない。

ウ　例外措置の申請書の管理

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。

（5）法令順守

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、次の法令等のほか関係法令等を順守し、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　教育公務員特例法（昭和 24 年 1 月 12 日法律第 1 号）

ウ　著作権法（昭和 45 年法律第 48 号）

エ　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）

オ　個人情報の保護に関する法律（平成 15 年法律第 57 号）

カ　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）

キ　吹田市個人情報保護条例（平成 14 年条例第 7 号）

ク　吹田市個人番号の利用等に関する条例（平成 27 年条例第 24 号）

（6）違反に対する対応

教職員等の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実施しなければならない。

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、当該教職員等が所属する学校等の教育情報管理者に通知し、適切な措置を求めなければならない。

イ　システムを所管する教育情報システム管理者が違反を確認した場合は、速やかに統括教育情報セキュリティ責任者及び当該教職員等が所属する学校等の教育情報管理者に通知し、適切な措置を求めなければならない。

ウ　教育情報管理者の指導によっても改善されない場合、統括教育情報セキュリティ責任者は、当該教職員等の教育ネットワーク又は教育情報システムの使用を禁止することができる。統括教育情報セキュリティ責任者はその後速やかに、禁止した旨を CISO に報告し、当該教職員等が所属する学校等の教育情報管理者に通知しなければならない。

8　外部サービスの利用

（1）外部委託

ア　外部委託事業者の選定基準

（ア）教育情報システム管理者は、外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）教育情報システム管理者は、必要に応じて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等を参考にして、事業者を選定しなければならない。

（ウ）教育情報システム管理者は、クラウドサービスを利用する場合は、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。

イ　契約項目

情報システムの開発、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。

（ア）セキュリティポリシー及び実施手順の順守
（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順守
（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義務
（サ）市による監査及び検査
（シ）市による情報セキュリティインシデント発生時の公表
（ス）セキュリティポリシーが順守されなかった場合の規定（損害賠償等）

ウ　確認、措置等

教育情報システム管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、イの契約に基づき措置しなければならない。また、その内容を重要度に応じて CISO、統括教育情報セキュリティ責任者、教育情報責任者及び統括教育情報システム管理者に報告しなければならない。

（２）約款による外部サービスの利用

ア　約款による外部サービスの利用に関する規定の整備

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、重要性区分Ⅰの情報が取り扱われない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

イ　約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を教育

情報システム管理者に申請し、適切な措置を実施し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　教育情報システム管理者は、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）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実施すること。

（イ）パスワード等の認証情報、これを記録した媒体等を適切に管理するなどの方法で、不正アクセス対策を実施すること。

イ　重要性区分Ⅰ又はⅡ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。

9　評価及び見直し

（1）監査

ア　実施方法

PMO は、ネットワーク、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、定期的に監査を行わなければならない。また、開発又は運用等を外部事業者に委託している場合、必要に応じて外部事業者に対し監査を実施するものとする。その他監査の実施に関する事項は、実施手順に定める。

イ　セキュリティポリシー、関係規定等の見直し時の反映

PMO は、監査結果をセキュリティポリシー、関係規定等の見直し、その他情報セキュリティ対策の見直し時に反映しなければならない。

（2）自己点検

ア　実施方法

（ア）PMO は統括教育情報システム管理者及び教育情報システム管理者に、所管するネットワーク及び情報システムについて、定期的に自己点検を実施させなければならない。

（イ）PMO は統括教育情報セキュリティ管理者に、教育情報管理者と連携して、学校等における情報セキュリティ対策について、定期的に自己点検を行わせなければならない。

イ　報告

統括教育情報セキュリティ管理者、統括教育情報システム管理者、教育情報システム管理者は、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、PMO 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）PMO は、この点検結果をセキュリティポリシー、関係規定等の見直し、その他情報セキュリティ対策の見直し時に反映しなければならない。

（3）セキュリティポリシー、関係規定等の見直し

PMO は、情報セキュリティ監査及び自己点検の結果、情報セキュリティに関する状況の変化等をふまえ、セキュリティポリシー、関係規定等について重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。