Ver.1.0

東海村教育情報
セキュリティポリシー

東海村教育委員会

Ver 1.0

東海村
Tokai Village

目次

東海村
Tokai Village

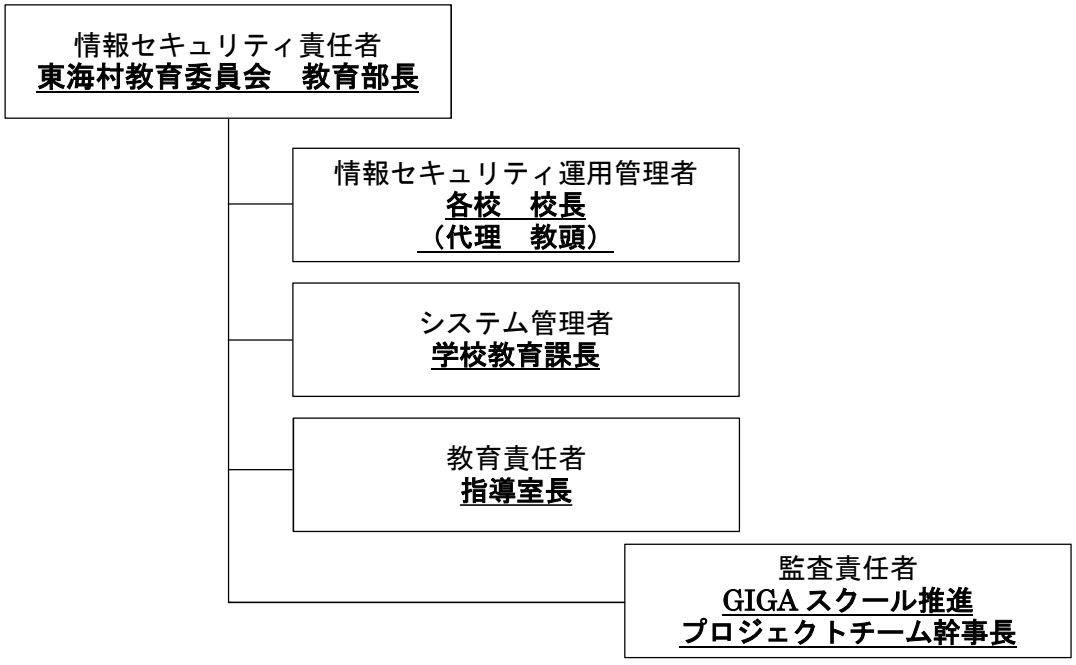
１　組織的対策

１－１　情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として，**東海村情報セキュリティ委員会**を設置する。東海村情報セキュリティ委員会は以下の構成とし，情報セキュリティ対策状況の把握，情報セキュリティ対策に関する指針の策定・見直し，情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに，全責任を負う。
情報セキュリティ運用管理者	情報セキュリティの運用管理責任者。各学校における情報セキュリティ対策の実施などの責任を負う。
システム管理者	情報セキュリティ対策のためのシステム管理を行う。 情報漏えい等の事故発生時にはその影響を判断し，対応を行う。
監査責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し，助言を行う。
教育責任者	情報セキュリティ対策を推進するために教職員への教育・訓練を企画・実施する。

＜東海村情報セキュリティ委員会体制図＞



１－２　情報セキュリティ取組みの監査

監査責任者は，情報セキュリティ関連規程の実施状況について，年１回程度監査を行い，監査結果を東海村情報セキュリティ委員会に報告する。東海村情報セキュリティ委員会は，報告に基づき，以下の点を考慮し，必要に応じて改善計画を立案する。

・情報セキュリティ関連規程が有効に実施されていない場合は，その原因の特定と改善
・情報セキュリティ関連規程に定められたルールが，新たな脅威に対する対策として有効でない場合は，情報セキュリティ関連規程の改訂
・情報セキュリティ関連規程に定められたルールが，関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は，情報セキュリティ関連規程の改訂

１－３　情報セキュリティに関する情報共有

情報セキュリティ運用管理者及びシステム管理者は，新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し，委員会で共有する。

＜専門機関＞

- 独立行政法人情報処理推進機構（略称：IPA）

[情報セキュリティ]

https://www.ipa.go.jp/security/

[ここからセキュリティ]

https://www.ipa.go.jp/security/kokokara/

- JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

- 一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

https://www.jpcert.or.jp/

- 個人情報保護委員会

http://www.ppc.go.jp/

２　人的対策

２－１　雇用条件

教職員を雇用する際には秘密保持に関する誓約書等を提出させる。

２－２　教職員の責務

教職員は，以下を遵守する。

・教職員は，当教育員会が秘匿情報として管理する情報及びその複製物の一切を許可されていない組織，人に提供してはならない。

・教職員は，当教育員会の情報セキュリティ方針及び関連規程を遵守する。違反時の懲戒については，就業規則に準じる。

※当教育委員会が秘匿情報として管理する情報とは，「情報資産管理台帳」の機密性評価値が 1 以上のものをいう

(1)趣旨

懲戒は，使用者が企業秩序を維持し，企業の円滑な運営を図るために行われるものですが，懲戒の権利濫用が争われた裁判例もみられ，また，懲戒は労働者に労働契約上の不利益を生じさせるものであることから，権利濫用に該当する懲戒による紛争を防止する必要があります。このため，法第 15 条において，権利濫用に該当するものとして無効となる懲戒の効力について規定したものです。

(2)内容

①法第 15 条は，使用者が労働者を懲戒することができる場合であっても，その懲戒が「客観的に合理的な理由を欠き，社会通念上相当であると認められない場合」には権利濫用に該当するものとして無効となることを明らかにするとともに，権利濫用であるか否かを判断するに当たっては，労働者の行為の性質及び態様その他の事情が考慮されることを規定したものです。

②法第 15 条の「懲戒」とは，労働基準法第 89 条第 9 号の「制裁」と同義であり，同条により，当該事業場に懲戒の定めがある場合には，その種類及び程度について就業規則に記載することが義務付けられているものです。

２－３　雇用の終了

・教職員は，在職中に交付された業務に関連する資料，個人情報，児童・生徒・取引先から当教育委員会が交付を受けた資料又はそれらの複製物の一切を退職時に返還する。

・教職員は，在職中に知り得た当教育委員会の秘匿情報もしくは業務遂行上知り得た技術的機密を利用して，競合的あるいは競業的行為を行ってはならない。

２－４　情報セキュリティ教育

教育責任者は以下の点を考慮し，情報セキュリティに関する教育及び訓練計画を立案する。

対象者：全教職員

テーマ：以下は必須とする。

- ➢情報セキュリティ関連規程の説明（採用時，就業時）
- ➢最新の脅威に対する注意喚起（随時）
- ➢個人情報の取り扱いに関する留意事項

３　情報資産管理

３－１　情報資産の管理

３－１－１　情報資産の特定と機密性の評価

当教育委員会事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し，「情報資産管理台帳」に記載する。情報資産の機密性は，以下の基準に従って評価する。

機密性２：極秘	・法律で安全管理が義務付けられている ・守秘義務の対象として指定されている ・限定提供データ（一定の条件を満たす特定の外部者に提供することを目的とする情報）として指定されている ・漏えいすると取引先や児童・生徒に大きな影響がある
機密性１：対外秘	・漏えいすると運営に大きな影響がある
機密性０：公開	・漏えいしても運営にほとんど影響はない

なお，学校毎に適宜，情報資産管理台帳を作成すること。

３－１－２　情報資産の分類の表示

情報資産の機密性は以下の方法で表示する。

・電子データ：保存先サーバーのフォルダー名に表示

・書類：保管先キャビネット，ファイル，バインダーに表示

表示が困難な場合は，「情報資産管理台帳」に機密性評価値を表示する。

３－２　情報資産の持ち出し

情報資産を外に持ち出す場合には，以下を実施する。

・対外秘及び極秘の情報を持ち出す場合には情報セキュリティ運用管理者の許可を得る。

・情報をハードディスク等に保存して持ち出す場合は，データを暗号化する。

・情報をタブレット等に保存して持ち出す場合は，セキュリティロックを設定する。

・USB メモリは，原則禁止とする。業務の都合でやむを得なく必要となる場合は，情報セキュリティ運用管理者の許可を得たうえで利用することとし，大きなタグを付け，ストラップで体やカバンに固定し使用する。

・学校外でネットワークへ接続して極秘又は対外秘の情報資産を送受信することは原則禁止とする。

・情報媒体等を携行するときは，常に監視可能な距離を保つ。

３−３　媒体の処分

３−３−１　媒体の廃棄

対外秘又は極秘の情報資産を廃棄する場合は以下の処分を行う。

書類・フィルム	細断
USB メモリ・HDD・CD・DVD	破壊/完全消去 ※OS による削除・クイックフォーマットは不可

３−３−２　媒体の再利用

極秘又は対外秘の情報資産を保存した媒体を再利用する場合は，以下の処分を行う。

書類	再利用禁止
USB メモリ・HDD・CD-RW ディスク・DVD-RW ディスク	完全消去後再利用 ※OS による削除・クイックフォーマットは不可
CD-R・DVD-R	再利用禁止

３−４　バックアップ

３−４−１　バックアップ取得対象

システム管理者は，以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
校務支援システム	データベース	Windows Server バックアップ	HDD 等
ファイルサーバ	ファイル	ファイルコピー	HDD 等

４　アクセス制御及び認証

４－１　アクセス制御方針

対外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。

・「情報資産管理台帳」の利用者範囲に基づき，利用者の業務・職務に応じた必要最低限のアクセス権を付与する。

・特定の情報資産へのアクセス権が，同一人物に集中することで発生し得る不正行為等を考慮し，複数名に分散してアクセス権を付与する。

４－２　利用者の認証

対外秘又は極秘の情報資産を扱う組織内情報システムは，以下の方針に基づいて利用者の認証を行う。

・利用者の認証に用いるアカウントは，利用者１名につき１つを発行する。

・複数の利用者が共有するアカウントの発行は原則禁止とする。

４－３　利用者アカウントの登録

利用者の認証に用いるアカウントは，情報セキュリティ責任者の承認に基づき登録する。

４－４　利用者アカウントの管理

利用者の認証に用いるアカウントが不要になった場合，情報セキュリティ責任者は，当該アカウントの削除又は無効化を，当該アカウントが不要になる日の翌日までに実施する。

４－５　パスワードの設定

利用者の認証に用いるパスワードは，以下に注意して設定する。

・十分な強度のあるパスワードを用いる。

・他者に知られないようにする。

４－６　教職員以外の者に対する利用者アカウントの発行

当教育委員会の教職員以外の者にアカウントを発行する場合は，情報セキュリティ責任者の承認を得たうえで，秘密保持契約を締結する。

４－７　機器の識別による認証

対外秘又は極秘の情報資産を扱う情報システムに，ネットワーク接続によりアクセスする際の認証方式として，機器の識別による認証を用いる。

４－８　端末のタイムアウト機能

対外秘又は極秘の情報資産を扱う情報システムの端末もしくは情報機器を，アカウントを付与していない者が接触可能な場所に設置する場合は，接続時間制限やタイムアウト等機能を利用する。

４－９　標準設定等

４－９－１　アクセス制御対象情報システム及びアクセス制御方法

情報システム・サービス	アクセス制御方法
校務用 PC	OS のユーザ認証
校務支援システム	アプリケーションのユーザ認証
GIGA スクールタブレット	OS のユーザ認証
GIGA スクールタブレットソフト ・ まなびポケット：ポータルサイト ・ SKY MENU Cloud GIGAスクール版：学習端末支援システム ・ こどもOffice:Office365の小学生向け ・ リアテンダントデジタルドリル：デジタルドリル ・ ソビーゴ：プログラミング ・ ピクチャーキッズ：児童向けペイント・発表	アプリケーションのユーザ認証

４－９－２　利用者アカウント・パスワードの条件

	特権アカウント	一般アカウント
アカウント名	• 推奨：推測困難であるもの ＜禁止アカウント名＞ WindowsOS：administrator，admin • 1 つの特権アカウント名を 2 名以上で共用しない •Guest 用アカウントは基本的に無効化する	•教職員番号
パスワード	＜パスワードに使う文字＞ • 8 文字以上 • 当人の名前，電話番号，誕生日等，他者が推測できるものを使わない	＜パスワードに使う文字＞ • 8 文字以上 • 当人の名前，電話番号，誕生日等，他者が推測できるものを使わない

	• アルファベット大文字･小文字，数字，記号のうち３つを含む • 辞書に含まれる単純な語を使わない ＜パスワードの管理＞ • システムにパスワードポリシー設定機能がある場合は本項の条件を設定する • 原則としてロックアウトのしきい値は 10 回，時間は 6 時間に設定する	• アルファベット大文字･小文字，数字，記号のうち３つを含む • 辞書に含まれる単純な語を使わない ＜パスワードの管理＞ • システムにパスワードポリシー設定機能がある場合は本項の条件を設定する • 原則としてロックアウトのしきい値は 10 回，時間は 1 時間に設定する

５　物理的対策

５－１　諸注意事項

セキュリティ領域では区分にかかわらず以下の点に注意する。

- 複合機，プリンタに原稿，印刷物を放置しない。
- FAX 送信時には誤送信防止のため宛先を複数回確認する。
- ホワイトボードは利用後に消去する。
- 室内での撮影，録音は禁止する。業務上必要な場合は，情報セキュリティ運用管理者の許可を得ること。
- 外線受話時の際に相手が不審な場合は，教職員の個人情報を伝えてはならない。
- 部外者を見かけた場合は用件を確認する。
- ＰＣなどは施錠可能な場所に保管すること。保管する場所は，警備システム管理されている室内とすること。

６　ＩＴ機器利用

６－１　ソフトウェアの利用

６－１－１　標準ソフトウェア

業務に利用するパソコンには，当教育委員会の標準ソフトウェアを導入する。当教育委員会の標準ソフトウェア以外のソフトウェアを導入する場合は，システム管理者の許可を得たうえで導入する。

６－１－２　ソフトウェアの利用制限

システム管理者は，業務に不要な機能等をあらかじめ取除いてシステムを構築する。教職員は，業務に不要なシステムユーティリティやインストールされているソフトウェアを利用しないこと。

＜利用を禁止するソフトウェア＞

- インターネット上で，不特定多数のコンピュータ間でファイルをやりとりできるソフトウェア（ファイル共有ソフト）。
- 不審なベンダーが提供するソフトウェア。
- 正規ライセンスを取得していないソフトウェア。

業務上必要と認められるソフトウェアを新たにインストールする場合は，システム管理者の承認を得たうえでインストールする。

６－１－３　ソフトウェアのアップデート

教職員は，業務で使用するソフトウェアを最新の状態で利用する。ただし，システム管理者が認める場合は，この限りではない。

６－２　ウイルス対策ソフトウェアの利用

６－２－１　ウイルス検知

教職員は，以下の方法でウイルス検知を行う。

- ネットワーク経由で入手するファイルは，自動検知機能を有効にしてウイルス検知を実施する。
- 電子媒体を用いてファイルの受け渡しを行う場合は，媒体内のファイルにウイルス検知を実施する。

６－２－２　ウイルス対策ソフト定義ファイルの更新

教職員は，パソコン・スマートフォン・タブレットに導入したウイルス対策ソフトウェアの定義ファイルを随時更新し最新のものにして運用する。

６－２－３　外部機器の LAN 接続

当教育委員会が管理するパソコン及びサーバー以外の機器を内部 LAN に接続することを禁止する。業務上必要な場合は，システム管理者の許可を得たうえで，当該機器にインストールされているウイルス対策ソフトの定義ファイルを最新版に更新し，当該機器のフルスキャンを実行し，ウイルスが検知されないことを確認してから接続する。

６－２－４　ウイルス対策の啓発

システム管理者および情報セキュリティ管理者は，適宜ウイルスに関する情報を収集し，重大な被害を与えるウイルスに対しては，対応策及び対応に必要な修正プログラムを校内に公開及び通知する。教職員は，感染防止策が通知された場合は，速やかに実施完了すること。

６－３　ＩＴ機器の利用

教職員は，業務に利用するパソコン・タブレット等には，ログインパスワードを設定する。

- ログインパスワードを他者の目に触れる所に書き記さない。
- 屋外で利用する場合は，他者が画面を盗み見可能な環境で利用しない。
- 退勤時又は使用しないときには電源を切り，ノートパソコン・タブレット・スマートフォン・USB メモリ，HDD，CD 等の電子媒体は施錠保管する。

６－４　クリアデスク・クリアスクリーン

６－４－１　クリアデスク

教職員は，対外秘又は極秘の書類及び電子データを保存したノートパソコン，USB メモリ，HDD，CD 等の持ち運び可能な機器や媒体の扱いについて，以下のようにクリアデスクを徹底する。

- 利用時以外には机上に放置しない。
- 離席時には書類を伏せる，又は引き出しに入れる等する。
- 退勤時又は使用しないときには施錠可能な場所に保管する。

６－４－２　クリアスクリーン

教職員は，離席時に以下のいずれかによりパソコンの画面をロックし，クリアスクリーンを徹底する。

- スクリーンセーバー起動時間を **15 分以内**に設定し，パスワードを設定する。
- スリープ起動時間を **30 分以内**に設定し，解除時のパスワード保護を設定する。
- **離席時に［Windows］＋［L］キーを押してコンピュータをロックする。**
- ログオフ状態ではシステム操作画面は非表示に設定する。退勤時又は使用しないときにはパソコンの電源を切る。
- スマートフォン・タブレットを外出先で利用する場合は，他者が盗み見できる環境で利用しない。

６−５　インターネットの利用

教職員は，インターネットを利用する際には以下を遵守する。

６−５−１　ウェブ閲覧

情報セキュリティ責任者は，ウイルス等の悪意のあるソフトウェアに感染するおそれがあると認められる有害ウェブサイトは校内周知して，教職員の閲覧を制限する。教職員は，業務でウェブ閲覧を行う場合は以下に注意する。

- 公序良俗に反するサイトへのアクセスを原則禁止する。
- 不審なサイトへのアクセス及び学校用メールアドレス登録を原則禁止する。
- パスワードをブラウザに保存しない。業務で特定のウェブサービスを利用する場合で，パスワードをブラウザに保存する必要があるときはシステム管理者の許可を得る。
- 業務上，個人情報（メールアドレス，氏名，所属等）を入力する場合は，通信の暗号化，接続先の実在性等を十分に確認したうえで行う。
- 信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き，モバイルコード（クライアントパソコン側で動作するプログラム）を実行しない。

６−５−２　オンラインサービス

教職員は，インターネットで提供されているサービスを業務で利用する場合は，情報セキュリティ責任者の許可を得る。利用する際には以下に注意する。

＜インターネットバンキング・電子決済＞

- インターネットバンキングを利用する際には，自分で設定したブックマークや銀行が提供する専用アプリケーションソフトを用いる。
- 電子メールに記載されているリンクや，他のウェブサイト等に設置されているリンクは，偽サイトへの誘導である可能性があるためアクセスしない。

＜オンラインストレージ＞

- 対外秘又は極秘の情報資産を保存する場合は，情報セキュリティ運用管理者の許可を得る。
- セキュリティポリシーを公表していないサービスの利用は禁止する。
- 不審なベンダーが提供しているサービスの利用を禁止する。

６−５−３　SNS の個人利用

- **当教育委員会の業務に関わる情報の書き込みは行わない。**
- 取引先従業者と SNS 上で私的に交流する場合，双方の立場をわきまえ，社会人として良識の範囲で交流する。
- SNS 用のアプリケーションが提供するセキュリティ設定を行い，アカウントの乗っ取りやなりすましに注意する。
- 使用するパソコン，スマートフォン，タブレット上のデータ，写真，位置情報が，予期せず公開される可能性のあることに注意する。

６－５－４　電子メールの利用

教職員は，業務で電子メールを利用する際には以下を実施する。

＜誤送信防止＞

- メール作成後，必ず目視確認の上送信する。

＜メールアドレス漏えい防止＞

- 同報メール（外部の多数相手に同時に送信するとき）を送信する場合は，宛先（TO）に自分自身のアドレスを入力し，BCC で複数相手のアドレスを指定する。

＜傍受による漏えい防止＞

- 対外秘又は極秘の情報資産を送信する場合は，メール本文ではなく添付ファイルに記載し，ファイルを暗号化して送信する。

＜添付ファイル暗号化の方法＞

- パスワード保護の設定又はパスワード付きの ZIP ファイルにする。

＜クラウド型メールの利用＞

- 業務でクラウド型メールを利用する場合は，システム管理者の許可を得る。
- システム管理者から許可されたパソコン以外で，メールサーバーからのメールの取り出し及びエクスポートを禁止する。

＜禁止事項＞

- 業務に支障をきたすおそれがある使用。
- 私用電子メールサーバーへの接続。
- 受信メールの HTML 表示（テキスト形式に変換して表示すること）。
- プレビューウィンドウの有効化。

６－５－５　ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため，以下の内容に複数合致する場合は十分に注意し，添付ファイルを開く，又はリンクを参照するなどしない。受信した場合は，情報セキュリティ責任者に報告し，情報セキュリティ責任者は校内に注意を促す。

メールのテーマ	知らない人からのメールだが，メール本文のURL や添付ファイルを開かざるを得ない内容 ・新聞社や出版社からの取材申込や講演依頼 ・就職活動に関する問い合わせや履歴書送付 ・製品やサービスに関する問い合わせ，クレーム ・アンケート調査 心当たりのないメールだが，興味をそそられる内容 ・議事録，演説原稿などの内部文書送付 ・VIP 訪問に関する情報 これまで届いたことがない公的機関からのお知らせ 情報セキュリティに関する注意喚起／インフルエンザ等の感

	染症流行情報／災害情報 組織全体への案内 人事情報／新年度の事業方針／資料の再送，差替え 心当たりのない，決裁や配送通知（英文の場合が多い） 航空券の予約確認／荷物の配達通知 IDやパスワードなどの入力を要求するメール メールボックスの容量オーバーの警告／銀行からの登録情報確認
差出人のメールアドレス	フリーメールアドレスから送信されている 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
メールの本文	日本語の言い回しが不自然である 日本語では使用されない漢字（繁体字，簡体字）が使われている 実在する名称を一部に含むURL が記載されている 表示されているURL（アンカーテキスト）と実際のリンク先のURLが異なる（HTML メールの場合） 署名の内容が誤っている ·組織名や電話番号が実在しない ·電話番号がFAX 番号として記載されている
添付ファイル	ファイルが添付されている 実行形式ファイル(exe/scr/cplなど)が添付されている ショートカットファイル(lnkなど)が添付されている アイコンが偽装されている 実行形式ファイルなのに文書ファイルやフォルダーのアイコンとなっている ファイル拡張子が偽装されている／二重拡張子となっている ファイル拡張子の前に大量の空白文字が挿入されている

６−５−６　私有ＩＴ機器・電子媒体の利用

教職員個人が所有するパソコン，タブレット，スマートフォン，携帯電話等のＩＴ機器及びUSB メモリ，HDD，CD 等の電子媒体を業務で利用することは原則禁止とする

7　情報セキュリティインシデント対応ならびに事業継続管理

7－1　対応体制

情報セキュリティインシデント(教育委員会内のみ)が発生した場合には，以下の体制で対応する。※村全体での対応が必要な場合は東海村のセキュリティポリシーに準ずる。

最高責任者	教育長
対応責任者	情報セキュリティ責任者
一次対応者	発見者又は情報セキュリティ運用管理者，システム管理者

7－2　情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合，以下を参考に影響範囲を判断して対応。

事故レベル	影響範囲	責任者
3	個人情報が漏えいしたとき	教育長
2	事業に影響が及ぶとき	情報セキュリティ責任者
1	教職員の業務遂行に影響が及ぶとき	情報セキュリティ責任者
0	インシデントにまでは至らないが，将来においてインシデントが発生する可能性がある事象が発見されたとき	システム管理者

7－3　インシデントの連絡及び報告

レベル１以上のインシデントが発生した場合，発見者は一次対応者または対応責任者に速やかに報告し，指示を仰ぐ。

7－4　対応手順

インシデントを以下のとおりに区分し，それぞれの対応手順を示す。

区分	事件・事故の状況
漏えい・流出	対外秘又は極秘情報資産の漏えい，流出，盗難，紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん，消失，破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

7－4－1　漏えい・流出発生時の対応

事故レベル	対応手順
3	①発見者は即座に一次対応者又は対応責任者に報告する。 ②対応責任者は漏えい等の原因を特定するとともに，二次被害が想定される場合には防止策を実行する。 ③対応責任者は被害者/本人対応を準備する。 ④対応責任者は問い合わせ対応を準備する。

	⑤対応責任者は影響範囲・被害の大きさによっては報道発表の準備を行う。 ⑥対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は茨城県警察本部に届け出る。
2	①発見者は発見次第，対応責任者に報告する。 ②対応責任者は漏えい先を調査し，最高責任者に報告する。 ③情報セキュリティ運用管理者は校内の関係者に周知する。
1	※情報漏えい・流出は全て事故レベル 2 以上

7－4－2　改ざん・消失・破壊・サービス停止発生時の対応

事故レベル	対応手順
3	①発見者は即座に対応責任者に報告する。 ②対応責任者は原因を特定し，応急処置を実施する。 ③情報セキュリティ運用管理者は校内に周知・連絡する。 ④システム管理者は，バックアップ等からシステムの復旧を実行する。 ⑤書類・フィルム等の原本の場合は情報セキュリティ運用管理者が可能な範囲で修復する。 ⑥対応責任者は原因対策を実施する。
2	①発見者は発見次第，対応責任者に報告する。 ②対応責任者は原因を特定し，応急処置を実行する。 ③情報セキュリティ運用管理者は校内に周知・連絡する。 ④システム管理者は，バックアップ等からシステムの復旧を実行する。 ⑤書類・フィルム等の原本の場合は情報セキュリティ運用管理者が可能な範囲で修復する。 ⑥対応責任者は原因対策を実施する。
1	①発見者は発見次第，対応責任者に報告する。 ②対応責任者は原因を特定し，応急処置を実行する。 ③システム管理者は，バックアップ等からシステムの復旧を実行する。 ④書類・フィルム等の原本の場合は情報セキュリティ運用管理者が可能な範囲で修復する ⑤対応責任者は原因対策を実施する
0	発見者は発見次第，発生可能性のあるインシデントと想定される被害を対応責任者に報告する。

7－4－3　ウイルス感染時の初期対応

教職員は，業務に利用しているパソコン，サーバー又はスマートフォン，タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には，以下を実行する。

①ネットワークからコンピュータを切断する。

②情報セキュリティ責任者に連絡する。

③ウイルス対策ソフトの定義ファイルを最新版に更新する。

④ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥駆除後再度ウイルス対策ソフトでスキャンし，駆除を確認する。
⑦情報セキュリティ責任者に報告する。

以下の場合など教職員自身で対応できないと判断される場合は情報セキュリティ責任者に問い合わせる。

- ウイルス対策ソフトで駆除できない。
- システムファイルが破壊・改ざんされている。
- ファイルが改ざん・暗号化・削除されている。

７－４－４　届出及び相談

情報セキュリティ責任者は，インシデント対応後に以下の機関への届け出，報告又は相談を検討する。

＜届出・相談・報告先＞

【独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)】

➢ ウイルスの届出

https://www.ipa.go.jp/security/outline/todokede-j.html
TEL: 03-5978-7518
E-mail：virus@ipa.go.jp

➢ 不正アクセスに関する届出

E-mail：crack@ipa.go.jp
FAX：03-5978-7518

➢ 情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/index.html
TEL:03-5978-7509
E-mail：anshin@ipa.go.jp

【個人情報保護委員会】

➢ 個人データの漏えい等の事案が発生した場合等の対応

①個人データ（特定個人情報に係るものを除く。）の漏えい，滅失又は毀損
②加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい
③上記①又は②のおそれ
漏えい等事案が発覚した場合は，速やかに下記 UR を参照して個人情報保護委員会等に対し，報告すること
https://www.ppc.go.jp/personalinfo/legal/leakAction/
TEL：03-6457-9685
個人情報保護委員会事務局　個人データ漏えい等報告窓口

➢ 特定個人情報の漏えい事案が発生した場合の対応

①番号法違反又は違反のおそれ

番号法違反又は違反のおそれを把握した場合は，速やかに下記 UR を参照して個人情報保護委員会等に対し，報告すること

https://www.ppc.go.jp/legal/rouei/

②重大事態に該当する事案又はそのおそれ

≪重大事態≫

- 情報提供ネットワークシステム等又は個人番号利用事務を処理するために使用する情報システムで管理される特定個人情報が漏えい等した事態
- 漏えい等した特定個人情報に係る本人の数が 100 人を超える事態
- 特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり，かつ閲覧された事態
- 教職員等が不正の目的をもって，特定個人情報を利用し，又は提供した事態

重大事態が発覚した場合は，直ちに下記 UR を参照して個人情報保護委員会等に対し，報告すること

https://www.ppc.go.jp/legal/rouei/

個人情報保護委員会事務局　特定個人情報漏えい等報告窓口

TEL:03-6457-9680

８　個人番号及び特定個人情報の取り扱い

８－１　関係法令・ガイドライン等の遵守

教育委員会は，個人番号及び特定個人情報（以下「特定個人情報等」といいます。）を適正な業務の範囲に於いて利用する場合の取り扱いに関し，「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」（以下「マイナンバー法」といいます。）及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編)」，並びに「個人情報の保護に関する法律」（以下「個人情報保護法」といいます。）及び「個人情報保護委員会のガイドライン」，「東海村個人情報保護条例」の規定を遵守します。

８－２　利用目的

教育委員会は，提供を受けた特定個人情報等を，適正な業務の範囲内に於いて利用します。

(1)特定個人情報等

・報酬，料金，契約金及び賞金に関する支払調書等作成事務

(2)当教育委員会の教職員等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書，保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出，申請・請求事務

・雇用保険・労災保険届出，申請・請求，証明書作成事務

(3) 当教育委員会教職員等の配偶者及び親族等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書，保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出事務

８－３　安全管理措置に関する事項

教育委員会は，特定個人情報等の漏えい，滅失又は毀損の防止その他の個人番号の適切な管理に努めます。

８－４　継続的改善

教育委員会は，特定個人情報等の取り扱いを継続的に改善するよう努めます。

８－５　特定個人情報等の開示

教育委員会は，本人又はその代理人から，当該特定個人情報等に係る保有個人データの開示の求めがあったときは，東海村の規定に基づき対応します。