沖縄県立首里東高等学校における情報セキュリティポリシー

(Information Security Policy)

基本方針

１　目　的

学校には生徒はもちろん、保護者、教職員などの個人情報や教育情報などの様々な情報資産があり、それらに対する運用基準が必要である。

そこで、沖縄県立首里東高等学校内の情報資産の運用の仕方を統一し、組織的にセキュリティ対策を実施するため、沖縄県立首里東高等学校では「情報セキュリティポリシー」（以下ＩＳＰ)を定める。

なお、ＩＳＰについては、

- 基本方針
- 対策基準

を作成するとともに、各担当者や全教職員が運営しやすいような簡易な手順マニュアルについても作成し、スムーズな運営を図る。

２　定　義

（１）ネットワーク

学校内において、生徒、保護者、教職員および学校関係者が使用するハードウェア相互の接続のための通信網、および機器（ハードウェアおよびソフトウェア）、記憶媒体で構成された、処理を行う仕組みを指す。

（２）情報システム

学校内におけるネットワーク、ハードウェア、ソフトウェアおよび記憶媒体を指す。

（３）情報資産

ネットワーク、情報システムの運用において取り扱うすべてのデータ及び印刷物、手書き文書等の生徒、保護者、教職員などの個人情報や教育情報を指す。

（４）情報セキュリティ

情報資産の機密の保持、正確性、完全性の維持、および定められた範囲での利用可能な状態を維持すること。

３　対象範囲と定義

○　本校の取扱う情報資産

○　本校の校内ネットワークに接続するすべての機器・コンピュータ等、教職員所持の機器も含む

※常時接続ではなくても接続することがある機器はすべて

○　生徒及び教職員が使う電磁的記憶媒体

・USB メモリ、CD－R などのデータを記録する物

○　上記のいずれかのものを使用する生徒、保護者、教職員、学校関係者

○　外部・内部公開の学校公式ホームページの内容等

４　ポリシーの位置づけ

ＩＳＰは、本校における情報資産への情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最上位に位置されるものである。

５　情報セキュリティ管理体制

学校内の情報資産に関して、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。

６　情報資産の分類

情報資産をその機密性により分類し、それぞれに応じた情報セキュリティ対策を行う。

７　情報資産のリスク分析

学校内の情報資産に関して、特に認識すべきリスクは以下の通りである。

（１）機器について

○　地震、火災、落雷などによるシステムの故障および停止。

○　機器、媒体そのものの盗難。

（２）不正アクセスについて

○　外部からの故意または意図しない操作などでの不正アクセスによる､情報資産の盗聴、持ち出し、改ざん、消去。また不正アクセスの踏み台。

○　内部からの故意または意図しない操作などでの不正アクセスによる､情報資産の盗聴、持ち出し、改ざん、消去。また不正アクセスの踏み台。

（内部・本校内のネットワーク内）

（３）ウィルスについて

○　電子メールや、ＵＳＢメモリなどの記憶媒体、もしくはネットワークを経由したウィルス感染によるデータ、システムの破壊。

○　ウィルス感染による第３者へのウィルス送信。

（４）プライバシー、有害情報、その他

○　情報資産公開における生徒・保護者・教職員のプライバシー情報流出。

○　生徒への有害情報流入。

○　生徒間もしくは、Web サイトへの書き込みなどのデータ授受における故意または無意識での誹謗中傷行為。

８　情報セキュリティ対策

情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（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や、情報資産を保護するために物理的な対策を講じる。

（２）人的セキュリティ対策

情報セキュリティに関する権限や責任を明確にし、全教職員に
情報セキュリティポリシーの内容を周知させるための研修や啓発などの対策を講じる。

（３）技術的セキュリティ対策

情報資産を保護するために、アクセス制御、ネットワーク管理など主に技術的な面での対策を講じる。また、緊急事態が発生した場合の対応策など、危機管理対策を講じる。

９　情報セキュリティ対策基準の策定

学校内の情報資産を保護するために遵守すべき行為や判断基準の統一化などに関して、基本的な要件を明記した情報セキュリティ対策基準を策定する。

10　情報セキュリティ具体的方策例の策定

情報セキュリティ実施手順を行う際の具体的な実施方法や、活用ソフト等を紹介し、ＩＳＰの円滑な運営を促す。

11　情報セキュリティ監査の実施

情報セキュリティポリシーが遵守されていることを検証するために、定期的に監査を実施する。

12　評価および見直しの実施

情報セキュリティ監査の実施結果や、新規機器の導入、さらには最新セキュリティ情報により、ＩＳＰに定める事項の見直しを実行する。

沖縄県立首里東高等学校における

情報セキュリティポリシー（ＩＳＰ）

対策基準

１　情報セキュリティ管理体制

情報セキュリティ対策に関して、沖縄県立首里東高等学校においては以下の体制をとる。

○ 情報システム責任者　学校 CIO(Chief Information Officer) 学校長
○ ネットワーク・情報セキュリティ管理者　教頭
○ ネットワーク・情報セキュリティ担当者　情報教育担当
○ ネットワーク委員会

また、情報セキュリティに関する情報等については機器納入業者とも連携して対処する。

２　情報の分類と管理

２－１情報の管理責任

本校の情報システムにおける情報に関しては、情報システム責任者が管理責任を有する。

２－２情報の分類と管理方法

（１）情報の分類

対象となる情報システム内や、対象範囲となる生徒、保護者、教職員、学校関係者が作成した、本校に関係のある情報資産を、秘匿性の高さにより以下のように分類する。

［A］ 生徒・保護者・教職員および学校関係者の個人情報が含まれているもの
［B］ 教育機関など特定の対象において公開可能なもの
［C］ 一般的に公開しても問題のないもの

（２）情報の管理方法

ア　情報の管理および取り扱い

情報については、それぞれの分類にしたがって管理する。

イ　情報の作成、更新

情報の作成、更新にあたり、上記[A][B][C]の情報を教職員のパソコンで行うことが多いが、その作成、更新についての情報を管理する。

ウ　記憶媒体の管理

学校内の、データを記録できる様々な記憶媒体については、適切な管理を行う。

エ　記憶媒体の処分

上記[A][B][C]の情報については、それぞれの分類に従って適切に処分する。

３　物理的セキュリティ

３－１サーバ

Web 公開用・メールに関するサーバは、ＩＴ教育センターに設置・管理されている。

校内に設置しているファイルサーバは、耐震、耐水、耐熱、耐湿対策を講じた場所に設置し、容易に移動できないように固定する。

３－２コンピュータ室

コンピュータ室への入退出については、基本的に本校職員と生徒のみとする。

参観日等で、保護者が入退出することもできるが、教職員がいるときに限る。

３－３普通教室、特別教室

普通教室、特別教室に設置してあるネットワークに接続できる機器に関しては、容易に移動できないようにする。

また、教職員個人のコンピュータや、ノートパソコンのように持ち運びが可能な機器については、その管理責任は個人に有するものとする。

３－４ネットワーク

外部へのネットワーク接続は、委員会が定めた方法のみとする。

３－５生徒用端末

生徒が使用する端末は、盗難防止のための対策を講じる。

４　人的セキュリティ

４－１役割・責任

（１）情報システム責任者（学校 CIO　学校長）

学内のネットワーク、情報システムおよび情報資産のすべてを統括管理する。 またセキュリティに関する全責任を負う。

（２）ネットワーク・情報セキュリティ管理者（教頭）

情報システム責任者を補佐し、（３）の意見を聞きながら、ネットワーク全般の管理とすべてのセキュリティに関する管理を行う。

（３）ネットワーク・情報セキュリティ担当者

（１）、（２）の指示の元で、ネットワーク・セキュリティ全般に関する作業を行う。

（４）ネットワーク委員会

４－１（１）・（２）・（３）と、教務、各学年代表とで構成し、学内のネットワークに関する内容について話し合う。

（５）教職員

すべての教職員は、ＩＳＰに定められている事項を遵守しなければならない。

また、すべての生徒に対し、ＩＳＰを遵守するように学年の発達段階に応じて指導しなければならない。

４－２教育・訓練

４－１（１）・（２）・（３）は、情報セキュリティポリシーの啓発を行う。

また、情報セキュリティポリシーに関する研修会を設ける。

４－１（１）・（２）・（３）のいずれかは、最新の技術を維持するために研修会を受講するか、情報の収集をする。また、研修内容のうち、要点を全職員に知らせ、円滑なＩＳＰの運営を図る。

４－３事故、欠陥に対する報告

情報セキュリティに関する事故、システム上の欠陥などを発見した場合は、速やかにネットワーク・情報セキュリティ担当者に報告し、指示によって適切な処置をとる。

ネットワーク・情報セキュリティ管理者は、報告内容の分析を行い、再発防止のための記録を保存する。

また、○県教育委員会、○県内の他の高等学校への影響が考えられる場合には速やかに連絡をする。

４－４パスワードの管理

教職員には、ログインパスワード、学校の共有フォルダ等のパスワード、学校のホームページのコンテンツにかかわるパスワードが配布され、教職員はこれを秘密にし、管理しなければならない。

５　技術的セキュリティ

５－１コンピュータ及びネットワークの管理

（１）アクセス記録の取得

情報セキュリティの確保に必要な記録を取得し、一定期間保持する。 また、アクセス記録が改ざん、窃取されないように管理するとともに、アクセス記録を定期的に分析、監視する。

（２）障害記録

情報システムに発生した障害については、その内容を記録し保存すること。

（３）情報およびソフトウェアの交換

学校内において情報システムに関する情報およびソフトウェアを交換する際は、ネットワーク・情報セキュリティ管理者の許可を得る。

（４）バックアップ

ファイルサーバなどに記録された情報については、定期的にバックアップをとる。

（５）メール（教育を目的としたもの）　（詳細は実施手順２）

教育を目的としたものに活用する。

（６）沖縄県立首里東高等学校公式 Web サイト公開　（詳細は実施手順３）

学校の教育活動の紹介や、学校運営に関わる内容を公開したり、広く意見を聞くために沖縄県立首里東高等学校公式 Web サイトを公開する。

（７）サーバ

校内のファイルサーバを適切に管理する。

（８）暗号化

外部にデータを送る場合は、暗号化などの手段を用いる。

（９）利用の制限

教育目的もしくは、学校で必要のある事項以外の使用は禁止する。

生徒、教職員以外の外部の人間が、情報システムを利用する場合は、必ず届けをし、教職員の立ち会いの下で利用する。

(10) 機器構成の変更

端末の機器構成の追加変更などは、４－１（１）・（２）・（３）に相談し、各学校の担当者・教育委員会と相談し許可を得る。

教職員個人のコンピュータをネットワークに接続する際には、４－１（１）、（２）、（３）のいずれかに連絡する。その際には必要なセキュリティの対策を講じる。

(11) 生徒への有害情報の排除

外部からのメールや、ウェブサイトの閲覧などに関しては、生徒にとって有害な情報が入らないように、常に監視し、不適切なものがあれば、即座に４－１（１）・（２）・（３）に連絡し、これを排除するよう努めなければならない。

(12) その他

生徒のＴＶ会議使用に関しては４－１（１）・（２）・（３）に届け、相手校の４－１（１）・（２）・（３）の了解・協力を得て行う。

５－２アクセス制御

（１）利用者登録

ネットワーク・情報セキュリティ管理者は、利用者の登録、変更、削除について定められた方法に従って行う。

（２）管理者権限

ネットワーク・情報セキュリティ管理者の権限は、４－１（１）・（２）・（３）にのみ与える。

（３）外部からのアクセス

他校や、外部からの本校の情報システムへのアクセスは、原則的に禁止する。

（４）事務系情報システムの相互接続

事務用として使用する事務系情報システムと生徒用端末とは、物理的または論理的に切り分けを行い、相互にアクセスできないようにしなければならない。

５－３システム開発、導入、保守等

教育委員会の方針に従う。なお、学校現場の意見を教育センターで集約し、提示することでよりよい導入を図る。

５－４コンピュータウィルス対策

コンピュータウイルスの対策は常に最新の情報を収集し、適切な対策を講じる。

５－５不正アクセス

４－１（１）・（２）・（３）のいずれかは、ネットワーク接続の確認、学校以外のコンピュータからの接続状況を把握する。

５－６セキュリティ情報の収集

４－１（１）・（２）・（３）は、常に情報セキュリティに関する情報を収集し、学内のネットワークおよび情報システムについてセキュリティ上必要な措置を講じる。

６　運用

６－１運用管理

- ４－１（１）・（２）・（３）は、情報セキュリティポリシーが遵守されているかどうかについて、常に確認を行わなければならない。
- 情報システム責任者は、問題が発生した場合には、速やかに対応しなければならない。

６－２運用管理における留意点

- 情報システム責任者は、アクセス記録などプライバシーにかかわる情報については、閲覧を制限できるようにしなければならない。

６－３侵害時の対応策

- 情報資産への侵害が発生した場合には、あらかじめ定めた手段によって、迅速に連絡をとり、証拠保全、被害拡大の防止、復旧などの作業を円滑に実施しなければならない。
- このために以下の緊急時計画を準備しておく。
  a. 緊急時連絡網
  b. 調査内容
  c. 緊急対応策
  d. 再発防止策

７　法令遵守

４－１（１）・（２）・（３）は、ネットワークに関する法令はもちろん、学校教育法その他の法令を遵守しなければならない。また、法令に対する啓発も教職員にしなければならない。

８　情報セキュリティに関する違反に対する対応

違反があった場合には、速やかにその原因を究明し、対処しなければならない。

９　評価・見直し

９－１監査

ネットワーク・情報セキュリティ管理者は、ネットワークおよび情報システムの情報セキュリティについて定期的に監査を実施すること。

９－２点検

４－１（１）・（２）・（３）は、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が実施されているかどうかを、 アンケートなどにより把握すること。

９－３ポリシーの更新

新たに必要な対策が発生した場合は、情報セキュリティポリシーの再評価を行い、必要な改訂、追加を行う。

沖縄県立首里東高等学校情報セキュリティポリシー

（ Information Security Policy）

各教職員の皆様へ

■　目的とお願い

学校には生徒はもちろん、保護者、教職員などの個人情報や教育情報などの様々な情報資産があり、それらに対する運用基準が必要です。

そこで、沖縄県立首里東高等学校内の情報資産の運用の仕方を統一し、組織的にセキュリティ対策を実施するため、沖縄県立首里東高等学校では「情報セキュリティポリシー」（以下ＩＳＰ）を定めました。

この内容は多岐にわたります。全てを全教職員で共通理解して運営することが望ましいのですが、私たちは校務が忙しく共通理解をする時間もなかなか取れないのも現実です。

従って、ここからは、ＩＳＰの簡易バージョンとして、できるだけ分かりやすく記述していますので、各教職員の皆様もご一読いただき共通実践をお願いいたします。

１　各学校の情報セキュリティーに関する責任者等

○　学校ＣＩＯ(Chief Information Officer)　（学校長）

○　ネットワーク・情報セキュリティ管理者（教頭）

○　ネットワーク・情報セキュリティ担当者（教務部情報係）

２　情報セキュリティーで大切にする情報資産(重要度の高いデータ)

・　生徒・保護者・教職員その他学校に関する人の個人情報

■　各教職員が配慮すべきこと

情報セキュリティに関することで困ったら担当者にすぐに相談してください。

１　データの持出

生徒・保護者・教職員その他学校に関する人の個人情報の学校外への持出は基本的に禁止です。

特に以下の物には注意が必要です。

・　学習指導要録　　・　住所録　・　家庭環境調査票　・　生徒の成績　・通知表

※これまでと同じですが、特にデータとして作成された場合、保存先も個人のＵＳＢメモリなどにせずに、学校のサーバーに保存します。

※持出に迷うものがあれば責任者等に相談してください。

２　データの保存

個人で作成されたデータは、個人情報等が入っているかどうかでどこに保存するか決めます。

（１）作成のデータの重要度を決めます。

外部に公開できる内容かどうかを考えます。

（２）重要度により保管場所を決めます。

基本的には校内のサーバーに保存します。特に重要度の高い個人情報等が入っているデータは必ずサーバー内に保存します。

（３）個人のＵＳＢメモリに保存するものは外部に公開してもよい物にします。

例えば学級通信などのデータは持ち帰って作成される方も多いと思います。その際には学校外でのデータ作成においては生徒の個人名は空欄で作成し、学校で印刷する前に　記

入するなどの方法も考えられます。また、データそのものに強固なパスワードをかけておけばよろしいです。

3　ＵＳＢメモリ・ＣＤによるデータの持出の際に気をつけましょう。

重要度の高いデータについては持出をしませんが、その他のデータについても紛失した場合流出の可能性があります。データにはパスワードをかけるようにしましょう。

4　学校のデータをメールにてやりとりする場合にも気をつけましょう。

現在教育委員会からの連絡もメールを利用している場合が多くあります。メールについては以下の点を配慮しましょう。

（１）重要度の高いデータはメールでは送りません。

（２）連絡で必要なデータをメールで送る場合は、パスワードをかけます。なお、そのパスワードは、同じメールでは送りません。

（３）添付ファイルには要注意です。特に親しい人や学校関係者からのメールほど慎重に取り扱いをしましょう。

5　学校のパソコンにソフトをインストールするときには担当者に連絡してください。

学校のパソコンは自由にソフトを入れることができないようになっています。公的なパソコンですのでそれは当然ですが、私たちの周りには素晴らしいソフトウエアがたくさんあります。

そこで、パソコンにインストールする必要が生じたソフトウエアについては、まず、学校の情報教育担当者に連絡してください。

その後教育センターの情報教育担当者で協議・確認をし、校長会、教育委員会の承認を経て利用できます。

※有料のソフトウエアについては予算が伴いますのですぐに入るとは限りません。

※フリーソフトウエアの場合様々な検討をした後の導入になります。

※使わせないための措置ではありません。

6　不明な点はすぐに相談してください。

データについての相談等はすぐに相談をしてください。これらの情報セキュリティポリシーは、先生方の校務等を難しくするために作成するものではありません。先生方情報の流出等の被害に遭わないためにも作成しています。