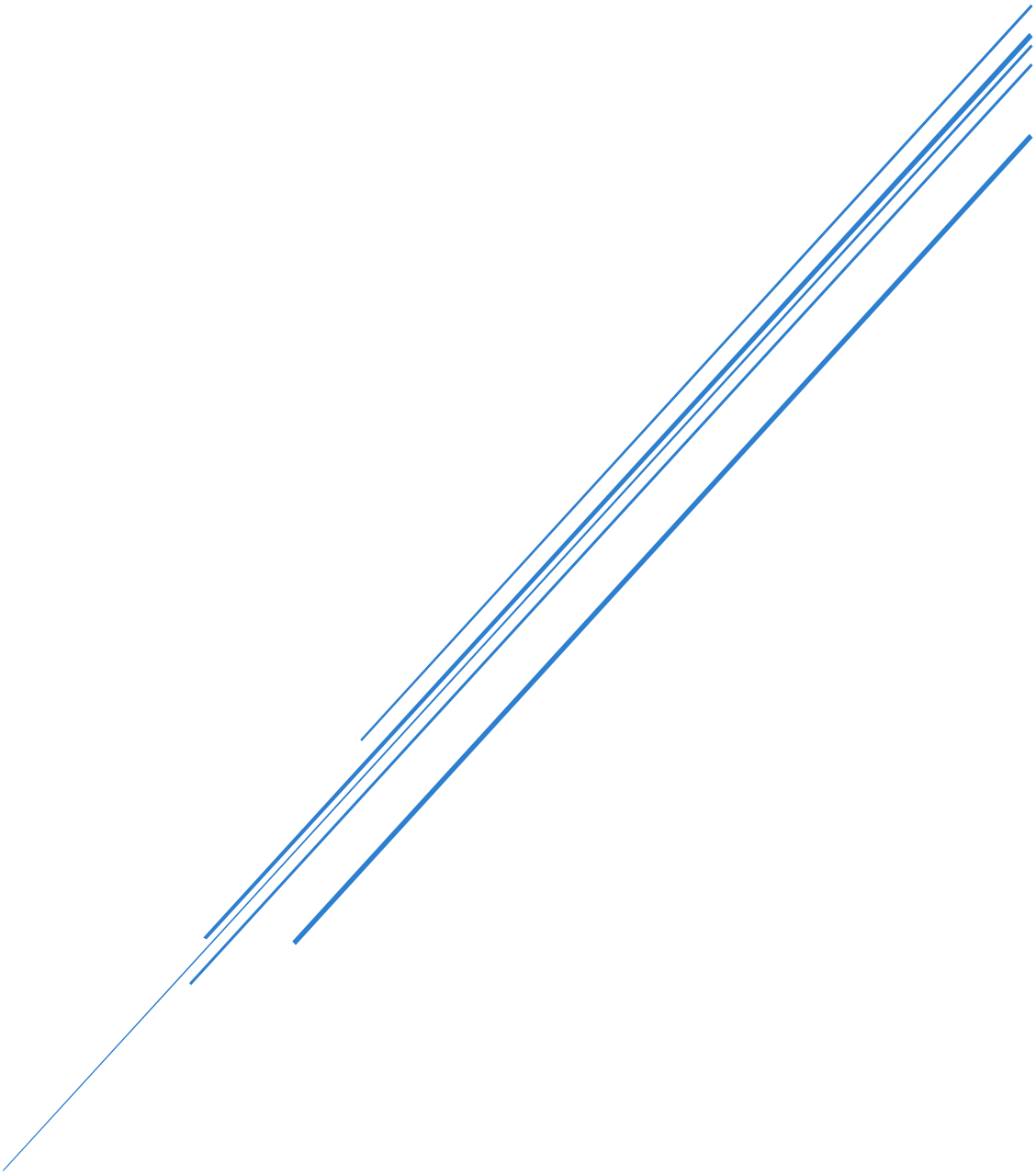
さぬき市教育情報セキュリティポリシー

教育情報セキュリティ基本方針



教育情報セキュリティ基本方針

令和８年３月１日
さぬき市教育委員会

１．目的

さぬき市立小学校及び中学校（以下「学校」という。）においては、令和元年度以降、ＧＩＧＡスクール構想に基づく１人１台端末の整備、クラウドサービスの活用が進み、個別最適な学びと協働的な学びを充実させることができるようになった。

学校には、児童生徒、保護者、教職員等の個人情報及び学校運営上重要な情報が保管されており、外部への漏洩等が発生した場合は、二次被害も含め、極めて重大な結果を招くおそれがある。

そのため、学校のＩＣＴ環境整備が進むにあたり、不正アクセス、ウイルス攻撃や部外者の侵入等の意図的な要因による情報資産の漏洩・破壊・改ざん・消去などの脅威からの情報資産の保護に向けた十分な情報セキュリティ対策を講じることは、教職員及び児童生徒等が安心してＩＣＴを活用するために不可欠である。

これらのことから、本基本方針は、本市教育委員会及び学校が保有する情報資産の機密性、完全性及び可用性を維持するため、本市教育委員会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．教育情報セキュリティポリシー

ＧＩＧＡスクール構想の推進により、クラウドサービスの活用を前提としたネットワーク構成等の課題に対応するとともに、児童生徒等の端末と教職員の端末から得られる各種教育情報を効果的に活用して教育の質的改善を図るため、文部科学省の「教育情報セキュリティポリシーに関するガイドライン（令和７年３月版）」を参考に、本市教育委員会において、本基本方針に基づいた「教育情報セキュリティ対策基準」（以下「対策基準」という。）を策定し、本基本方針と対策基準を合わせて「教育情報セキュリティポリシー」（以下「ポリシー」という。）とする。

なお、学校に敷設されている行政系ネットワークの取扱いについては、「さぬき市情報セキュリティポリシー」に準拠するものとする。

３．用語の定義

(1) ネットワーク

学校、教育委員会における学校用の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) 情報資産

情報システム及びネットワーク並びにこれらで取り扱われる学校情報（これらを印刷したものを含む。）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

情報にアクセスすることが認められた者だけが、情報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

情報にアクセスすることが認められた者だけが、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(7) 校務系情報

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をいう。

(8) 校務外部接続系情報

校務系情報のうち、保護者メールや学校ホームページ等の外部と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をいう。

(9) 学習系情報

学校が保有する情報資産のうち、それら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をいう。

(10) サーバ

ネットワーク上で学校情報を処理し、端末に提供するコンピュータをいう。

(11) 端末機

ネットワークを通じてサーバに接続されたパソコンやモバイル端末（タブレット等）機器をいう。

(12) 校務用端末

校務系情報全てにアクセス可能な端末をいう。

(13) 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をいう。

(14) 指導者用端末

学習系情報にアクセス可能な端末で、教職員のみが利用可能な端末をいう。

(15) 教育情報システム

情報資産を扱うハードウェア、ソフトウェア、クラウドサービス等をいう。

(16) 情報セキュリティインシデント

情報セキュリティに関する問題としてとらえられる事象（障害、事件、事故、欠陥、攻撃、侵害等）をいう。

(17) 記録媒体

情報システムでデータ等を記録するための媒体（メディア)。サーバ、端末機、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内臓電磁的記録媒体と、外付けハードディスク、ＣＤ－ＲＯＭ、ＤＶＤ－Ｒ、ＵＳＢメモリ、ＳＤカード等の外部電磁的記録媒体をいう。

(18) スマートデバイス

情報処理端末（デバイス）のうち、スマートフォンやタブレット等、携行可能な多機能端末をいう。

(19) 無線ＬＡＮ

電波等を利用してデータの送受信を行う構内通信網システムをいう。

(20) クラウド

学校外、庁舎外でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念をいう。

(21) ソーシャルメディアサービス

インターネット上における、ホームページ、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等をいう。

(22) 教職員等

本市教育委員会所管の学校に勤務する教職員等であり、学校長、教頭、教職員、会計年度任用職員やその他学校に所属する職員をいう。

４．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、教育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や部外者の侵入等の意図的な要因による情報資産の漏洩・破壊・改ざん・消去、重要情報の搾取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規則違反、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洩・破壊・消去等

(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

(4) 大規模・広範囲にわたる疾病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

５．適用範囲

ポリシーが対象とする情報資産は、次のとおりとする。

(1) ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

(2) 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。）

(3) 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

６．教職員等の遵守義務

教職員等は、情報セキュリティについて共通認識を持ち、情報資産の利用にあたっては、関係法令を遵守しなければならない。また、教職員等は、教育情報セキュリティの重要性を認識し、ポリシーを遵守しなければならない。

７．教育情報セキュリティ対策

情報資産を脅威（４．対象とする脅威）から保護するため、以下の教育情報セキュリティ対策項を講じる。

(1) 管理体制

情報資産を管理し、機密性、完全性及び可用性を維持するための体制を確立する。

(2) 情報資産の分類と管理

学校の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。

(3) 物理的セキュリティ

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・盗難等から保護するために施設整備等の物理的な対策を講じる。

(4) 人的セキュリティ

教育情報セキュリティに関する権限や責任を定めるとともに、全教職員等にポリシーを周知徹底させるための教育及び啓発を行う等の人的な対策を講じる。

(5) 技術的セキュリティ

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、不正アクセス対策等の技術的対策を講じる。

(6) 運用

情報システムの監視、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の確保等、ポリシーの運用面の対策を講じるものとする。また、自用法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、緊急的対応計画を策定する。

(7) 外部委託及び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、利用できるソーシャルメディアごとの責任者を定める。

８．監査及び自己点検

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教育情報セキュリティ監査及び自己点検を実施する。

９．ポリシーの見直し

教育情報セキュリティ監査及び自己点検の結果、ポリシーの見直しが必要となった場合及び教育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、ポリシーを見直す。

１０．　教育情報セキュリティ実施手順の策定

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を策定する。

なお、情報セキュリティ実施手順は、公開すると情報セキュリティ目的の達成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。