令和３年１月２８日
第２回教育委員会資料
教育部学務課

立川市立学校情報セキュリティポリシーの概要

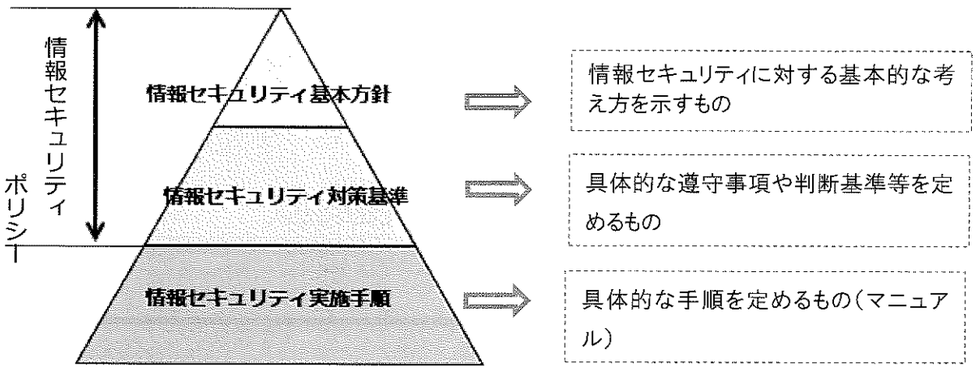
学校における情報セキュリティを確保するための方針、体制、対策等を包括的に定めている情報セキュリティポリシーについて、教育ICTシステム・校務支援システム等の導入に伴い、再構築します。情報セキュリティポリシーの主な変更点は組織体制、情報資産の管理、技術的セキュリティ対策、クラウドサービスの利用です。概要は以下のとおりです。

【 情報セキュリティとは・・・情報資産の機密性・完全性・可用性を保つこと 】

機密性：許可された者だけが、情報にアクセスできること。　完全性：情報が正確で完全であること。　可用性：必要なときに情報資産にアクセスできること。

情報セキュリティポリシーとは

情報セキュリティ対策に関する規程は下図の体系で構成され、「情報セキュリティ基本方針」と「情報セキュリティ対策基準」をあわせて「情報セキュリティポリシー」と称します。



1. 対象

①対象者　立川市立学校及び教育委員会に所属する教職員

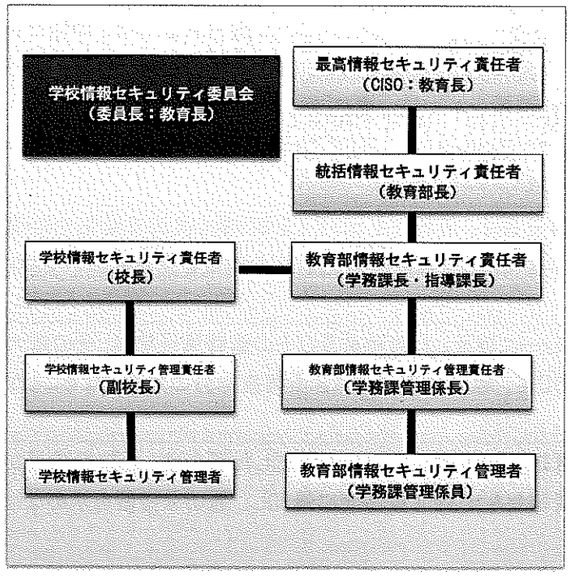
※市が保有する情報資産（ネットワーク、情報システム等）を利用する教職員は、市の情報セキュリティポリシーも遵守すること

※学校が保有する情報資産を利用する委託業者やボランティア等も、情報セキュリティポリシーを遵守すること

②対象とする情報資産

情報資産の種類		情報資産の例
情報システム等	ネットワーク	通信回線、ルータ等の通信機器
	情報システム	サーバ、パソコン、タブレットPC、ソフトウェア等
	これらに関する設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
	電磁的記録媒体	USBメモリ、外付けハードディスクドライブ、DVD、磁気テープ等の外部電磁的記録媒体
紙文書		紙文書全般

2. 組織体制



POINT

①最高情報セキュリティ責任者（CISO）をトップとして体系的に責任者等を配置します。

②各校の校長は学校情報セキュリティ責任者とし、学校における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します。

③情報セキュリティの重要事項に関する調査・決定、統一的な維持管理等を行う組織として学校情報セキュリティ委員会を設置します。

3. 情報資産の管理

情報資産は重要性に応じて次のとおり分類しています。

分類	定義	該当する情報資産のイメージ例
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	指導・学籍要録原本 教職員の人事情報
Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす	出席簿 成績に関する個票等 個別の教育支援計画
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす	児童・生徒の学習記録（ワークシート、レポート、作品等） 卒業アルバム
Ⅳ	影響をほとんど及ぼさない	学校要覧

上記の分類は情報資産の機密性・完全性・可用性をどこまで確保すべきかを基準にした分類であり、この3点についてどの段階に属するかによって情報資産が上記4段階のいずれかに分類されます。

4. 物理的セキュリティ対策

サーバ、通信回線及びパソコン等の管理について、物理的な対策を講じます。

POINT

サーバの管理	✓ 地震、火災、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しなければならない。 ✓ 重要情報を格納している校務系サーバ、教育系サーバのバックアップを取るなど同一データを保持するよう努めなければならない。
端末の管理	✓ 指導者用端末・・・校内においては施錠できる充電保管庫にて保管すること ✓ 校務用端末・・・端末のワイヤーによる固定、鍵の管理を行わなければならない。
認証機能	✓ 情報システムにログインするための認証機能(ID・パスワード等)を設定しなければならず、必要に応じてパスワード以外に指紋認証、物理認証等の多要素認証を併用しなければならない。
モバイル端末の遠隔消去機能	✓ モバイル端末の学校外での業務利用の際には、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。
USB メモリの取扱い	✓ USB の保有は必要最小限とし、施錠できる場所にて保管を行い、利用に際しては利用簿に記録しなければならない。 ✓ 支給する USB メモリにウイルス対策やデータの暗号化対策、パスワード設定等の措置を講じなければならない

5. 人的セキュリティ対策

教職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じます。

POINT

教職員の遵守事項	✓ 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。 ✓ 支給以外の端末及び電磁的記録媒体等を業務に使用してはならない。
児童・生徒への指導	✓ 教職員は、学習用端末の適切な使用ができるよう指導しなければならない。
情報セキュリティインシデントの報告	✓ 教職員は、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報告しなければならない。
ID 及びパスワード等の管理	✓ 自己が保有している ID 及びパスワード等を他人に使用させてはならない。 ✓ 共有 ID 及びパスワード等を使用する場合には、利用者以外に使用させてはならない。
インターネット及び各種機器等の取扱い制限	✓ 業務以外の目的でインターネットを使用してはならない。 ✓ 付与されたメールアドレス以外を使用してはならない。 ✓ 個人情報の外部送信を行ってはならない。 ✓ 自動転送機能を用いて、電子メールを送信してはならない。

6. 技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、不正プログラム対策等の技術的な対策を講じます。

POINT

ネットワークの分離	✓ インターネットに接続されている教育系ネットワークとインターネット分離環境下の校務系ネットワークについて、物理的または論理的に分離する措置を講じなければならない。
校務システムにおける無害化処理	✓ 校務系システムとその他のシステムとの間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。
支給端末の管理	✓ 原則、支給端末以外の端末をネットワークに接続してはならない。 ✓ 支給端末に許可なくソフトウェアを導入してはならない。
無線 LAN の利用	✓ 無線 LAN を利用する際、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。ただし、重要性分類Ⅰ・Ⅱの情報を無線 LAN で取り扱ってはならない。
不正プログラム対策	✓ 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、原則として学校及び教育委員会事務局が管理している媒体以外を使用してはならない。

7. 運用

セキュリティポリシーの運用面の対策について定めます。

POINT

情報セキュリティポリシーの遵守状況の確認	✓ 学校情報セキュリティ責任者及び学校情報セキュリティ管理責任者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに是正するとともに統括情報セキュリティ責任者に報告しなければならない。 ✓ CISO 及び統括情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対応しなければならない。
侵害時の対応等	✓ 統括情報セキュリティ責任者は、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。
懲戒処分	✓ 情報セキュリティポリシーに違反した教職員及びその監督責任者は、その重大性や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なることがある。
違反時の対応	✓ 統括情報セキュリティ責任者は教職員の違反を認知した場合は、当該教職員が所属する学校の学校情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

8. 外部サービスの利用

外部サービスの利用を想定した対策について定めます。

POINT

外部委託	✓ 統括情報セキュリティ責任者及び学校情報セキュリティ責任者は、外部委託事業者の選定にあたり、業務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。
約款による外部サービスの利用	✓ 教職員は、約款への同意及び簡易なアカウント登録により利用可能なサービス（電子メール、ファイルストレージサービス等）を許可なく利用してはならない。 ✓ 教職員は、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。
ソーシャルメディアサービス・ホームページの利用	✓ 教職員はソーシャルメディアサービスを利用してはならない。業務上の必要から利用する場合は、統括情報セキュリティ責任者及び学校情報セキュリティ責任者の許可を得た上で、情報セキュリティ対策に関する運用手順を定めなければならない。
情報発信の制限	✓ 重要性Ⅰ・Ⅱの情報をソーシャルメディアサービスで発信してはならない。（個人のアカウントでの情報発信を含む。）

9. クラウドサービスの利用

クラウドサービスを利用する際の対策について定めます。

POINT

利用者認証	✓ 適切な利用者認証がなされていること。
アクセス制限	✓ アクセスする権限のないものがアクセスできないようにすること。
保管するデータの暗号化	✓ データの保管に際し、情報漏洩等に備えて暗号化等の保護の措置が講じられていること。
技術的セキュリティ対策	✓ 情報システムを監視し、セキュリティ侵害を検知すること。
物理的セキュリティ対策	✓ サーバ等の管理条件を情報セキュリティ対策基準の「4.1 サーバ等の管理」に準じた対策をとること。
データの廃棄等	✓ サービスの利用終了時等において、データが不用意に残置されないようにすること。
守秘義務・目的外利用及び第三者への提供の禁止	✓ クラウド事業者との契約時に守秘義務、目的外利用及び第三者への提供の禁止事項を締結しなければならない

クラウドサービスの情報セキュリティの実態を、利用者が詳細に調査することは困難としているため、実際の運用では、ISO 等の第三者認証を得ていることがその代わりとなることとされている

10. Web 会議の利用に関するガイドライン

Web 会議の利用に関するガイドラインついて定めます。

POINT

情報資産の取り扱い	✓ 学校または教育委員会が保有する情報資産を利用すること。 ✓ Web 会議では重要性分類Ⅰ・Ⅱの情報は取り扱わないこと。
Web 会議のツール	✓ 教育委員会が提供するアカウント及び Google Meet を使用すること。 ✓ 上記の方法以外で Web 会議を行う場合は統括情報セキュリティ責任者の許可を得ること。
外部サービスの利用	✓ 外部サービスを利用する場合は、情報セキュリティ対策基準の「8.外部サービスの利用」の規定に沿い事前に許可を得ること。
Google Meet 使用時の注意点	✓ ファイル共有機能によるファイル授受は行わないこと。 ✓ 画面共有機能により他の参加者と画面を共有する場合、重要性分類Ⅰ・Ⅱの情報が共有されることが無いようにすること。 ✓ 録画・録音機能を使用する場合には、事前に会議参加者の許可を得ること。 ✓ カメラを使用する場合には、会議に不要な情報が背景に映り込まないようにすること。また、会議と関連の無い音声を取得されることが無いよう、機器等の設置場所等に注意すること。

11. 評価・見直し

セキュリティポリシーを運用するにあたっての評価・見直しについて定めます。

POINT

情報セキュリティ監査	✓ CISO は学校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を実施しなければならない。
監査結果への対応	✓ CISO は、監査により、指摘された事項について所管する学校情報セキュリティ責任者に対し、対処を指示しなければならない
自己点検	✓ 学校情報セキュリティ責任者は、自校の情報セキュリティ対策の実施状況について、定期的又は必要に応じて点検を実施しなければならない。
自己点検結果の活用	✓ 学校情報セキュリティ管理責任者は、自己点検の結果に基づき、自己の責任において問題点の改善を図らなければならない。
ポリシーの見直し	✓ CISO 及び学校情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシーについて、必要に応じて評価を行い、必要があると認めた場合は改善・見直しを行うものとする。