上勝町情報セキュリティポリシー

平成１５年　９月１８日　策定
平成２６年１１月　４日　改正
平成３０年１０月　１日　改正

上　　勝　　町

【改 正 履 歴】

改正（決裁）年月日	版番号	内容（改正理由）
平成１５年　９月１８日	第 1.0 版	初版発行
平成２６年１１月　４日	第 2.0 版	一部改正（組織体制及び各運用状況の変更）
平成 30 年 10 月　１日	第 3.0 版	全部改正

＜ 目　次 ＞

序　情報セキュリティポリシーの構成

情報セキュリティポリシーは、上勝町が所掌する情報資産に関する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を総称する。情報セキュリティポリシーは、上勝町が所掌する情報資産に関する業務に携わる全職員、非常勤、臨時職員（以下、「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

① 情報セキュリティ基本方針
② 情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順

第１章　情報セキュリティ基本方針

1. 目　的

上勝町の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、住民の財産、プライバシー等を守るためや事務の安定的な運営のためにも必要不可欠である。ひいては、このことが上勝町に対する住民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるＩＴ革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっている。上勝町が電子自治体を構築するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、上勝町の情報資産の機密性、完全性及び可用性(注)を維持するための対策（情報セキュリティ対策）を整備するために上勝町情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については上勝町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際化標準機構(ISO)が定めるもの（ISO7498-2：1989）

機密性(confidentiality)：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性(integrity)　　：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性(availability)　：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

2. 定　義

（１）　ネットワーク

上勝町における本庁舎、出先機関及び教育委員会（小学校・中学校を除く）の電子計算機等を相互に接続するための通信網、その構成機器（ハードウエア及びソフトウエア）及び記録媒体で構成され、処理を行う仕組みをいう。

（２）　情報システム

業務系ネットワークの電子計算機（基幹系・情報系におけるネットワーク、ハードウエア及びソフトウエア）及び記録媒体で構成され、処理を行う仕組みをいう。

（３）　情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

なお、情報資産には紙等の有体物に出力された情報も含むものとする。

（４）　情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

3. 情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、上勝町が所掌する情報資産に関する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頂点に位置するものである。

したがって、上勝町長をはじめとして上勝町が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行にあたって情報セキュリティポリシーを遵守する義務を負うものとする。

4. 情報セキュリティ管理体制

上勝町の情報資産について、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ものとする。必要な体制、権限、責任等については、情報セキュリティ対策基準にて定める。

5. 情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6. 情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（1） 部外者の侵入による機器または情報資産の破壊・盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊・盗聴・改ざん・消去等

（2） 職員等及び外部委託事業者による機器または情報資産の持出、誤操作、アクセスのための認証情報またはパスワードの不適切管理、故意の不正アクセスまたは不正操作による破壊・盗聴・改ざん・消去等、搬送中の事故等による機器または情報資産の盗難、規定外の端末接続によるデータ漏洩等

（3） コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

7. 情報セキュリティ対策

上記６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ずるものとする。

（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への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（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定め、全ての職員等及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（3） 技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

8. 情報セキュリティ対策基準の策定

上勝町の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準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行う上で必要となる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ものとする。

9. 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基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、各所属の長等が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティポリシー（情報セキュリティ対策基準）及び情報セキュリティ実施手順は、公にすることにより上勝町の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

10. 情報セキュリティ監査及び自己点検の実施

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、必要に応じて定期的に監査及び自己点検を実施する。

11. 評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

第２章　上勝町行政全般における情報セキュリティ対策基準

上勝町行政全般における情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための上勝町行政全般の情報資産に関する情報セキュリティ対策の基準である。

１．行政機関の範囲

この情報セキュリティポリシーが対象とする行政機関の範囲は、町長，教育委員会，選挙管理委員会，監査委員，農業委員会，固定資産評価審査委員会及び議会とする。ただし、小学校・中学校は対象外とする。

なお、教育委員会における教育のために用いるネットワーク及びシステム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

２．管理体制

（１） 体制

- 最高情報統括責任者（ＣＩＯ）　……　副町長
- ネットワーク管理者　……　総務課長
- 情報セキュリティ管理者　……　総務課長
- 情報システム担当者　……　総務課情報担当
- 情報セキュリティ各課責任者　……　課長等
- 監査責任者　……　総務課長

（２） 権限・責任

ア　最高情報統括責任者（ＣＩＯ）

上勝町副町長を、上勝町における全てのネットワーク、情報システム・情報資産・情報セキュリティに関する最終決定権限及び責任を有する最高責任者（ＣＩＯ：最高情報統括責任者）とする。

イ　ネットワーク管理者

(ア)　上勝町総務課長を、最高情報統括責任者直属のネットワーク管理者とする。ネットワーク管理者は、最高情報統括責任者を補佐しなければならない。

(イ)　ネットワーク管理者は、上勝町の全てのネットワークにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

(ウ)　ネットワーク管理者は、上勝町全てのネットワークにおける情報セキュリティに関する権限及び責任を有する。

(エ)　ネットワーク管理者は、情報システム担当者に対して上勝町全てのネットワークにおける情報セキュリティに関する指導及び助言を行う権限を有する。

(オ)　ネットワーク管理者は、上勝町の情報資産に対する侵害または侵害の恐れのある場合には、最高情報統括責任者の指示に従い、最高情報統括責任者が不在の場合には自らの判断に基づき必要かつ十分な全ての措置を行う権限及び責任を有する。

この場合、全ての職員等はネットワーク管理者の指示に従わなければならない。

(カ)　ネットワーク管理者は、上勝町の全てのネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持、管理を行い、緊急時対応計画に基づく訓練を実施する。

ウ　情報セキュリティ管理者

(ア) 上勝町総務課長を、情報セキュリティに関する権限及び責任を有する情報セキュリティ管理者とする。

(イ) 情報セキュリティ管理者は、各所属における情報セキュリティポリシーの遵守に関する権限と責任を有する。

(ウ) 情報セキュリティ管理者は、庁内にて稼働している情報システムの追加・変更の承認等を行う。

(エ) 情報セキュリティ管理者は、情報資産に対する侵害または侵害の恐れのある場合には、最高情報統括責任者へ速やかに報告を行い、指示を仰がなければならない。

エ 情報システム担当者

情報システム担当者は、担当する情報システムに関して、ネットワーク管理者、情報セキュリティ管理者の指示等に従い、開発、設定の変更、運用、更新等の作業を行う。

オ 情報セキュリティ各課責任者

(ア) 課長等を、情報セキュリティ各課責任者とする。

(イ) 情報セキュリティ各課責任者は、当該課等における情報資産を適正に管理する権限と責任を有する。

(ウ) 情報セキュリティ各課責任者は、情報資産を取扱う職員の指名、並びに職員が取扱う情報資産の範囲を指定する。

カ 情報セキュリティ委員会

情報セキュリティ委員会は、ＣＩＯ、ネットワーク管理者及び情報セキュリティ管理者で構成する。上勝町情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、情報セキュリティポリシーの運用、情報セキュリティ事故・事件への対応等、情報セキュリティに関する重要な事項を審議する。

キ 監査責任者

監査責任者を一人置くこととし、総務課長をもって充て、情報セキュリティについて監査する任に当たります。

３. 情報資産の分類と管理

（１）情報資産の範囲

本情報セキュリティ対策基準が適用される情報資産の範囲は、次の通りとする。

・ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

・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。）

・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

（２） 情報資産の管理責任

ア 管理責任

情報資産は、当該情報資産を作成した課長等が管理責任を有する。

イ 利用者の責任

情報資産を利用する者は、情報資産の分類に従い利用する責任を有する。

ウ 重要性の効力

情報資産が複製または伝送された場合には、当該複製等も分類に基づき管理しなければならない。

（３） 情報資産の分類と管理方法

ア　情報資産の分類

対象となるネットワーク及び情報システムの情報資産は、各々の情報の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重　要　性　分　類
Ⅰ　個人情報及びセキュリティ侵害が上勝町の住民の生命、財産等へ重大な影響を及ぼす影響。
Ⅱ　公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
Ⅲ　外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等軽微な影響を及ぼす情報。
Ⅳ　上記以外の情報

イ　情報資産の管理方法

(ア)　情報資産の管理

- 情報資産の分類に従い、アクセス権限を定めなければならない。
- 情報システムで扱う情報資産について、第三者が重要性の識別を容易に認識できないよう適切な管理を行わなければならない。
- 職員等は、情報資産の複製を保管場所へ移動する場合、当該保管場所からバックアップのために情報システムの設置個所に戻す場合及び業務上必要な場合には、最高情報統括責任者の許可を得たうえで外部への持出または送付をしなければならない。
- 重要な情報資産（重要性分類Ⅰ）は、暗号化を施して管理するものとし、暗号化に用いた暗号鍵及び暗号化された当該情報資産は別々に適切な管理を行わなければならない。

(イ)　外部記録媒体の管理

- 取り出しが可能な外部記録媒体は、適切な管理を行わなければならない。
- 最終的に確定した情報資産を記録した外部記録媒体は、書込禁止措置を行った上で保管しなければならない。
- 外部記録媒体を送る場合は信頼できる者を選定し、複製の禁止及び当該媒体の物理的保護規定を定め、違反した場合の罰則規定を定めなければならない。

(ウ)　情報資産の変更または廃棄の管理

- 外部記録媒体が不要となった場合は、当該媒体に含まれる重要な情報資産（重要性分類Ⅱ以上）は、当該媒体の初期化など情報資産を復元できないように消去を行ったうえで廃棄しなければならない。
- 重要な情報（重要性分類Ⅱ以上）を記載した文書を廃棄する場合には、情報が再読できないようにシュレッダー処分又は焼却処分等をしなければならない。
- 情報資産の廃棄については、情報セキュリティ管理者の許可を得ることとし、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(エ)　外部記録媒体の取扱いについて

- 外部記録媒体のその他取扱いについては、別に定めるところに従い適切に処理しなければならない。

4. 物理的セキュリティ

（1）　サーバ等

ア　装置の取付け等

(ア) ネットワーク及び情報システムの取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に管理し、容易に取り外せないよう適切な措置を施さなければならない。

(イ) 次のサーバは二重化し、ミラーリングにより常に同一データを保持し、メインサーバに障害が発生した場合には速やかにセカンダリサーバに移行させ、システムの運用が停止しないようにしなければならない。

- 重要な情報資産（重要性分類Ⅱ以上）を格納しているサーバ
- セキュリティサーバ
- 住民サービスに関するサーバ
- その他の基幹サーバ

(ウ) ネットワーク管理者、情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が容易に操作できないように、利用者のＩＤ、パスワード設定等の措置を施さなければならない。パスワードは可能な限り複雑なものにしなければならない。

(エ) サーバ等の取付けに当たっては、配線等から放射される電磁波により重要な情報資産（重要性分類Ⅱ以上）が外部に漏洩することがないよう措置しなければならない。

(オ) 無線ＬＡＮ導入するに当たって、重要性分類Ⅱ以上の情報資産は、同ＬＡＮ上にて送信してはならない。

イ 電源

(ア) サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

(イ) 落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

ウ 配線

(ア) 配線は、傍受または損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

(イ) 主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

(ウ) ネットワーク接続口（ハブのポート等）は、他の者が容易に発見できない場所に設置しなければならない。

(エ) ネットワーク管理者、情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

エ 外部に設置する装置

(ア) 外部に設置する装置は、最高情報統括責任者の承認を受けたものでなければならない。
また、最高情報統括責任者は、定期的に当該装置の情報セキュリティの水準について確認しなければならない。

（2） 管理区域

ア 管理区域

(ア) ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等または重要性分類Ⅱ以上の情報資産の管理並びに運用を行うための部屋（以下「電算室」という。）は、外部からの侵入が容易にできないように外壁等に囲まれた管理区域としなければならない。

(イ) 電算室から外部に通ずるドアは１ヶ所のみとし、鍵等によって許可されていない立入りを防止しなければならない。

(ウ)　電算室内の機器類は、耐震対策を講じた場所に設置しなければならない。なお、電算室内の機器類の配置は、緊急時に職員等が円滑に避難できるように配慮しなければならない。

(エ)　電算室を囲む外壁等の床下開口部は全て塞がなければならない。

イ　電算室の入退室管理

電算室の入退室は情報セキュリティ管理者に許可された者のみとし、入退室管理または入退室管理簿の記載を行い、職員等及び外部委託事業者は身分証明書を携帯し、求めにより提示しなければならない。

ウ　機器等の搬入場所

(ア)　電算室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、職員による確認を行わなければならない。

(イ)　機器等の搬入には職員が同行する等の必要な措置を施さなければならない。

（３）　ネットワーク

(ア)　外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

(イ)　ネットワークに使用する回線は、伝送途上において破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

(ウ)　既存住基、税、社会保障などを利用する基幹系システム、ＬGWAN等を活用する情報系システム及びＷｅｂ閲覧やインターネットメールなどを利用するシステムは、それぞれのネットワークを分離しなければならない。また、行政系のネットワークは、総合行政ネットワーク（ＬGWAN）に集約するように努めなければならない。

（４）　職員等の端末等

(ア)　情報システムの事務室等の端末については、盗難防止のための物理的措置を施さなければならない。

５．人的セキュリティ

（１）　職員等の責任

ア　職員

(ア)　情報セキュリティ対策の遵守義務

・全ての職員は、情報セキュリティポリシー及び職員向け実施手順等に定められている事項を遵守しなければならない。

・情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ管理者に相談し、指示等を仰がなければならない。

(イ)　その他

・全ての職員は、使用する端末や外部記録媒体について、第三者に使用されること、または許可なく情報資産を閲覧されることがないように、適切な措置を施さなければならない。

・全ての職員は、情報セキュリティ管理者の許可を得ず、端末等を事務室外に持ち出してはならない。

・全ての職員は、異動、退職等により業務を離れる場合には、知り得た情報資産を秘匿しなければならない。

イ　非常勤及び臨時職員

(ア) 情報セキュリティ対策の遵守義務

・全ての非常勤及び臨時職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

・情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ管理者に相談し、指示等を仰がなければならない。

(イ) 非常勤及び臨時職員の雇用及び契約

・非常勤及び臨時職員には、雇用及び契約時に必ず情報セキュリティポリシーのうち、非常勤及び臨時職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

・非常勤及び臨時職員には、雇用及び契約の際、必要な場合は情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

・非常勤及び臨時職員に端末による作業を行わせる場合においては、インターネットへの接続及び庁内ＬＡＮのメールの使用が不要の場合には、これを利用できないように設定しなければならない。

(ウ) その他

・全ての非常勤及び臨時職員は、使用する端末や外部記録媒体について、第三者に使用されることまたは許可なく情報資産を閲覧されることがないように、適切な措置を施さなければならない。

・全ての非常勤及び臨時職員は、情報セキュリティ管理者の許可を得ず、端末等を事務室外に持ち出してはならない。

・全ての非常勤及び臨時職員は、異動、退職等により業務を離れる場合には、知り得た情報資産を秘匿しなければならない。

ウ　外部委託に関する管理

(ア) ネットワーク及び情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受託する業者も含めて、下記事項を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

・業務上知り得た情報の守秘義務

・提供された情報の目的外利用及び受託者以外の者への提供禁止

・提供された情報の返還義務

・上勝町に対する報告義務

・上勝町による定期的な報告徴収、監査・検査の実施

・従業員に対する教育の実施

・情報セキュリティポリシー遵守のために構築する体制

・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

特に、重要性分類Ⅰ以上の情報資産に関しては、情報システムにおける取扱いのみでなく、データバックアップのための外部施設等への搬送時においても情報資産を盗難、不正コピー等の防止を厳重に実施する旨を契約書に明記しなければならない。

（２） 教育・訓練

ア　最高情報統括責任者は、説明会の実施等により全ての職員等及び関係する者に対し情報セキュリティポリシーについて啓発しなければならない。また、新規採用の職員等を対象とする情報セキュ

リティポリシーに関する定期的な研修を設けなければならない。

また、最高情報統括責任者は、一般職員とは別に、ネットワーク管理者、情報セキュリティ管理者及び情報システム担当者に対して、それぞれの役割、情報セキュリティに関する理解度等に応じた研修を実施しなければならない。

イ　ネットワーク管理者は、最新の技術力を維持するための研修を常に受けなければならない。

ネットワーク管理者は、緊急時対応を想定した訓練を職員等に計画的に行わせなければならない。訓練の計画に当たっては、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を適宜定めることとする。また、より効果的に実施できるよう計画を立てることとする。

ウ　情報セキュリティ管理者及び情報システム担当者は、情報システムに関する研修を受けなければならない。

エ　職員等は、研修に参加し情報セキュリティ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が生じないようにしなければならない。

（3） 事故、欠陥に対する報告

ア　職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合には、速やかにネットワーク管理者に報告し、ネットワーク管理者の指示に従い必要な措置を講じなければならない。また、別途、職員等は、情報セキュリティ管理者に報告し、情報セキュリティ管理者は、報告のあった事故等について全て最高情報統括責任者に報告しなければならない。

イ　職員等は、上勝町が管理するネットワーク及び情報システムに関する事故、欠陥に関する住民からの報告・連絡を受けた場合には、速やかにネットワーク管理者に報告し、ネットワーク管理者の指示に従い必要な措置を講じなければならない。また、別途、職員等は、情報セキュリティ管理者に報告し、情報セキュリティ管理者は、報告のあった事故等について全て最高情報統括責任者に報告しなければならない。

ウ　ネットワーク管理者は、これらの事故等を分析し、再発防止のための情報資産として記録を保存しなければならない。

（4） アクセスのためのパスワードの管理

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

- パスワードを秘密にし、パスワードの照会等には一切応じないこと。
- パスワードのメモを作らないこと。
- パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。
- 情報システムまたはパスワードに対する危険の恐れがある場合には、パスワードを速やかに変更すること。
- パスワードは定期的に、またはアクセス回数に基づいて変更し、古いパスワードの再利用はしないこと。管理者パスワードはさらにこのサイクルを頻繁にしなければならない。
- 複数の情報システムを扱う職員等は、パスワードをシステム間で共有しないこと。
- 仮のパスワードは、最初のログイン時点で変更すること。
- 端末にパスワードを記憶させないこと。必要に応じて暗号化等を行うことによって他者がパスワードを読めないようにすること。
- 職員等間でパスワードを共有しないこと。

6. 技術的セキュリティ

（1） ネットワーク、情報システム及び情報資産の管理

情報資産の重要性分類に従ってネットワーク、情報システム及び情報資産を以下のとおり管理する。

ア Ⅰ及びⅡ

- ネットワーク管理者及び情報システム担当者は、アクセス記録及び情報セキュリティの確保に必要な記録を取得し、盗難、改ざん、消去等を防止する措置を施したうえで一定期間保存しなければならない。また、定期的にそれらを分析、監視しなければならない。
- ネットワーク管理者及び情報システム担当者は、ネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わりなく適切な保管をしなければならない。
- 情報システム担当者は、所管する重要性分類Ⅰ以上の情報資産を最高情報責任者が定めた暗号により暗号化しなければならない。また、重要性分類Ⅱ以上の情報資産を外部へ送信又は搬出する際には、最高情報統括責任者が定めた電子署名方式及び暗号を使用しなければならない。
- 緊急時に直ちに対処できるようにするため、最高情報統括責任者が定めた特に重要な情報システムは、ミラーリングにより常時バックアップしなければならない。また、最高情報統括責任者が定めた重要なネットワーク及び情報システムは、システムを二重化しなければならない。
- ネットワーク管理者及び情報システム担当者は、ミラーリング及び二重化したネットワーク及び情報システムの動作検証を少なくとも四半期ごとに行わなければならない。
- 情報システム担当者は、情報システムのミラーリング等に関わりなく、情報資産の重要度に応じた期間を設定し、定期的に情報資産のバックアップ用の複製を取らなければならない。
- ネットワーク管理者は、職員等が送信等により情報資産を外部に持ち出すことが不可能となるように、システム上制限しなければならない。
- 情報システム担当者は、閲覧制限がない職員等が所管するシステムにアクセスすることが不可能となるように、システム上制限しなければならない。

イ Ⅲ及びⅣ

- 原則、重要性分類Ⅱ以上に分類される情報資産の管理に準拠するが、重要性分類Ⅲ以下の情報資産は公開を前提としているため、この範囲において基準を緩和することができる。ただし、Web サイトにより情報を公開・提供する場合には、当該サイトに係るシステムにおいて改ざん・消去、踏み台、Dos 等を防止しなければならない。また、メールシステム等においても、他のシステムに対する攻撃の踏み台とならないように適切な管理を実施しなければならない。

（2） ネットワーク及び情報システムを使用する際の規定

ア 業務目的以外の使用の禁止

職員等によるネットワーク及び情報システム資源の使用は、業務目的に沿ったもののみが許可される。業務目的外での情報システムへのアクセス、メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

イ 情報資産の持ち出し及びインターネット等による情報資産の送信禁止

職員等は、重要性分類Ⅱ以上に該当する情報資産を取り扱う場合、下記の行為を行ってはならない。特に、重要性分類Ⅱ以上に該当する情報資産のインターネットへの自動転送は厳禁する。

- 庁外への持ち出し
- インターネット等による庁外との送受信
- 個人の所有する情報が記録された媒体の管理区域への持ち込み

ただし、情報資産のバックアップ等、合理的理由のある場合、かつ最高情報統括責任者の事前の

了解を得た場合に限り、庁外への持ち出し又は庁外との送受信ができるものとする。

ウ　無許可ソフトウエアの導入の禁止

職員等は、各自に供用された端末等に対して、ネットワーク管理者が定める以外のソフトウエアの導入は行ってはならない。特にネットワーク上の情報資産を盗聴するような監視ソフトウエアやネットワークの状態を探索するセキュリティ関連のソフトウエア及びハッキングソフトウエアの使用は厳禁し、導入または使用した職員等は地方公務員法による懲戒処分の対象とする。ただし、業務を円滑に遂行するために必要なソフトウエアについては、合理的理由のある場合、かつネットワーク管理者及び情報システム担当者の事前の了解を得た場合に限り、利用することができる。

エ　機器構成の変更の禁止

職員等は、各自に供用された端末等に対して機器の増設または改造を行ってはならない。特にモデム等の機器を増設して他の環境（インターネット等）へのネットワーク接続を行うことや、庁外からのアクセスを可能とする仕組みを構築した職員等は地方公務員法による懲戒処分の対象とする。ただし、業務を円滑に遂行するための合理的理由がある場合、かつネットワーク管理者及び情報システム担当者の事前の了解を得た場合に限り、機器の増設または変更を行うことが出来る。

オ　情報及びソフトウエアの交換

組織間において、情報システムに関する情報及びソフトウエアを交換する場合は、その取扱いに関する事項をあらかじめ定め、ネットワーク管理者の許可を得なければならない。

カ　メール

・メールの容量は１００ＭＢを上限とし、１００ＭＢを超えるメールの送受信を不可能としなければならない。

・職員等が使用するメールボックスは職員等が自らメールを整理し、削除しなければならない。

キ　その他

職員等が利用するプロトコルは業務上必要最低限のものとする。

（3）　アクセス制御

ア　利用者登録

ネットワーク管理者及び情報システム担当者は、利用者の登録、変更、抹消、登録した情報資産の管理、異動や上勝町外への出向等の職員等及び退職者における利用者ＩＤの取扱い等については、定められた方法に従って行わなければならない。

必要な利用者登録・変更は、ネットワーク管理者及び情報システム担当者に対する申請により行う。

イ　管理者権限

ネットワーク、情報システムの管理者権限は、厳重に管理しなければならない。

ネットワーク管理者の権限を代行する者は、ネットワーク管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は速やかにネットワーク管理者及び情報システム担当者に周知しなければならない。

ウ　インターネット以外のネットワークにおけるアクセス制御

ネットワーク管理者は、アクセス可能なネットワーク及びネットワーク上のサービス毎にアクセス出来る者を定めなければならない。

ネットワーク管理者及び情報システム担当者は、ネットワークサービスを使用する権限を有しな

い職員等が当該サービスを使用できるようにしてはならない。

エ　強制的な経路制御

ネットワーク管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

オ　外部からのアクセス

(ア)　外部からのアクセスの許可は、必要最低限にしなければならない。

外部からアクセスを認める場合には、内部のネットワーク及び情報システムとの間に IP リサーチャビリティが発生しないように機器を構成しなければならない。

アクセス方法及び使用方法等は、利用者の真正性の確保が確定できるものでなければならない。

(イ)　モバイル端末による内部のネットワーク及び情報システムに対するアクセスは、合理的理由を有し、かつネットワーク管理者が定める必要最小限の者に限定しなければならない。

カ　総合行政ネットワーク及び住民基本台帳ネットワークシステムとの接続

総合行政ネットワーク及び住民基本台帳ネットワークシステムについては、当該接続において取り扱う情報資産の重要性を考慮し、担当課との十分な協議をした上で、適切なアクセス制御を実施する。

キ　外部ネットワークとの接続

(ア)　外部ネットワークとの接続にあたり、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を詳細に検討し、上勝町の全てのネットワーク、情報システム及び情報資産に影響が生じないと明確に確認したうえで、最高情報統括責任者及びネットワーク管理者の許可に基づき接続しなければならない。

その利用はネットワーク管理者の適切な管理下で行い、接続に際しては情報セキュリティに留意したネットワーク構成を採らなければならない。

この場合、当該外部ネットワークの瑕疵により上勝町のデータの漏洩、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

(イ)　接続した外部ネットワークのセキュリティに問題が認められ、上勝町の情報資産に脅威が生じることが想定される場合には、ネットワーク管理者の判断に従い速やかに当該外部ネットワークを物理的に遮断しなければならない。

ク　自動識別

上勝町で使用されるネットワーク機器については、機器固有情報によってアクセスの可否を自動的に判別しなければならない。

ケ　ログイン手順

ログイン手順中におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等、正当なアクセス権を持つ職員等がログインしたことを確認することができる手順を定めなければならない。

コ　パスワードの管理方法

(ア)　ネットワーク管理者または情報システム担当者は、職員等のパスワードに関する情報を厳重に管理しなければならない。職員等のパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

(イ)　ネットワーク管理者または情報システム担当者は、パスワードの変更を行わない職員等にパ

スワードを変更する旨勧告し、当該職員等が勧告に従わない場合には速やかに当該職員等のアクセス権を一定期間経過後に停止しなければならない。

(ウ)　ネットワーク管理者または情報システム担当者は、当該職員等からパスワード変更の申告があり次第当該職員等のアクセス権の停止を解除するものとする。

(エ)　ネットワーク管理者または情報システム担当者は、職員等のパスワードについて、定期的にその妥当性について調査を行わなければならない。

(オ)　ネットワーク管理者または情報システム担当者は、第三者に読まれることのないよう、暗号化等パスワードを扱う方法を定めなければならない。

サ　接続時間の制限

管理者権限によるネットワーク及び情報システムへの接続については、必要最小限の接続時間に制限しなければならない。

（４）　システム開発、導入、保守等

ア　情報システムの調達

(ア)　最高情報統括責任者は応用ソフトウエアの開発、変更及び運用についての手順及び基準を明らかにしなければならない。

(イ)　最高情報統括責任者は機器及び基本ソフトウエアの導入、保守及び撤去についての手順及び基準を明らかにしなければならない。

(ウ)　ネットワーク管理者または情報システム担当者は、情報システムの調達にあたっては、一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

(エ)　ネットワーク管理者または情報システム担当者は、機器及びソフトウエアを購入等する場合は、当該製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。

イ　ネットワーク及び情報システム更新

ネットワーク管理者または情報システム担当者は、ネットワーク及び情報システムを更新するに当たり、更新の内容、必要性、計画等を文書にて最高情報統括責任者に提出し承認を得なければならない。ネットワーク及びシステムの移行は、擬似環境による動作確認後に行わなければならない。移行の際にはシステムに記録されている情報資産の保存を確実に行い、復帰が即座に可能な状態にしておき、原則として執務時間外に行わなければならない。また、作業を行う際には作業状況を確認しながら実施するとともに、作業内容を記録しなければならない。

ウ　情報システムの開発及び導入

最高情報統括責任者はシステム開発及び保守時の事故・不正行為対策のため、次の事項を定めなければならない。

- 責任者及び監督者
- 作業者及び作業範囲
- システム開発及び保守等の事故・不正行為に係るリスク分析
- 開発・保守するシステムと運用システムの分離
- 開発・保守に関するソースコードの提出
- 開発・保守の際のセキュリティ上問題となりうる恐れのあるＯＳ、ミドルウエア及びアプリケーションソフトの使用禁止
- 開発・保守の際のアクセス制限
- 機器の搬出入の際の、情報システム担当者の許可及び確認

・開発・保守記録の提出義務
・マニュアル等の定められた場所への保管
・開発・保守を行った者の利用者 ID、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消
・守秘義務
・再委託管理

エ　システムの導入

(ア)　情報システム担当者は、新たにシステムを導入する際には、既に稼動しているシステムに接続する前に十分な試験を行わなければならない。

(イ)　情報システム担当者は、試験に使用したデータ及びその結果を最高情報統括責任者及びネットワーク管理者へ提出するとともに厳重に保管しなければならない。

オ　ソフトウエアの保守及び更新

ソフトウエア（独自開発ソフトウエア及び汎用ソフトウエア）等を更新、又は修正プログラムを導入する場合は、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

情報システム担当者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかな対応を行うこととし、その他のソフトウエアの更新等については、計画的に実施しなければならない。

カ　システムの受諾業者への規定

(ア)　新たなシステムの開発を外部の事業者に委託する場合は、ソースコードの提出を求め、再委託契約を行う際には再委託先については契約課において経営状況等、契約履行が可能であるか確認をとり、導入前の検査要求事項等を契約に定めなければならない。

(イ)　信頼のおける事業者に委託するために、必要な資格等を定めなければならない。

(ウ)　情報システム担当者は、作業中に身分証明書の提示を事業者に求め、契約で定められた資格を有するものが作業に従事しているか確認を行わなければならない。

また、守秘のための契約を事業者と結ばなければならない。

キ　機器の修理及び廃棄

(ア)　外部記憶媒体の含まれる機器について、外部の事業者に修理させまたは廃棄する場合は、その内容が消去された状態で行わなければならない。

(イ)　故障を外部の事業者に修理させる際、情報資産を消去することが難しい場合は、修理を委託する事業者に対し秘密を守ることを契約に定めなければならない。また重要な機器については、復元不可能な廃棄を行わなければならない。

ク　管理記録

ネットワーク管理者及び情報システム担当者は、担当するシステムにおいて行ったシステム変更等の作業については、記録を作成し適切に管理を行わなければならない。

（5）　コンピュータウイルス対策

ア　無許可ソフトウエアの導入は禁止する。

イ　外部ネットワークから情報またはソフトウエアを取り入れる際には、サーバ側、端末側においてウイルスチェックを行なわなければならない。

ウ　外部のネットワークへ情報またはソフトウエアを送信する際にも端末側においてウイルスチェ

ックを行い、外部へウイルスが拡散することを未然に防止しなければならない。

エ　ネットワーク管理者は、次の事項を実施しなければならない。

・ウイルス情報について職員等に対する注意喚起を行うこと。

・常時ウイルスに関する情報収集に努めること。

・サーバ及び端末において、ウイルスチェックを行うこと。

・ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

オ　職員等は、次の事項を遵守しなければならない。

・外部からデータ又はソフトウエアを取り入れる場合には、必ずウイルスチェックを行うこと。

・差出人が不明または不自然に添付されたファイルは速やかに削除すること。

・ネットワーク管理者が提供するウイルス情報を常に確認すること。

カ　ネットワーク管理者及び情報システム担当者は、職員等から報告のあった情報、システムの障害に対する処理または問題等は障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

（6）　不正アクセス対策

ア　ネットワーク管理者は、次の事項を実施しなければならない。

・使用終了若しくは使用される予定のないポートを長時間空けた状態のままにしてはならない。

・セキュリテイホールの発見に努め、メーカー等からパッチの提供があり次第速やかにパッチをあてなければならない。

・不正アクセスによるウェブページ書換防止を確実にするために、担当職員等によるものであるか否かに関わりなくデータの書換を検出し、ネットワーク管理者及び情報システム管理者へ通報する設定を施さなければならない。

・重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

イ　攻撃を受けることが明確な場合には、ネットワーク管理者はシステムの停止を含む必要な措置を講じなければならない。また、関係機関との連絡を密にして情報の収集に努めなければならない。

ウ　攻撃を受け、当該攻撃が不正アクセス禁止法違反等犯罪の可能性がある場合には記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

エ　攻撃の可能性が明確であるにもかかわらず職員等の怠惰が原因でデータの漏洩、破壊、改ざんまたはシステムダウン等により行政業務に深刻な影響をもたらした場合、当該職員等を地方公務員法による懲戒の対象とする。

オ　職員等による不正アクセスがあった場合、ネットワーク管理者または情報システム担当者は当該職員等が所属する長等に通知し、適切な処置を求めなければならない。

　職員等による不正アクセスの結果、データの漏洩、破壊、改ざんまたはシステムダウン等により行政業務に深刻な影響をもたらした場合、当該職員等を地方公務員法による懲戒の対象とし、悪質な場合には刑事告発の対象とする。

（7）　セキュリティ情報の収集

(ア)　ネットワーク管理者は、情報セキュリティに関する情報を収集し、上勝町の全てのネットワーク及び情報システムについてソフトウエアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

(イ)　ネットワーク管理者は、緊急時対応計画に定める緊急に連絡すべき情報を入手した場合は当

該計画に定める情報連絡先に連絡しなければならない。

7. 運用

（1） 情報システムの監視

(ア) セキュリティに関する事案を検知するため、ネットワーク管理者及び情報システム管理者は、常に情報システムの監視を行わなければならない。

(イ) 外部と常時接続するシステムについては、24 時間監視を行わなければならない。

(ウ) 内部のシステムについて、アクセスコントロール等を行い、異常な運用等の監視を行わなければならない。

(エ) 監視により得られた結果については、盗難、改ざん、消去等を防止するために必要な措置を施し、安全な場所に保管しなければならない。また、これらの記録の正確性を確保するため、正確な時刻の設定を行わなければならない。

（2） 情報セキュリティポリシーの遵守状況の確認

(ア) 情報セキュリティ管理者は、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、また、問題が発生していないかについて常に確認を行い問題が発生していた場合には速やかに最高情報統括責任者に報告しなければならない。

(イ) 最高情報統括責任者は速やかに発生した問題に適切に対処しなければならない。

(ウ) 職員等は、情報セキュリティポリシーの違反が発生した場合は、直ちにネットワーク管理者及び情報セキュリティ管理者に報告を行わなければならない。違反の発生時には、それが直ちに情報セキュリティ上重大な影響を及ぼす可能性があるとネットワーク管理者が判断した場合は、緊急時対応計画に従って連絡を行わなければならない。

(エ) ネットワーク管理者及び情報システム担当者は、サーバ等のシステム設定が情報セキュリティポリシーが遵守しているかどうかについて、また問題が発生していないかについて定期的に確認を行い、問題が発生していた場合には速やかなに適切に対処しなければならない。

（3） 運用管理における留意点

(ア) 最高情報統括責任者は、アクセス記録、メール等個人のプライバシーに係る情報を閲覧できる権限を有する職員を情報セキュリティ実施手順に定めなければならない。ただし、法令で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法令に定められた手続きに従う。

(イ) 情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を参照できるよう配慮しなければならない。

（4） 侵害時の対応

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のとおり定める。

ア 連絡先

具体的には、各情報システムごとに情報セキュリティ実施手順に明記する。

- 上勝町長
- 最高情報統括責任者
- ネットワーク管理者
- 情報システム担当者

・ネットワーク及び情報システムに係る外部委託業者
・徳島県政策創造部地方創生局地域振興課
・警察
・関係機関
・影響が考えられる個人及び法人

イ　事案の調査

セキュリティに関する事案を認めた者は、次の項目について、速やかにネットワーク管理者に報告しなければならない。

・症状の分類
・事案が発生した原因として、想定される行為
・確認した被害・影響範囲
・記録

ネットワーク管理者は、事案の詳細な調査を行うとともに、最高情報統括責任者との情報共有並びに関係各位への報告を行わなければならない。

ウ　事案への対処

(ア)　ネットワーク管理者は、次の事案が発生した場合、それぞれ定められた連絡先へ連絡しなければならない。

・サイバーテロその他の住民に重大な被害が生じる恐れがあるとき（上勝町長、最高情報統括責任者、警察、影響が考えられる個人及び法人）
・不正アクセスその他犯罪と思慮されるとき（上勝町長、最高情報統括責任者、警察）
・踏み台となって他者に被害を与える恐れがあるとき（上勝町長、最高情報統括責任者、警察）
・情報システムに関する被害（情報システム担当者、必要と認められる事業者等）
・その他情報資産に係る被害（関係部局等）

(イ)　ネットワーク管理者は、次の事案が発生し情報資産の防護のためにネットワークの切断がやむを得ない場合は、ネットワークを切断する措置を講ずる。

・異常なアクセスが継続しているとき、又は不正アクセスが判明したとき
・システムの運用に著しい支障をきたす攻撃が継続しているとき
・コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき
・情報資産に係る重大な被害が想定されるとき

(ウ)　情報システム担当者は、次の事案が発生し情報資産の防護のために情報システムの停止がやむを得ない場合は、情報システムを停止する。

・コンピュータウイルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき
・災害等により電源を供給することが危険又は困難なとき
・その他の情報資産に係る重大な被害が想定されるとき

(エ)　個々の端末のネットワークからの切断については、ネットワーク管理者の許可が必要である。ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合には、事後報告とすることができる。

(オ)　事案に係るシステムのアクセス記録及び現状を保存する。

(カ)　事案に対処した経過を記録する。

(キ)　事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討する。

(ク)　再発防止の暫定措置を講じた後、復旧する。

(ケ)　復旧後、必要と認められる基幹、再発監視を行う。

エ　再発防止の措置

(ア)　ネットワーク管理者は、当該事案に係るリスク分析を実施し、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画を策定しなければならない。

(イ)　ネットワーク管理者は、各種セキュリティ対策の改善に係る再発防止計画を策定し、最高情報統括責任者へ報告しなければならない。最高情報統括責任者は、これらの再発防止計画が有効であると認められる場合は、これを承認し、事案の概要と併せ職員等に周知しなければならない。

オ　外部委託による運用契約

運用を外部委託する場合は、委託に関する責任を有する部署を明確にするとともに、外部委託事業者に対し必要なセキュリティ要件を記載した契約書による契約を締結しなければならない。

委託に関する責任を有する部署は、委託先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、その内容をネットワーク管理者に報告するとともに、その重要度に応じて最高情報統括責任者に報告しなければならない。

８. 法令遵守

職員等は、職務の遂行において使用する情報資産について、次の法令等を遵守しこれに従わなければならない。

- 地方公務員法(昭和２５年１２月１３日法律第２６１号)
- 不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
- サイバーセキュリティ基本法（平成２６年１１月１２日法律第１０４号）
- 著作権法（昭和４５年法律第４８号）
- 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」（平成 25 年法律第 27 号）
- 上勝町個人情報保護条例（平成１５年条例第４号）
- 上勝町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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成 27 年条例第 24 号）

９. 情報セキュリティに関する違反に対する対応

情報セキュリティポリシーに違反した職員等及びその監督責任者に対しては、その重大性、発生した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する。

なお、職員等に情報セキュリティポリシーに違反する行動がみられた場合には、速やかに次の措置を講じなければならない。

- 情報セキュリティ管理者の指導によっても改善されない場合、ネットワーク管理者は、当該職員等のネットワーク又は情報システムの使用に関する権利を停止あるいは剥奪することができる。その後速やかに、ネットワーク管理者は、職員等の権利を停止あるいは剥奪した旨を最高情報統括責任者及び当該職員の所属する長等に通知しなければならない。

10. 監査・点検

（１） 監査

ア　実施方法

(ア)　ネットワーク及び情報システムの情報セキュリティについて監査を定期的に行わなければならない。なお、ネットワーク管理者及び情報システム担当者は、監査とは別に所管するネットワーク及び情報システムについて点検を実施しなければならない。

イ　監査を行う者の要件

（ア）　監査責任者は、監査を実施する場合に、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

（イ）　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

ウ　監査実施計画の立案及び実施への協力

（ア）　監査責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

（イ）　被監査部門は、監査の実施に協力しなければならない。

エ　外部委託事業者に対する監査

外部委託事業者に委託している場合、監査責任者は外部委託事業者から下請けとして受託している事業者も含めて、必要に応じて情報セキュリティポリシーの遵守について監査を行わなければならない。

オ　報告

監査責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

カ　保管

監査責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（２）　自己点検

ア　実施方法

（ア）　統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ管理者は、所管するネットワーク及び情報システムについては、毎年度及び必要に応じて自己点検を実施しなければならない。

（イ）　情報セキュリティ管理者は、所管する部署における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状況について、毎年度及び必要に応じて自己点検を実施しなければならない。

イ　報告

情報セキュリティ管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

ウ　自己点検結果の活用

(ア)　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

(イ)　情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

11. 評価・見直し

（１）　情報セキュリティポリシーの更新

新たに必要な対策が発生した場合又は監査の結果及び自己点検の結果を踏まえ、情報セキュリティ

ポリシーの実効性を評価し、必要な部分を見直し、内容、時期について決定を行う。この決定に基づき、情報セキュリティポリシーの更新を実施する。