岸和田市立学校園
情報セキュリティポリシー

平成２５年４月

岸和田市教育委員会

はじめに

■　情報セキュリティとは

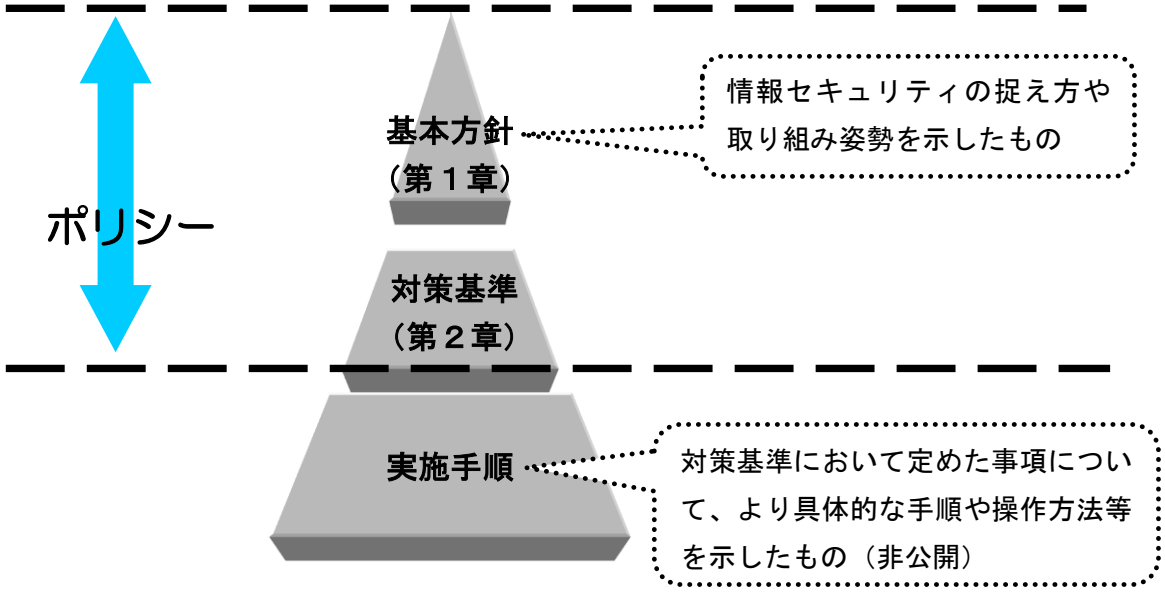
情報セキュリティとは、岸和田市立学校園が保有する情報資産の機密性、完全性、可用性を維持することをいう。

① 機密性
　情報資産を利用する権限のない者に、情報が漏れないようにすること。
② 完全性
　情報が常に完全かつ安全に維持され、改ざんや破壊等がされないようにすること。
③ 可用性
　定められた方法であれば、いつでも情報を利用できるようにすること。

■　構成

情報セキュリティを適正に維持するための方策について、岸和田市立学校園ではそれを３階層による構成とする。そのうち、上位の２階層（基本方針、対策基準）をポリシーと定め、ここに取りまとめる。【下図参照】

【構成イメージ図】



目次

第１章　情報セキュリティ基本方針

１．目的

岸和田市立学校園（以下「学校園」という。）の幼児・児童・生徒をはじめ、その保護者・職員等、学校園に関わるすべての者の財産、プライバシー等の保護、及び、学校園の安定的な運営を図ることを目的として岸和田市立学校園情報セキュリティポリシー（以下「本ポリシー」という。）を制定する。

２．位置づけ

本ポリシーは、学校園の保有する情報資産についての情報セキュリティ対策を、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を実施するうえでの基礎となるものである。

３．定義

本ポリシーにて使用する用語の定義は、以下のとおりとする。

① 電子計算機

ハードウェア（計算機自体の物理的部分）及びソフトウェア（計算機を動作させる手順・命令）で構成するコンピュータ及び周辺機器並びに記録媒体をいう。

② ネットワーク

電子計算機を通信回線で接続することにより、一体として情報の処理を行う情報通信網をいう。

③ 情報システム

電子計算機、及び、ネットワークを利用して行う業務処理の体系（構成機器を含む。）をいう。

④ 情報資産

情報システム及びこれらで取扱う情報をいう。

４．対象範囲

（１）組織の範囲

① 学校園の内部の組織

学校園の内部のすべての組織。ただし、産業高校学務課における庁内ＬＡＮは岸和田市情報セキュリティポリシーの範囲に属するため除く。

② 学校園の外部の組織

学校園の保有する情報資産を取扱う外部の事業者・団体等

（２）人の範囲

上記（１）①に掲げる学校園の全ての職員（非常勤、臨時を含む)、それに準じる者、及び②の組織の従業者であって学校園の情報資産の取扱いに従事している者（以下「職員等」という。）

（３）情報資産の範囲

本ポリシーを適用する情報資産は、次の通りとする。なお、これらの複製も含む。

① 校務用ネットワーク、学習用ネットワーク、情報システム、及び、これらで取扱う電磁的記録媒体

② 校務用ネットワーク、学習用ネットワーク、情報システムで取扱う情報

情報資産の範囲に紙情報を原則含まないが､情報システムから紙等の有体物に出力された情報は、対象範囲内とする。

５．対象範囲外への対応

本ポリシーの対象範囲外とした紙情報についても、本ポリシーの趣旨を尊重しつつ、これまでと同様、当該文書の取扱いを定めた関連法令等に基づいて、引続き適正な取扱いに努めるものとする。

６．本ポリシー及び関連法令等の遵守

（１）職員の責務

① 職員は､情報セキュリティの重要性を認識し､業務の遂行にあたっては､本ポリシーを遵守する義務を負う。また､情報資産の利用や保管等を行う際は､岸和田市個人情報保護条例（平成 12 年条例第 10 号）等関連する法令等を遵守しなければならない。

② 本ポリシーに違反した職員は、生じた結果の重大性及び違反の悪質性等の状況に応じて、地方公務員法等に基づき懲戒処分等の対象になることがある。

（２）外部の事業者・団体等への対応

外部の事業者・団体等に対しても、情報セキュリティの重要性を認知させ、契約書等において本ポリシーの遵守事項及び違反した場合の責任について明確にするものとする。

（３）児童・生徒への対応

児童・生徒に対しても､情報モラル教育の観点より情報セキュリティの重要性を認知させる等、監督・指導するものとする。

７．情報資産に対する脅威

（１）情報資産に対する主な脅威は、次に掲げるものである。

・部外者の侵入
・コンピュータウイルス（コンピュータ・システムに侵入してデータやプログラムなどを壊すソフトウエア）
・不正アクセス（情報資産の不正利用）又は不正操作による情報資産の破壊、盗聴、改ざん、消去
・職員又は外部の事業者・団体等による情報資産の持出し
・アクセス（情報資産を利用すること）のための認証情報（パスワード（本人確認に用いる秘密の文字列）等）の不適切な管理
・搬送中の事故等による情報資産の盗難、紛失
・規定外の端末接続によるデータ漏洩
・地震、落雷、火災等の災害
・事故、故障等による業務の停止

（２）職員等は、上記⑴の脅威に対し認識を深めるとともに、これら以外の脅威についても注意を払わなければならない。

８．運用体制

情報セキュリティ対策の推進、情報セキュリティへの侵害（以下「セキュリティ侵害」という。）に対する迅速な対応を図るための運用体制を確立するものとする。

なお、セキュリティ侵害とは、「７.情報資産に対する脅威」に記述するような脅威が発生した状態をいう。

９．情報資産の分類

情報資産を内容に応じて分類し、その重要度に即した対策を講じるものとする。

10．対策

「７.情報資産に対する脅威」で示した脅威から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ものとする。

① 物理的対策

学校園への不正な立ち入りや、自然災害により起こる破壊等から情報資産を保護するために行う入退室管理等の物理的な対策

② 人的対策

情報資産を取扱う職員等の情報セキュリティに関する権限や責任、運用体制の明確化、本ポリシーの内容を周知徹底するために行う研修等の人的な対策

③　技術的対策

情報資産を不正なアクセス等から適切に保護するため行う情報資産へのアクセス制限、コンピュータウイルス対策ソフトの導入等の技術的な対策

11. 情報セキュリティ対策基準の策定

「10. 対策」で示した対策を講じるにあたって、職員等が遵守すべき事項や判断の基準等を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を実施する上で必要となる一定の基準を示した情報セキュリティ対策基準を策定するものとする。

12. 情報セキュリティ実施手順の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する具体的な対策の方法や手順を定めておく必要がある。そのため、情報セキュリティ対策基準に基づく実施マニュアル（手引き）として、情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、具体的な対策の手順やノウハウ（技術的知識・情報）について記述するものであり、公開することにより学校園運営に重大な支障を及ぼすおそれがあるため、非公開とする。

13. セキュリティ対策の点検と本ポリシーの見直し

日々の情報セキュリティに対する脅威に対応するため、本ポリシーに定める事項及び実施手順に基づく具体的対策の実施状況を定期的に点検する。

また、本ポリシーの内容についても必要に応じて見直し、学校園におけるセキュリティレベルの向上を図るものとする。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針（第１章）に沿った個々の対策を具体化したものであり、学校園における情報セキュリティ対策の基準となるものである。

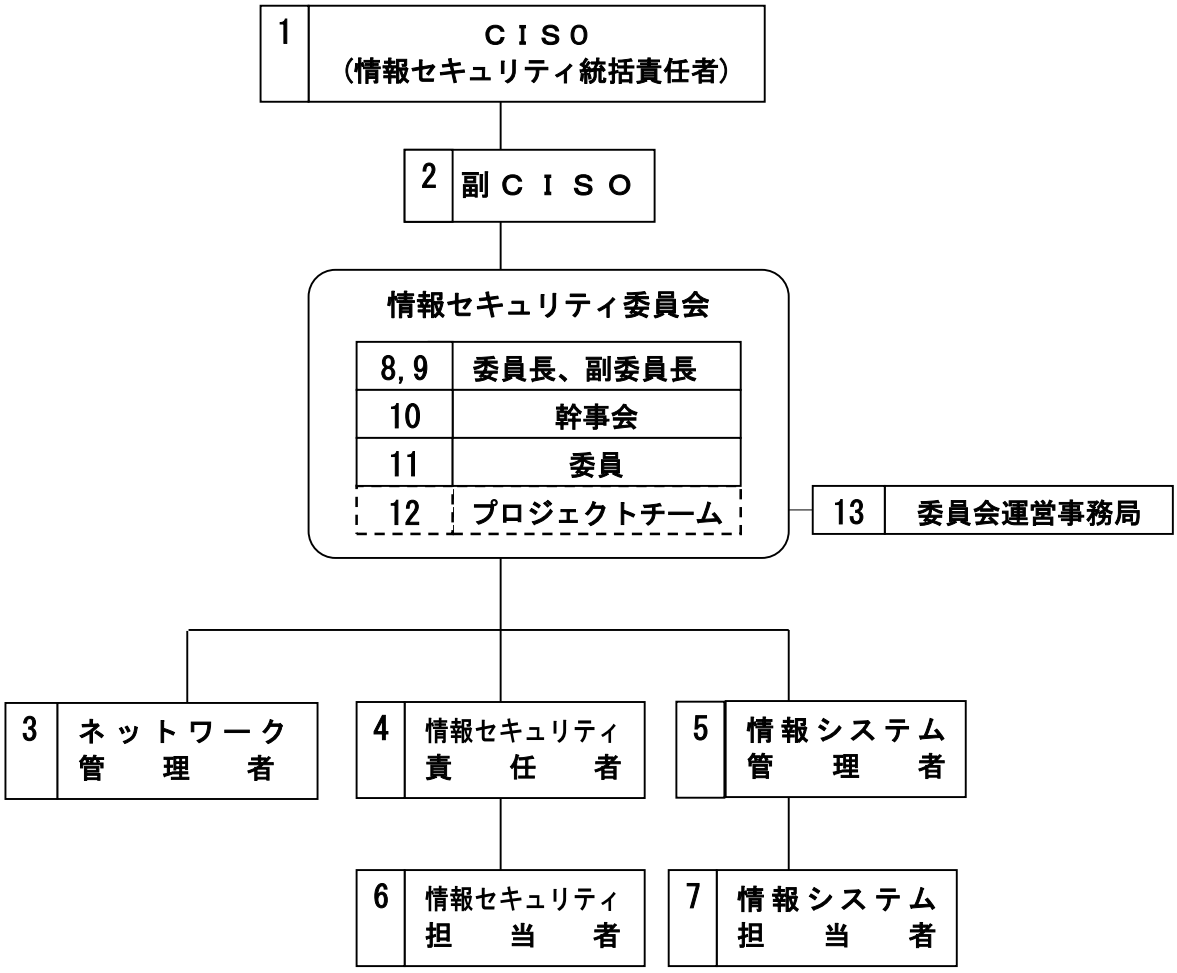
１．組織及び体制

（１）運用体制

情報セキュリティ対策の推進及びセキュリティ侵害への迅速な対応等を行うため、（図１）に示す運用体制を確立する。

また、必要に応じて外部の有識者に助言を求めることができるものとする。

（図１）情報セキュリティ運用体制



（２）情報セキュリティ運用関係者の役割

情報セキュリティ運用体制の中でのそれぞれの役割、責任及び権限の範囲等を明確にするため、役割等一覧を表１に示す。

表１　情報セキュリティ対策運用体制役割等一覧　※項番は、図１の番号と対応しています。

項番	名称	役職等	主な役割等
1	ＣＩＳＯ （情報セキュリティ統括責任者）	教育長	○情報セキュリティに関する全ての責任と権限を有する。 ○情報セキュリティ委員会の委員長を務め、必要に応じて委員を召集し、委員会を開催する。 ○セキュリティ侵害発生時（発生の可能性が高い場合も含む）には、侵害内容や状況等の報告を受け、対策等を指示する。
2	副ＣＩＳＯ	教育総務部長 学校教育部長	○ＣＩＳＯを補佐し、ＣＩＳＯに事故あるときは、その職務を代理する。 ○ＣＩＳＯと協議の上、情報セキュリティ責任者及び担当者、情報システム管理者及び担当者に対し、情報セキュリティに関する指導、助言を行うことができる。 ○セキュリティ侵害発生時には、ＣＩＳＯの指示に従って必要な措置を行う責任と権限を有する。この場合、職員等は副ＣＩＳＯの指示に従わなければならない。
3	ネットワーク管理者	教育総務部 学校管理課長 ※ネットワーク管理者は、学校教育部学校教育課長が補佐できるものとする。	○学校園ネットワークの情報セキュリティに関する責任と権限を有する。
4	情報セキュリティ 責任者	所属長 （校園長）	○学校園の情報セキュリティに関する責任と権限を有し、学校園において、情報セキュリティ対策の指導や本ポリシーの普及及び遵守の徹底を図る。 ○所管する情報資産について、情報資産管理台帳及び情報セキュリティ実施手順の作成、管理を行う。 ○セキュリティ侵害発生時には、情報セキュリティ委員会に侵害内容や状況等を報告し、所属内に対処を指示する。
5	情報システム管理者	所属長 （校園長）	○学校園の情報システムのセキュリティ対策について全てを管理する責任と権限を有する。 ○学校園の情報システムの情報セキュリティ実施手順を作成する。
6	情報セキュリティ 担当者	教頭 （幼稚園においては教頭または主任等）	○情報セキュリティ責任者の指示の下、学校園の情報セキュリティ対策を実施する。 ○セキュリティ侵害発生時には、速やかに情報セキュリティ責任者へ侵害内容や状況等の報告を行い、責任者の指示の下、適切な対処を行う。
7	情報システム担当者	情報システム管理者が指名した者	○学校園の情報システムに関して、情報システム管理者の指示に従い、開発、運用、更新等の作業を行う。

※岸城、東光、城北の各幼稚園は、６・７を担当職員が兼務してもよい。

（３）セキュリティ統括組織

岸和田市立学校園情報セキュリティ委員会が、学校園の情報セキュリティについて、統括的な管理を行う。同委員会の中でのそれぞれの役割、責任及び権限の範囲等を明確にするため、同委員会の役割等一覧を表２に示す。

【岸和田市立学校園情報セキュリティ委員会の所掌事務】

① 学校園の情報セキュリティに関する重要事項についての協議及び決定に関すること。
② 本ポリシーの制定及び改正、運用、普及並びに教育に関すること。
③ セキュリティ侵害についての情報収集及び侵害発生の予防に関すること。
④ セキュリティ侵害時の対応に関すること。
⑤ ポリシーとの適合性点検の実施及びその結果を基に行う改善策の協議に関すること。

表２　岸和田市立学校園情報セキュリティ委員会役割等一覧

※項番は、図１の番号と対応しています。

項番	名称	役職等	主な役割等
8	委員長	ＣＩＳＯ（情報セキュリティ統括責任者＝教育長）が兼任	○委員会を統括する。
9	副委員長	副ＣＩＳＯ（副情報セキュリティ統括責任者＝教育総務部長、学校教育部長）が兼任	○委員長を補佐し、委員長に事故あるときは、その職務を代理する。
10	幹事会	教育総務部 　総務課長 　学校管理課長 学校教育部 　学校教育課長 　人権教育課長 企画調整部 　情報政策課長 産業高校 　総務課長	○運営事務局と連携し、委員会に付議する事項についての、調整等を行う。 ○緊急を要するセキュリティ侵害の発生時には、委員長と対応策等についての協議を行う。
11	委員	幼稚園長代表 小学校校長会代表 中学校校長会代表 岸和田市立 　産業高等学校長	○情報セキュリティに関する重要事項について協議する。 ○セキュリティ侵害及びセキュリティに関する点検の結果に対する改善策を協議する。 ○セキュリティ侵害発生時には、必要に応じて、委員長と対応策等についての協議を行う。

項番	名称	役職等	主な役割等
12	情報セキュリティポリシープロジェクトチーム	本ポリシーの改訂等を行うために委員長が指名した者(学校教育部学校教育課指導主事、人権教育課指導主事、教育総務部学校管理課員、総務課員、企画調整部情報政策課員)	○必要に応じて委員会の指示の下設置され、本ポリシーを維持させるために改訂等を行う。
13	運営事務局	学校教育部 学校教育課	○本ポリシーの運用、普及及び教育を推進する。 ○委員会の決定事項を推進する。 ○セキュリティ侵害に関する情報を収集し、必要に応じて委員会へ報告する。 ○情報セキュリティ実施手順の維持、管理を行う。

２．情報資産の分類及び管理

（１）情報の重要度による分類

情報セキュリティ責任者（校園長）は、各々が所管する情報資産について適正な取扱いを図るため、情報の重要度により表３に示す分類を行うものとする。

表３　情報の分類

重要度	情報の内容
A	○個人情報及びセキュリティ侵害が、幼児・児童・生徒及びその保護者等の生命、財産、プライバシー等へ重大な影響を及ぼす情報
B	○セキュリティ侵害が、学校園における事務の執行に重大な支障を及ぼす情報
C	○セキュリティ侵害が、学校園における事務の執行に軽微な支障を及ぼす情報

（２）情報資産管理台帳の作成

情報セキュリティ責任者(校園長)は、学校園における情報資産の管理を円滑に行うため、各情報システムに関連づけた目録を作成しなければならない。

なお、情報資産管理台帳の記載内容については、必要に応じて更新を行うものとする。

（３）情報資産の管理

情報セキュリティ責任者（校園長）は、所属内における情報資産について、（１）の重要度に応じた適切な対策を講じることにより管理しなければならない。

なお、具体的な対策については、後述の物理的対策、人的対策、技術的対策、システム開発・運用・保守、緊急時対応計画が記述された実施手順書を作成しなければならない。

３．物理的セキュリティ対策

（１）セキュリティ区画の分類

情報セキュリティを確保するために、その情報資産が使用・保管できる空間を限定し、管理水準を定め表４に示すセキュリティ区画を設定する。

表４　セキュリティ区画

区画の区分	区画の管理水準（例）	情報資産の例（小中）	
		使用	保管
L4	常時施錠され、厳重な入退室管理、室内での作業管理、その他厳重な管理空間 （例）使用時以外施錠しているサーバーラック	サーバー等 重要度ＡＢＣの情報にアクセスできる機器	サーバー等 重要度ＡＢＣの情報にアクセスできる機器
L3	常時施錠され、管理者の明示の許可を受けた少数の者だけがアクセスできる空間 （例）施錠されている金庫、職員室の施錠されている事務机、施錠されているロッカー	該当無し	重要度Ａの情報を保存した媒体
L2	職員の監視下で、管理者の明示の許可を得て入退室する空間 （例）職員室、事務室、保健室、校長室	重要度ＡＢＣの情報にアクセスできる機器	重要度ＡＢＣの情報にアクセスできる機器
L1	職員の監視下で、おもに幼児・児童・生徒が入退室する空間、かつ、不在時に施錠された空間 （例）教室、特別教室、図書室、会議室	重要度Ｃの情報を保存したパソコン 重要度Ｃの情報にアクセスできる機器	重要度Ｃの情報を保存したパソコン 重要度Ｃの情報にアクセスできる機器
L0	不特定の人が比較的自由に出入りする空間 （例）中庭、ピロティ、廊下等	該当なし	該当なし

＊ 複数の重要度にわたる情報を保存しているときは、上位の重要度を適用すること。

＊ Ｌ０区画にパソコン等を設置する場合は、盗難防止用チェーン等で対策すること。その際パソコン等は、区画Ｌ１に相当するものとする。

＊ 幼稚園のパソコン等は、盗難防止用チェーン等で対策すること。その際パソコン等は、区画Ｌ３区画に相当するものとする。

（２）区画図

情報セキュリティ責任者（校園長）は、表４で定めた区画の区分に従い、所管の事務室等の区画図を作成しなければならない。

（３）情報資産以外の管理

情報セキュリティ責任者（校園長）は、紙情報などの管理についても、セキュリティ区画の分類による保管に努めなければならない。

（４）サーバーの設置

① 情報システム管理者（校園長）及びネットワーク管理者（学校管理課長）は、サーバーを設置する場合は火災、水害、落雷、磁界、振動等の影響を受けにくい場所に設置すること。

② 情報システム管理者（校園長）及びネットワーク管理者（学校管理課長）は、サーバーの電源について落雷等による過電流対策を施し、停電時には機器が正常に停止するまでの間の十分な電力を供給しうる予備電源を備えつけること。

４．人的セキュリティ対策

（１）職員の責務

① 職員は、本ポリシー及び情報セキュリティ実施手順に定められている事項を遵守すること。

② 職員は、端末機及びサーバーの操作は、原則として情報システム管理者（校園長）が定める運用時間内に行うこと。

③ 職員は、業務目的以外での情報システムへのアクセス、及びこれを利用したメールの送受信を行わないこと。

④ 職員は、情報システムの使用を終了し、又は中断する場合は、適切な操作をすること。

⑤ 職員は、情報システム管理者（校園長）の許可を得ず、情報システムにソフトウェアのインストール（オペレーティングシステムやアプリケーションをコンピュータで使えるようにするために、記録し設定すること。）及び周辺機器等を接続しないこと。

⑥ 職員は、情報システムを使用するにあたり、外部に情報が漏れることのないよう必要な対策を講じること。

⑦ 職員は、情報セキュリティ責任者（校園長）の許可を得ず、情報資産を学校園外に持ち出さないこと。

（２）外部の事業者・団体等の管理

① 情報セキュリティ責任者（校園長）は、情報資産を取扱うことが予想される外部の事業者・団体等と契約等を締結する際には、必要に応じて、次の事項を追加すること。

・ソフトウェア及び周辺機器等の持込並びに持出に関する事項

・電子情報の授受及び搬送に関する事項
・委託を受けた事業者における電子情報の保管及び廃棄に関する事項
・名札等身分証明の着用に関する事項
・立入検査に関する事項
・その他情報資産の保護に関し必要な事項

② 情報セキュリティ責任者（校園長）は、所管する情報システムに係る開発等の業務を外部の事業者に委託し、当該事業者の従業員等の派遣を受けるときは、必要に応じてその代表及び本人の双方から秘密保持等のための情報資産の適正な取扱いを遵守させること。

（3）パスワードの管理

① パスワードは、口外並びにメモするなどにより、他に漏らさないこと。
② パスワードは、情報システムに記憶させないこと。
③ パスワードは、可能な限り定期的に変更すること。
④ 他人が容易に推測できるようなパスワードを使用しないこと。

（4）研修

① ＣＩＳＯ（情報セキュリティ統括責任者＝教育長）は、職員に対し、権限と責任に応じた次の事項について情報セキュリティポリシーに関する研修を実施すること。
・本ポリシーの周知徹底
・関連法令等の理解
・関連する実施手順の理解（関連する部門対象者への教育）
・セキュリティ事故対策の研修

② 職員は、定められた研修に参加し、本ポリシー及び実施手順を理解し、情報セキュリティ上の問題を生じさせないようにすること。

５．技術的セキュリティ対策

（1）コンピュータウイルスからの保護

① ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、情報システムにコンピュータウイルス対策ソフトを導入するなどの適切なウイルス対策を講じること。
② ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、コンピュータウイルス対策ソフトの定義ファイル(コンピュータウイルスに感染したファイル等を収録したファイル。ウイルス対策ソフトがウイルス等を検出するのに使う。）を、常に最新のものに更新すること。
③ ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、コンピュータウイルス感染時の対策手順を定めること。

（２）ネットワークの管理

①　ネットワーク管理者（学校管理課長）は、ネットワークにおける情報及びネットワークを支える基盤（システムを有効に機能させるために必要となる設備）の保護を確実にするため、ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること。

②　ネットワーク管理者(学校管理課長)は､ネットワークに接続したサービス及び情報を、許可されていないアクセスから確実に保護すること。

③　ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、公衆ネットワークを通過するデータの機密性及び完全性を保護するため､並びにネットワークに接続した情報システムを保護するために、必要に応じて、特別な管理策を確立すること。

④　ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、無線による通信を導入する場合、暗号化及びＭＡＣアドレス（ネットワークに接続する機器が持つ固有の番号）による制御等の対策を講じること。

（３）機器及び媒体の取扱い

①　情報セキュリティ責任者（校園長）及び情報システム管理者（校園長）は、コンピュータの取外し可能な記録媒体（CD-ROM、フロッピーディスク、USB フラッシュメモリー、ハードディスク、磁気テープ等）及び情報システムから印刷された文書の管理手順を定めること。

②　情報セキュリティ責任者（校園長）及び情報システム管理者（校園長）は、機器及び媒体の廃棄、修理にあたり情報の消去等について手順を定めること。

（４）ホームページ（Web）サーバーの保護

ホームページなど公開のために構築している情報システムの管理者は、情報の完全性を保護するように努めなければならない。

（５）情報の交換

①　情報セキュリティ責任者（校園長）及び情報システム管理者（校園長）は、他の組織との間で交換される情報の紛失、改ざん又は誤用を防止するため、他の組織との間の情報及びソフトウェアの交換手順について合意を取り交わすこと。なお、重要性に応じて契約又は協定等を締結すること。

②　情報セキュリティ責任者（校園長）は、電子メールにおけるセキュリティ上のリスクを回避するよう努めること。

（６）アクセス権限（情報資産を利用する権限）の管理

ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、情報資産を不正なアクセスから保護するためにアクセス権限の管理にあたり、次の事項を実施しなければならない。

① 利用者ごと、又は利用者からなるグループごとに対するアクセス権限の割り当て及び使用を制限し、管理すること。
② 利用者ごと、又は利用者からなるグループごとに対するアクセス制御に関するルールを定めること。
③ アクセス制御に関するルールは、明確に許可していなければ原則的に禁止するという前提に基づくこと。
④ 個人情報を含む特に重要な情報に関しては、個別のアクセス制御を考慮すること。
⑤ すべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続を定めること。
⑥ アクセス権限の割り当てを定期的に検査して、許可されていないアクセス権限は速やかに削除すること。
⑦ 利用者に対し、アクセス制御の必要性を周知徹底すること。

（7）パスワードの管理

ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、情報資産を不正なアクセスから保護するためにパスワードの管理にあたり、次の事項を実施するよう努めなければならない。

① 利用者認証については、ユーザＩＤ（ユーザー名）及びパスワード又は物理的認証手段を設定すること。
② ユーザＩＤ（ユーザー名）及びパスワード又は物理的認証手段の割り当ては、正規の手続によって管理すること。
③ 操作が誰の責任によるものかを追跡できるように、認証の記録を取ること。また、認証に失敗した試みについても記録するよう努めること。
④ 推測されにくいパスワードであることを確実にするために、有効な機能を提供するよう努めること。
⑤ 情報システムへログインするための手順は、一定回数以上の認証失敗後は権限を停止するなど、許可されていないアクセスの恐れを最小限に抑えるように設計するよう努めること。

（8）ネットワークのアクセス制御

ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、情報資産を不正なアクセスから保護するためにネットワークのアクセス制御にあたり、次の事項を実施しなければならない。

① 指定された経路以外の経路を、利用者が選択できないようにすること。
② 遠隔地からの利用者のアクセスには、認証を行うこと。
③ 遠隔コンピュータシステムへの接続は、認証されること。
④ ネットワーク機器のポート（パソコンと周辺機器を接続する機構部分）へのアクセスは、セキュリティを保つように制御されること。
⑤ 不正なアクセスが行われないよう、ネットワーク内に制御策を導入し、情報サービス、

利用者及び情報システムを分割するよう考慮すること。

⑥　外部の事業者・団体等のネットワークサービスを使用する場合は、使用するサービスのセキュリティの特質について明確な説明を受け、必要があれば対策を行うこと。

（9）管理者のアクセス制御

ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、情報資産を不正なアクセスから保護するために管理者のアクセス制御にあたり、次の事項を実施しなければならない。

①　システムユーティリティ（情報システムの管理をするためのプログラム）の使用は制限し、厳しく管理すること。

②　技術支援要員（オペレータ、ネットワーク技術者、システムプログラマ、データベース管理者等）は、その操作が誰の責任によるものかを追跡できるように、各個人の利用者ごとに識別できるもの(利用者 ID 等)を保有すること。

③　許可されていない者によるアクセスを防止するため、管理者権限によるログインは管理者権限が必要な操作を行うときだけとし、短時間の離席であっても管理者権限をログアウトすること。

(10) システムアクセス及びシステム使用状況の監視

ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、情報資産を不正なアクセスから保護するためにシステムアクセス及びシステム使用状況の監視にあたり、次の事項を実施しなければならない。

①　利用者が明確に許可された操作を実行するために、情報処理設備の使用状況を監視する手順を確立すること。

②　監視の結果は記録し、定期的に確認すること。

③　情報システムが直面する脅威を把握し、その対策を講じるために、監視記録を検証すること。

④　記録の正確性を保証するためにコンピュータの時計は正しく設定すること。

(11) 情報機器の外部使用

ネットワーク管理者（学校管理課長）及び情報セキュリティ責任者（校園長）は、原則としてコンピュータ等の情報機器を外部に持ち出すことができないよう、実施手順に記述しなければならない。

６．情報システムの開発及び運用・保守

情報システム管理者（校園長）は、情報システムの開発及び運用・保守を行う場合、次の事項を実施しなければならない。

（1）システム開発

①　岸和田市情報システム委員会設置規程（平成 12 年庁達第８号）で定める情報システム

導入計画書を提出し、情報セキュリティが確保されていること。また、すでに稼動している情報システムへの影響の有無を確認すること。

② 業務用ソフトの選定や評価にあたっては、セキュリティ対策を考慮すること。

③ 許可を受けた者以外、プログラムやシステムファイルの作成、更新及び削除を行わせないこと。

④ ベンダー（製品を販売する会社）又は外部の事業者・団体等が支援のために情報システムにアクセスするときは、承認と監視を行うこと。

⑤ データの誤入力を防止する機能を装備すること。また、異常データの入出力を防止する機能を装備すること。

⑥ パソコンで稼動する情報システムは、以下の点を考慮すること。

- 利用者の権限に応じたアクセス制御が実施されたパソコンを使用すること。
- 基本ソフトやアプリケーションソフトは、信頼されるベンダーによって維持、サポートされているものを使用すること。

⑦ 情報システムのテストは、できる限り本番データに近い内容と量で行うこと。ただし、本番のデータベースを直接使用しないこと。

⑧ 情報システムのテストであっても、本番と同等のアクセス制御を行うこと。

⑨ 情報システムのテスト結果の確認は、開発者と利用者の双方で行うこと。

（2）システム運用

① 情報システム管理者（校園長）は、システム構築にあたり作成したドキュメント（機能の仕様や使い方などを解説した資料や文書）類を適正に管理し保管すること。

② 情報システム管理者（校園長）は、情報処理設備のセキュリティを保った運用を確実にするため、実施手順に基づいた操作手順書を作成すること。

③ 情報システム管理者（校園長）は、情報処理の完全性及び可用性を維持するため、データ及びソフトウェアのバックアップ（データの写しを取って保存すること）は、定期的に取得し検査すること。

④ 情報システム担当者（校園長が指名した者）は、自分の作業の記録をとること。

⑤ 情報システム担当者（校園長が指名した者）は、セキュリティ侵害発生時は情報システム管理者（校園長）に報告を行い、実施手順に従い適切な処置をとること。

⑥ ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、セキュリティの維持に必要な情報（アクセスログ（情報資産を利用した記録）等）を適切に管理し、必要に応じ分析すること。

⑦ ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、設備の管理に関する責任及び手順を確立すること。

⑧ ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、セキュリティ侵害発生時において学校園の幼児・児童・生徒等へのサービスの影響を最小限にするよう対策をとること。

⑨ ネットワーク管理者（学校管理課長）及び情報システム管理者（校園長）は、情報システムの稼動やジョブ（コンピュータでの処理作業の単位。）の実行、パラメータ（ソフト

ウェアを実行したりプログラム内で関数を呼び出したりするときに、その動作を指定するために外部から与える設定値。）の設定、データのバックアップやログ（コンピュータの利用状況やデータ通信の記録。）の取得は可能な限り自動化し、人手による介入を削減すること。

⑩　相互監視の観点から、情報システムの操作は複数人で行うこと。ただし、セキュリティ侵害発生時などの緊急時はこの限りでない。

（3）システム変更

①　情報システム管理者（校園長）は、情報処理設備及び情報システムの変更について、その記録を適切に管理すること。また、情報セキュリティに影響を及ぼすシステム変更についてはＣＩＳＯ（情報セキュリティ統括責任者＝教育長）に報告すること。

②　情報システム管理者（校園長）は、情報システムの変更に際し、外部委託を行うときは契約書等において本ポリシーを遵守する義務を課すこと。

7．緊急時の対応

情報資産に対するセキュリティ侵害が発生した際に、迅速かつ円滑に必要な措置を実施するため、次の事項を定める。

（1）侵害への対応

①　職員等は、侵害の発生もしくは侵害の可能性が高まっている状態を発見した場合、当該情報資産を所管する情報セキュリティ責任者（校園長）へ直ちに報告すること。

②　情報セキュリティ責任者（校園長）は、侵害に関する情報を取りまとめ、ＣＩＳＯ（情報セキュリティ統括責任者＝教育長）へ報告すること。また、必要に応じて、危機管理課との情報共有に努めるものとする。

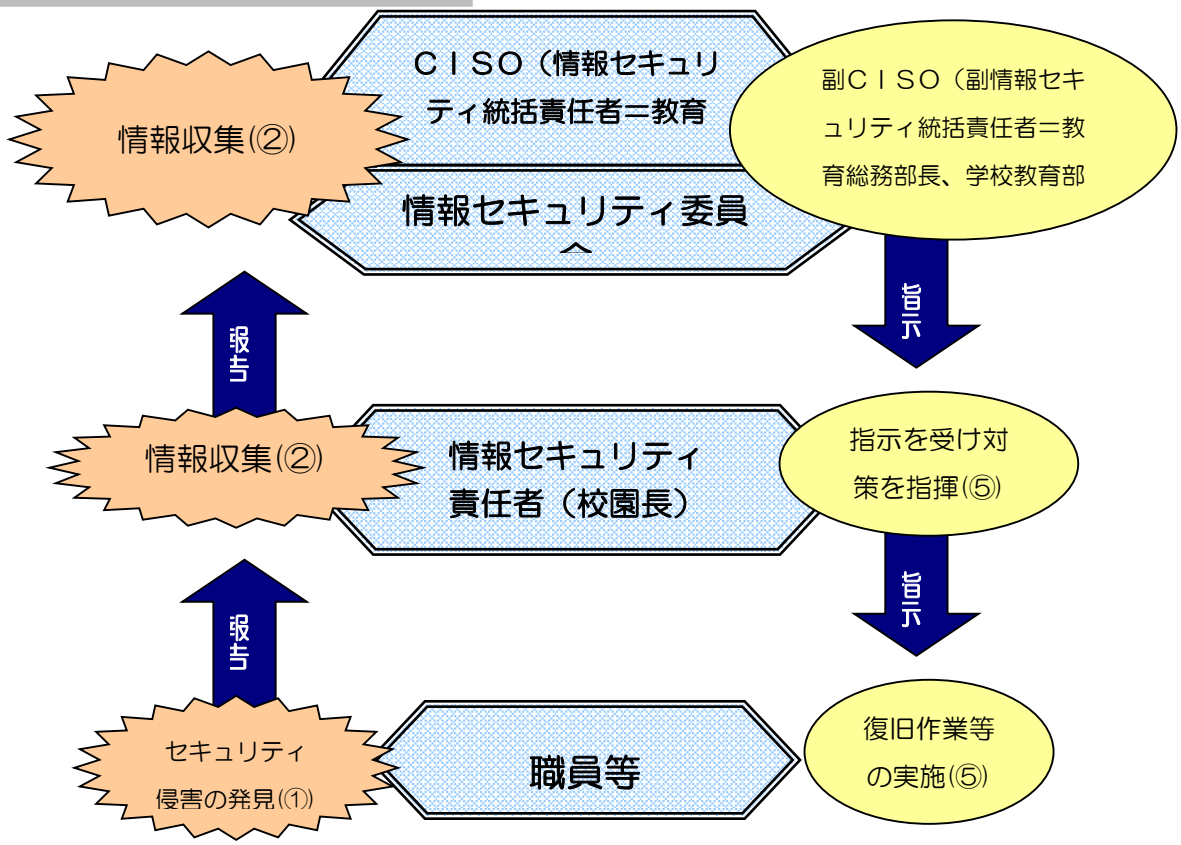
③　ＣＩＳＯ（情報セキュリティ統括責任者＝教育長）は、侵害の対象となった情報資産の重要度や侵害により生じた結果の重大性等に応じて委員会を開催し、対処方法の検討や外部への報告についての協議を行うこと。

なお、委員会は、必要に応じて危機管理監に意見を求めるものとする。

④　ＣＩＳＯ（情報セキュリティ統括責任者＝教育長）は、侵害内容や状況等の報告を受けた後、情報セキュリティ責任者（校園長）に対し速やかに指示を行い、復旧や被害の拡大防止に努めること。

⑤　職員等は、情報セキュリティ責任者（校園長）の指示に従い、復旧や被害の拡大防止に努めること。

（図２）侵害への対応フロー



（２）再発防止

①　情報セキュリティ責任者（校園長）は、セキュリティ侵害への対応を完了させた後、その原因を究明し、結果を基にして、速やかに再発防止策を講じること。

②　情報セキュリティ責任者（校園長）は、セキュリティ侵害の発生から再発防止策の実施までの一連の記録を収集し、ＣＩＳＯ（情報セキュリティ統括責任者＝教育長）へ報告すること。

③　職員等は、情報セキュリティ責任者（校園長）の指示に従い、再発防止に努めること。

８．適合性

（１）法令等の遵守

職員等は、職務の遂行において情報資産を使用する場合、関係する法令、及び岸和田市教育委員会が策定したネットワーク・コンピュータ運用ルール等を遵守しなければならない。

（２）点検等

①　情報セキュリティ責任者（校園長）は、本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について点検を行うこと。また、情報セキュリティ責任者（校園長）

はこれをとりまとめ、岸和田市立学校園情報セキュリティ委員会に報告を行うこと。

② 岸和田市立学校園情報セキュリティ委員会は、新たに必要な対策が発生した場合、又は点検の結果を踏まえ岸和田市立学校園情報セキュリティ委員会において本ポリシーの実効性を評価し見直しが必要となった場合、本ポリシーの見直し内容及び時期についての決定を行い、更新すること。

③ 岸和田市立学校園情報セキュリティ委員会は、更新に際して必要に応じて情報セキュリティポリシープロジェクトチームを設置すること。

補足　用語解説

CD-R(Compact Disk Recordable)	一度だけ書き込み可能なCDを利用した記録媒体
ＣＩＳＯ(Chief Information Security Officer)	最高情報セキュリティ管理責任者
MACアドレス(Media Access Control Address)	LANボードなど、ネットワークに接続する機器が持つ固有の番号 １つのMACアドレスを持つLANカードは世界中に１つしか存在しない
アクセス(access)	(情報資産を)利用すること
アクセス権限	(情報資産を)利用する権限
アクセスログ	(情報資産を)利用した記録
アプリケーションソフト	ワープロや表計算、データベースなどのソフトウエアの総称
コンピュータウイルス(computer virus)	第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能のいずれか一つ以上を有するもの
サーバー(server)	サービスを提供するソフトウエア又はハードウエア
システムユーティリティ	情報システムの管理をするためのプログラム
ソフトウエア(software)	プログラム、情報等の総称
ネットワーク(network)	通信のために用いられる装置及び回線
ハードウエア(hardware)	コンピュータ機器の総称
ハードディスク(hard disk)	固定ディスクを利用した記憶装置
パスワード(password)	利用者を認証するための符号
バックアップ(backup)	プログラム、情報等と同一の内容を別の媒体に記録すること
ベンダー(vender)	製品を販売する会社
モバイルコンピュータ(mobile computer)	携帯可能な情報システム
リスク(risk)	情報システムが侵害を受ける危険性
ログアウト(logout)	アクセスを終了すること
ログイン(login)	アクセスを開始すること
磁気テープ	磁気テープを利用した記憶装置
無線LAN	LANの一部又は全部の回線を無線化したもの
不正アクセス	不正アクセス禁止法第3条第2項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセス