交野市教育情報セキュリティ対策基準

（学校編）

令和７年４月　改訂

交野市教育委員会

目次

教育情報セキュリティ対策基準

交野市教育情報セキュリティ対策基準(学校編)とは、交野市情報セキュリティ基本要綱(基本方針)に基づき、情報セキュリティ対策等を実施するために適用範囲における共通の基準として具体的な遵守事項及び判断基準を定めたものである。

1.適用範囲

(1)適用する機関の範囲

交野市立学校に関する条例(昭和４０年３月３１日条例第７号)第１条、第２条及び第３条により設置する市立小学校、中学校及び義務教育学校(以下「学校」という。)並びに教育委員会とする。

(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。

①教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

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

③教育情報システムの仕様書及びネットワーク図等のシステム関連文書

2.組織体制

教育情報セキュリティの管理については、以下の組織、体制とする。

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

①教育長を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。

②CISO 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)教育情報セキュリティ統括責任者

①教育総務部長及び教育指導部長をCISO直属の教育情報セキュリティ統括責任者とする。教育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教育情報セキュリティ統括責任者は、本市の全ての教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③教育情報セキュリティ統括責任者は、本市の全ての教育ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④教育情報セキュリティ統括責任者は、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤教育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教育情報セキュリティ統括責任者は、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教育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、教育情報セキュリティ統括責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑧教育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)教育情報セキュリティ責任者

①教育指導部学校教育課長を教育情報セキュリティ責任者とする。

②教育情報セキュリティ責任者は、本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。

③教育情報セキュリティ責任者は、本市において所有している教育情報システムにおける情報セキュリティに関する開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④教育情報セキュリティ責任者は、本市において所有している教育情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等（校長、教員その他の学校に所属する職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

(4)教育情報セキュリティ管理者

①校長を教育情報セキュリティ管理者とする。

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

③教育情報セキュリティ管理者は、当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、教育情報セキュリティ責任者及び教育情報システム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。

(5)教育情報システム管理者

①教育総務部次長を、教育情報システムに関する教育情報システム管理者とする。

②教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。

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

(6)教育情報システム担当者

①まなび支援課・学校教育課・学校給食センターの職員のうち教育情報システムを管理、運用又は使用する職員を、教育情報システムに関する教育情報システム担当者とする。

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

(7)教育情報セキュリティ委員会

本市の教育情報セキュリティ対策を統一的に行うため、教育情報セキュリティ委員会において、教育情報セキュリティ基本要綱等、教育情報セキュリティに関する重要な事項を決定する。

(8)教育情報セキュリティに関する統一的な窓口の設置

①CISO は、教育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で整備し、教育情報セキュリティインシデントについて学校及び教育委員会に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。

②CISO に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、その内容を学校等に提供する。

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、関係機関及び報道機関への通知・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。

3. 情報資産の分類と管理方法

3.1. 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

機密性

3	学校業務で取り扱う情報資産のうち、特に機密性を要するもの (次のデータだけではなく、それらが含まれる電子記録媒体、パーソナルコンピュータ、システム等も同様) ・特定個人情報に関するデータ ・個人情報に関するデータ ・法令の規定により秘密を守る義務を課せられているデータ

	・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に学校の信頼を著しく害する可能性のあるデータ ・公開することでセキュリティ侵害が生じる可能性があるデータ
2	直ちに一般に公開することを前提としていないもの (機密性３には当てはまらないが、広報等は行っていないデータ及びそれらが含まれる電子記録媒体、パーソナルコンピュータ、システム等)
1	機密性２又は機密性３以外の情報資産

完全性

3	学校業務で取り扱う情報資産のうち、特に完全性を要するもの (次のデータだけではなく、それらが含まれる電子記録媒体、パーソナルコンピュータ、システム等も同様) ・改ざん、誤びゅう又は破損が生じると、児童、生徒、保護者及び市立学校関係者の権利が侵害される可能性があるデータ ・改ざん、誤びゅう又は破損が生じると、学校業務の適確な遂行に著しい支障を及ぼす可能性があるデータ
2	改ざん、誤びゅう又は破損が生じると学校業務の適確な遂行に支障を及ぼす可能性があるもの
1	完全性２又は完全性３以外の情報資産

可用性

3	学校業務で取り扱う情報資産のうち、特に可用性を要するもの (次のデータだけではなく、それらが含まれる電子記録媒体、パーソナルコンピュータ、システム等も同様) ・利用できないと児童、生徒、保護者及び市立学校関係者の権利が侵害される可能性があるデータ ・利用できないと学校業務の安定的な遂行に著しい支障を及ぼす可能性があるデータ
2	利用できないと学校業務の安定的な遂行に支障を及ぼす可能性があるもの
1	可用性２又は可用性３以外の情報資産

3.2. 情報資産の管理

(1)管理責任

教育情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

情報資産が複製又は伝送された場合には、複製等された情報資産も(1)の分類に基づき

管理しなければならない。

(2)情報資産の取り扱い

①情報資産の分類の表示

教職員等は、情報資産について、情報資産の分類や必要に応じて取扱制限がわかるよう適切な管理を行わなければならない。

②情報の作成

(ｱ)教職員等は、業務上必要のない情報を作成してはならない。

(ｲ)情報を作成する者は、情報の作成時に(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ)情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

③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、入手した情報資産の分類が不明な場合、教育情報セキュリティ管理者に判断を仰がなければならない。

④情報資産の利用

(ｱ)情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(ｲ)情報資産を利用する者は、情報資産の分類に応じ、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を取り扱わなければならない。

(3)情報資産の保管

(ｱ)教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

(ｲ)教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産を記録したUSBメモリ等の外部電磁的記録媒体を長期保管する場合は、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)教育情報セキュリティ管理者又は教育情報システム管理者は、情報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長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

(ｴ)教育情報セキュリティ管理者又は教育情報システム管理者は、機密性２以上、完全

性２以上又は可用性２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。

(4)情報資産の外部持ち出し

①情報資産の外部持ち出し制限

教職員等は、機密性２以上の情報資産を外部に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。

②電子メール、外部ストレージサービスによる情報の送信

(ｱ)電子メールにより機密性２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又はパスワード設定）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、教育委員会又は学校から提供される公式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。

③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、紛失・盗難リスクを伴うことから以下を遵守しなければならない。

(ｱ)管理された外部電磁的記録媒体以外の使用禁止

教育委員会又は学校から支給された公的な媒体のみを利用すること。

(ｲ)外部電磁的記録媒体の暗号化の徹底

暗号化機能つきの媒体を利用し、暗号化機能を活かすこと。

④FAX 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。

⑤情報資産の運搬

(ｱ)車両等により機密性２以上の情報資産を運搬する場合は、必要に応じ暗号化又はパスワードの設定を行う等の安全管理措置を講じなければならない。

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

⑥情報資産の公表

(ｱ)教育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)教育情報セキュリティ管理者は、住民に公開する情報資産について、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

①情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体についてその情報の機密性に応じ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。

②情報資産の廃棄やリース返却等を行う者は、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。

③情報資産の廃棄やリース返却等を行う者は、教育情報セキュリティ管理者の許可を得なければならない。

4. 物理的セキュリティ

4. 1. サーバ等の管理

(1)機器の取付け

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

(2)サーバの冗長化

①教育情報システム管理者は、校務系サーバその他の校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。なお、冗長化については、当該対策基準の策定時には、未整備のため、今後、校務支援システム等のシステム整備にあわせて検討するものとする。

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

(3)機器の電源

①教育情報システム管理者は、教育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。

②教育情報システム管理者は、教育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

①教育情報セキュリティ統括責任者及び教育情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

②教育情報セキュリティ統括責任者及び教育情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③教育情報セキュリティ統括責任者及び教育情報システム管理者は、ネットワーク接続

口(ハブのポート等)を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

④教育情報セキュリティ統括責任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又は、追加できないように必要な措置を施さなければならない。

(5)機器の定期保守及び修理

①教育情報システム管理者は、可用性２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。

②教育情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、教育情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等など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

教育情報セキュリティ統括責任者及び教育情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

(7)機器の廃棄等

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

4.2.管理区域(情報システム室等)の管理

(1)管理区域の構造等

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

②教育情報セキュリティ統括責任者及び教育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。

③教育情報セキュリティ統括責任者及び教育情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④教育情報セキュリティ統括責任者及び教育情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤教育情報セキュリティ統括責任者及び教育情報システム管理者は、施設管理部門と連携して、管理区域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。

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

(2)管理区域の入退室管理等

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

②地方公共団体職員等及び外部委託事業者が、管理区域に入室することを許可する場合、これらの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。

③教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された地方公共団体職員等が付き添うものとし、外見上地方公共団体職員等と区別できる措置を講じなければならない。

④教育情報システム管理者は、機密性２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、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。

(3)機器等の搬入出

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

②教育情報システム管理者は、情報システム室の機器等の搬入出について、地方公共団体職員を立ち会わせなければならない。

4.3.通信回線及び通信回線装置の管理

①教育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教育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を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③教育情報セキュリティ統括責任者は、機密性２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、送受信される情報の暗号化を行わなければならない。

④教育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教育情報セキュリティ統括責任者は、可用性２以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

⑥教育情報セキュリティ統括責任者は、学校運営上必要なネットワーク帯域を確保するとともに遅延等に対する適切な対策を講じなければならない。クラウドサービス提供事業者側のサービス要件基準を満たす配慮を含めてネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

4.4. 教職員等の利用する端末や電磁的記録媒体等の管理

（校務用端末、校務外部接続用端末及び指導者用端末について）

①教育情報システム管理者は、不正アクセス防止のため、ログイン時の ID パスワードによる認証、加えて多要素認証の実施等、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

②教育情報システム管理者は、校務系システム、教育情報システムへアクセスする端末へのログインパスワードの入力を必要とするように設定しなければならない。

③教育情報システム管理者は、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設定しなければならない。

④教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

⑤教育情報システム管理者は、モバイル端末の学校外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

（学習者用端末について）

⑥教育情報システム管理者は、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、OS によっては標準的にウイルス対策ソフトを備えている製品、OS としてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。強固なアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況及び通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

⑦教育情報システム管理者は、インターネットへ接続をする場合、教職員等のパソコン、

モバイル端末に対して不適切なウェブページの閲覧を防止する Web フィルタリング等の対策を講じなければならない。

4.5.学習者用端末のセキュリティ対策

(1)不適切なウェブページの閲覧防止

児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

＜対策例＞

①フィルタリングソフト

②検索エンジンのセーフサーチ

③セーフブラウジング

(2)マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

(3)端末を不正利用させないための防止策

端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

(4)セキュリティ設定の一元管理

児童生徒への端末配布後においても、端末のセキュリティ設定や OS アップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましい。

(5)端末の盗難・紛失時の情報漏洩対策

児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

5.人的セキュリティ

5.1.教育情報セキュリティ管理者の措置事項

(1)情報資産の管理

①情報資産の持ち出し及び持ち込みの記録管理

教育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。

②情報資産の廃棄管理

(ｱ)教育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会うように指示し、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)教職員等の情報セキュリティ意識醸成

①教育情報セキュリティ管理者は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

②教育情報セキュリティ管理者は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、すみやかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③教育情報セキュリティ管理者は、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・確認できるように配慮しなければならない。

(3)端末等の持ち出し及び持ち込みの記録

教育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。

(4)教職員等への情報セキュリティポリシー等の遵守指導

①教育情報セキュリティ管理者は、新規採用職員等及び他自治体から本市に新規赴任した教職員等並びに非常勤及び臨時の教職員に対し、教育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。

②教育情報セキュリティ管理者は、教職員等に対して、必要に応じて情報セキュリティポリシーの遵守の同意書への署名を求める。

(5)新規ソフトウェア及びコンテンツの導入・利用判断

教育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、教育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)インターネット接続及び電子メール利用の制限

①教育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。なお、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、教育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。

②教育情報セキュリティ管理者は、パソコンやモバイル端末の機能は、教職員等の業務内容に応じて、不必要な機能については制限することが適切である。

(7)校内及び執務室での管理

教育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。

①来校者の氏名及び入退時刻を記録しなければならない。

②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。

③地域住民、保護者などに校内施設を開放する場合は、執務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。

5.2.教職員等の遵守事項

(1)教育情報セキュリティ対策基準等の遵守

教職員等は、教育情報セキュリティ基本要綱及び情報セキュリティ実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに教育情報セキュリティ管理者に相談し、指示を仰がなければならない。

(2)執務上での管理

①執務室の施錠管理

執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

②机上の端末等の管理

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

(3)支給端末の取り扱い

①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。

②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。

③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

④教職員等は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をすること。

⑤支給端末から離れるときは、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。

⑥業務終了後と外出時には、電源を落とさなければならない。

(4)支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

①教職員等は、支給以外のパソコン、モバイル端末を業務に利用してはならない。また、支給以外のパソコン、モバイル端末からクラウドサービス等を通じて、教育委員会・学校が構築・管理している環境にアクセスしてはならない。

②教職員等は、支給以外の電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て利用することができ

る。なお、教育情報セキュリティ管理者の許可を得た上で、支給以外の電磁的記録媒体等を用いて、外部で情報処理作業を行う際は、安全管理措置を遵守しなければならない。

(5)モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築・管理している環境（本対策基準が適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

①教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

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

(6)ID の管理

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

①自己が利用している ID は、他人に利用させてはならない。

②共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

③教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、教育情報セキュリティ統括責任者又は教育情報システム管理者に依頼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い。

①パスワードは、他者に知られないように管理しなければならない。

②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④パスワードが流出したおそれがある場合には、教育情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く）

⑥仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。

⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

⑧教職員等間でパスワードを共有してはならない。（ただし、共有 ID に対するパスワードは除く）

(8)外部電磁的記録媒体の取扱い

①利用する外部電磁的記録媒体は、教育委員会又は学校から支給された公式の媒体を使用しなければならない。その他の媒体の使用は禁止。

②外部電磁的記録媒体は、盗難・紛失等がないように職員室の適切な場所で管理・保管しなければならない。

(9)電子メールの利用制限

①教職員等は、自動転送機能を用いて、電子メールを転送してはならない。
②教職員等は、業務上必要のない送信先に電子メールを送信してはならない。
③教職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
④教職員等は、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。
⑤教職員等は、ウェブで利用できるフリーメールサービス等を教育情報セキュリティ統括責任者の許可無しに使用してはならない。
⑥機密性２以上の情報を含む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。
⑦メールの送信前に誤送信を予防するため、送信先のメールアドレス、添付ファイルの内容を確認しなければならない。
⑧差出人、添付ファイル又は本文中のリンク先（URL）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にアクセスせずに、教育情報セキュリティ管理者に指示を仰がなければならない。

(10)クラウドサービス、ソーシャルメディアサービスの利用制限

①機密性２以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。なお、強固なアクセス制御による対策を講じたシステム構成の場合は、その限りではない。
②私的に契約したクラウドサービスを業務利用してはならない。
③ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

(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。

①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。OS 及びコンピュータウイルス対策ソフトウェアが常に最新の状態に保てるようにしなければならない。自動更新される設定の場合は、自動更新設定を変えてはならない。
②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。
⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。
⑥教育情報セキュリティ統括責任者が提供するウイルス情報を、常に確認しなければな

らない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、すみやかに教育情報セキュリティ管理者に報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。

(ｱ)パソコン等の端末の場合

直ちに利用を中止し、無線 LAN アダプタの取り外し又は無線 LAN 接続の切断等通信を行わない設定への変更を行わなければならない。また、LAN ケーブルの即時取り外しを行わなければならない。

(ｲ)モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

(ｳ)指示があるまでは、端末の電源は切らずに保持しなければならない。

(12)電子署名・暗号化

①教職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

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

③CISO 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

①教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②教職員等は、業務上の必要がある場合は、教育情報セキュリティ統括責任者及び教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育情報セキュリティ管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③教職員等は、不正にコピーしたソフトウェアを利用してはならない。

(14)機器構成の変更の制限

①教職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

②教職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、教育情報セキュリティ統括責任者及び教育情報システム管理者の許可を得なければならない。

(15)無許可でのネットワーク接続の禁止

教職員等は、教育情報セキュリティ統括責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

(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御

①教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、教育情報セキュリティ管理者を介して、教育情報セキュリティ統括責任者及び教育情報システム管理者の許可を得なければならない。

②教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、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。

①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。

②ID 及びパスワードは他の人に知られないようにすること。

③利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

④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、学習者用端末のローカル保存は必要最小限すること。

⑤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。

⑥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）以外利用しないこと。

⑦学習者用端末が動かない、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。

⑧学習者用端末は大事に取扱い、盗難・紛失・破損等に注意すること。

⑨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。

5.3.教育委員会事務局職員の遵守事項

教育委員会事務局職員は、教育情報セキュリティ責任者の指導の下、以下の規定を遵守しなければならない。なお、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すべて返却するとともに、その後も業務上知り得た情報を漏らさないこと。

①教育情報セキュリティ基本要綱等の遵守

②支給端末等の業務以外の目的での使用の禁止

③校務用端末による外部における情報処理作業の禁止

④機密性２以上の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止

⑤業務上知り得た情報の秘匿

⑥業務を離れる場合の遵守事項

5.4.研修・訓練

(1)情報セキュリティに関する研修・訓練

CISO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

①CISO 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、教育情報セキュリティ委員会の承認を得なければならない。

②研修計画において、教職員等は、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。

③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しなければならない。

④研修は、教育情報セキュリティ統括責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他教職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤CISO は、毎年度１回、教育情報セキュリティ委員会に対して、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。

(3)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。

(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。

5.5.情報セキュリティインシデントの報告

(1)学校内からの情報セキュリティインシデントの報告

①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、速やかに教育情報セキュリティ管理者に報告しなければならない。

②報告を受けた教育情報セキュリティ管理者は、速やかに教育情報セキュリティ責任者、教育情報システム管理者及び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。

③教育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及び教育情報セキュリティ統括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

①教職員等は、教育情報セキュリティ基本要綱に対する違反行為を発見した場合、直ちに教育情報セキュリティ統括責任者及び教育情報セキュリティ管理者に報告を行わなければならない。

②違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると教育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)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

①教職員等は、管理対象のネットワーク及び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、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。

②報告を受けた教育情報セキュリティ管理者は、速やかに教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。

③教育情報セキュリティ責任者は、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及び教育情報セキュリティ統括責任者に報告しなければならない。

④CISO 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。

(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

①教育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、教育情報セキュリティ管理者、教育情報システム管理者及び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。

②CISO は、教育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。

(5)支給端末の運用・連絡体制の整備

学校内外での支給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、実施手順に反映しなければならない。

6.技術的セキュリティ

6.1. コンピュータ及びネットワークの管理

(1)文書サーバ及び端末の設定等

①教育情報システム管理者は、教職員等が使用できる文書サーバの容量を設定し、教職員等に周知しなければならない。

②教育情報システム管理者は、文書サーバを学校等の単位で構成し、教職員等が他の学校等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③教育情報システム管理者は、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当職員以外の教職員等が閲覧及び使用できないようにしなければならない。

④教育情報システム管理者は、インターネット接続を前提とする外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、個人情報などを含む重要性が高い情報を保管する場合に限る）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

(2)バックアップの実施

教育情報セキュリティ統括責任者及び教育情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、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

①教育情報セキュリティ統括責任者及び教育情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②教育情報セキュリティ統括責任者及び教育情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③教育情報セキュリティ統括責任者及び教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(4)ネットワークの接続制御、経路制御等

①教育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、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。

②教育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、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

教育情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ教育ネットワーク及び教育情報システムと論理的又は物理的な分離、もしくは各システムにおけるアクセス権管理の徹底を行わなければならない。

(6)外部ネットワークとの接続制限等

①教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び教育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。

②教育情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④教育情報セキュリティ統括責任者及び教育情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、教育ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、教育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)ネットワークの分離

①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の物理的又は論理的な分離をするとともに、校務系システム及び校務外部接続系システム間の通信経路を物理的又は論理的に分離し、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。

②教育情報システム管理者は、校務系システムと校務外部接続系システム及び学習系システム間で通信する場合には、各システムにおけるアクセス権管理の徹底やウイルス感染のない無害化通信など、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

①教育情報セキュリティ統括責任者は、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。

②教育情報セキュリティ統括責任者は、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。

③教育情報セキュリティ統括責任者は、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

教育情報セキュリティ統括責任者は、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

①教育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。

②教育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

①教育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。

②教育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。

③教育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。

④教育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。

⑤教育情報セキュリティ統括責任者は、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。

6.2.アクセス制御

(1)アクセス制御等

教育情報セキュリティ統括責任者又は教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、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ることで、当該システムへの認証強度の向上とアクセス権管理を徹底すること。

(2)外部からのアクセス等の制限

①教育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。

②教育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、システム上利用者の本人確認を行う機能を確保しなければならない。

③教育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。

④教育情報セキュリティ統括責任者及び教育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、モバイル端末管理（MDM）の導入等を通じて、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。

⑤教育情報セキュリティ統括責任者は、外部から教育ネットワークに接続を許可する場合は、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

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

(4)ログイン時の表示等

教育情報システム管理者は、ログイン時におけるメッセージ、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

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

6.3.システム開発、導入、保守等

(1)情報システムの調達

①教育情報セキュリティ統括責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②教育情報セキュリティ統括責任者及び教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(2)情報システムの開発

①システム開発における責任者及び作業者の特定

教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者の ID の管理

(ｱ)教育情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管

理し、開発完了後、開発用 ID を削除しなければならない。

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

③システム開発に用いるハードウェア及びソフトウェアの管理

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

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

(3)情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

(ｱ)教育情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

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

(ｳ)教育情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう心配しなければならない。

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

②テスト

(ｱ)教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

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

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

(ｴ)教育情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

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

(4)システム開発・保守に関連する資料等の整備・保管

①教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

②教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

③教育情報システム管理者は、情報システムに係るソースコード及び使用したオープン

ソースのバージョン（リポジトリ）を適切な方法で保管しなければならない。

(5)情報システムにおける入出力データの正確性の確保

①教育情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②教育情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③教育情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6)情報システムの変更管理

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

(7)開発・保守用のソフトウェアの更新等

教育情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8)システム更新又は統合時の検証等

教育情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

6.4. 不正プログラム対策

(1)教育情報セキュリティ統括責任者の措置事項

教育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。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイなどにおいてコンピュータウ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。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイなどにおいてコンピュータウ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。

③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。

④所掌するサーバ及びパソコン等の端末に、コンピュータウ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。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

(2)教育情報システム管理者の措置事項

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

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

②不正プログラム対策は、常に最新の状態に保たなければならない。

③インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している電磁的記録媒体以外を教職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

6.5.不正アクセス対策

(1)教育情報セキュリティ統括責任者の措置事項

教育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。

①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。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、教育情報セキュリティ統括責任者及び教育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。

④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。

⑤教育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及び教育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受けるリスクがある場合、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

教育情報セキュリティ統括責任者及び教育情報システム管理者は、外部からアクセス

できる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(4)標的型攻撃

教育情報セキュリティ統括責任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。

6.6.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

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

(2)不正プログラム等のセキュリティ情報の収集及び周知

教育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

教育情報セキュリティ統括責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、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。

7.運用

7.1.情報システムの監視

①教育情報セキュリティ統括責任者及び教育情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

②教育情報セキュリティ統括責任者及び教育情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③教育情報セキュリティ統括責任者及び教育情報システム管理者は、機密性２以上、完全性２以上、可用性２以上の情報資産を格納する校務系システム及び校務外部接続系システムを常時監視しなければならない。

④教育情報セキュリティ統括責任者及び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。

7.2. 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

①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。

②教育情報セキュリティ統括責任者及び教育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。

③教育情報セキュリティ統括責任者、教育情報システム管理者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がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

(2)情報システム仕様書等の管理

教育情報セキュリティ統括責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧、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

教育情報セキュリティ統括責任者及び教育情報システム管理者は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を障害記録として記録し、適切に保存しなければならない。

(4)記録の保存

CISO 及び教育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。

7.3. 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

①教育情報セキュリティ統括責任者及び教育情報システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

②教育情報セキュリティ統括責任者及び教育情報システム管理者は、利用されていない ID 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。

(2)パスワードに関する情報の管理

教育情報セキュリティ統括責任者又は教育情報システム管理者は、教職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機

能がある場合は、これを有効に活用しなければならない。

7.4.特権を付与された ID の管理等

①教育情報セキュリティ統括責任者及び教育情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

②教育情報セキュリティ統括責任者及び教育情報システム管理者の特権を代行する者は、教育情報セキュリティ統括責任者及び教育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。

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

④教育情報セキュリティ統括責任者及び教育情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

⑤教育情報セキュリティ統括責任者及び教育情報システム管理者は、特権を付与された ID 及びパスワードについて、その利用期間に合わせて特権 ID を作成・削除する、もしくは、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教育情報セキュリティ統括責任者及び教育情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

⑦教育情報セキュリティ統括責任者及び教育情報システム管理者は、特権を付与された ID のログ監視を行わなければならない。

7.5.情報セキュリティ基本要綱の遵守状況の確認

(1)遵守状況の確認及び対処

①教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、教育情報セキュリティ基本要綱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 CISO 及び教育情報セキュリティ統括責任者に報告しなければならない。

②CISO は、発生した問題について、適切かつ速やかに対処しなければならない。

③教育情報セキュリティ統括責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における教育情報セキュリティ基本要綱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)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に、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。

(3)業務以外の目的でのウェブ閲覧の禁止

教育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、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

(4)教職員等による不正アクセスの管理

教育情報セキュリティ統括責任者及び教育情報システム管理者は、教職員等による不正アクセスを発見した場合は、当該教職員等が所属する学校等の教育情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

7.6.専門家の支援体制等

(1)専門家の支援体制

教育情報セキュリティ統括責任者は、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。

(2)他団体との情報システムに関する情報等の交換

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

7.7.侵害時の対応等

(1)緊急時対応計画の策定

CISO 又は教育情報セキュリティ委員会は、教育情報セキュリティインシデント、教育情報セキュリティ基本要綱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。

①関係者の連絡先

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

(3)業務継続計画との整合性確保

自然災害、大規模又は広範囲にわたる疾病等に備えて別途業務継続計画を策定し、教育情報セキュリティ委員会は当該計画と教育情報セキュリティ基本要綱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 又は教育情報セキュリティ委員会は、教育情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

7.8.例外措置

(1)例外措置の許可

教育情報セキュリティ管理者及び教育情報システム管理者は、教育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

教育情報セキュリティ管理者及び教育情報システム管理者は、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。

7.9.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 12 月 13 日法律第 261 号)

②教育公務員特例法(昭和 24 年 1 月 12 日法律第 1 号)

③著作権法(昭和 45 年法律第 48 号)

④不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)

⑤個人情報の保護に関する法律(平成 15 年 5 月 30 日法律第 57 号)

⑥行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号)

⑦サイバーセキュリティ基本法(平成 26 年法律第 104 号)

⑧交野市個人情報保護条例(昭和 63 年交野市条例第 10 号)

7.10.処分等

(1)懲戒処分

教育情報セキュリティ基本要綱に違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

(2)違反時の対応

教職員等の教育情報セキュリティ基本要綱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教育情報セキュリティ統括責任者が違反を確認した場合は、教育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の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

②教育情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに教育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の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

③教育情報セキュリティ管理者の指導によっても改善されない場合、教育情報セキュリティ統括責任者は、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を使用する権利を停止あるいは剥奪することができる。その後速やかに、教育情報セキュリティ統括責任者は、教職員等の権利を停止あるいは剥奪した旨をCISO及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知しなければならない。

8.外部サービスの利用

8.1.外部委託

(1)外部委託事業者の選定基準

①教育情報システム管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②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。

(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等を明記した契約を締結しなければならない。

・教育情報セキュリティ基本要綱及び教育情報セキュリティ実施手順の遵守
・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
・提供されるサービスレベルの保証
・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
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市教育委員会による監査、検査

・市教育委員会による教育情報セキュリティインシデント発生時の公表
・教育情報セキュリティ基本要綱が遵守されなかった場合の規定(損害賠償等)

(3)確認・措置等

教育情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置しなければならない。また、その内容を教育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)委託事業者に対する対応

教育情報セキュリティ管理者及び教育情報システム管理者は、教育情報セキュリティ基本要綱または、教育情報セキュリティ実施手順、その他の関連法令等のうち、委託事業者が守るべき内容について説明し、遵守させなければならない。

なお、個人情報を取り扱う作業を委託する場合は、委託事業者に対し、必ず個人情報の保護に関する覚書を取り交わさなければならない。

(5)特定個人情報を取り扱う委託契約における契約項目

特定個人情報を取り扱う委託契約を締結する場合は(2)の契約項目に示す内容に加え以下の①～④を規定しなければならない。

①事業所内からの特定個人情報の持ち出しの禁止
②漏えい事案等が発生した場合の委託先の責任
③特定個人情報を取り扱う従業員の明確化
④再委託先に対する監督義務及び当該監督の状況を市に報告する義務

8.2.約款による外部サービスの利用

(1)約款による外部サービスの利用に係る規定の整備

教育情報システム管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性２以上の情報の取り扱いには十分に留意するよう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。

8.3.ソーシャルメディアサービスの利用

①教育情報システム管理者は、教育委員会又は学校が管理するアカウントでソーシャル

メディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

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

(ｲ)パスワードや認証のためのコード等の認証情報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２以上の情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

9.評価・見直し

9.1.監査

(1)実施方法

CISO は、教育情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

(2)監査を行う者の要件

①教育情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②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

①教育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、教育情報セキュリティ委員会の承認を得なければならない。

②被監査部門は、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

外部委託事業者に委託している場合、教育情報セキュリティ監査統括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、情報セキュリティ基本要綱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。

(5)報告

教育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、CISO に報告する。

(6)保管

教育情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

(7)監査結果への対応

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教育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)教育情報セキュリティ基本要綱及び関係規程等の見直し等への活用

CISOは、監査結果を教育情報セキュリティ基本要綱及び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活用しなければならない。

9.2.自己点検

(1)実施方法

①教育情報セキュリティ統括責任者及び教育情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する部局における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、毎年度及び必要に応じて自己点検を行わなければならない。

(2)報告

教育情報セキュリティ統括責任者、教育情報システム管理者及び教育情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、CISOに報告しなければならない。

(3)自己点検結果の活用

①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。

②CISOは、この点検結果を教育情報セキュリティ対策基準及び関係規程等の見直し、その他教育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。

9.3.教育情報セキュリティ基本要綱及び関係規程等の見直し

CISOは、教育情報セキュリティ監査及び自己点検の結果並びに教育情報セキュリティに関する状況の変化等をふまえ、教育情報セキュリティ基本要綱及び関係規程等について重大な変化が発生した場合及び必要に応じて評価を行い、必要があると認めた場合、改善を行うものとする。

附　則

1 この要綱は、令和2年7月1日から施行する。

2 この要綱は、令和4年12月27日から施行する。

3 この要綱は、令和7年4月1日から施行する。