横手市情報セキュリティ対策及び
特定個人情報の安全管理に関する基準

目次

１　総則

１－１　目的

この基準は、横手市情報セキュリティ及び特定個人情報の安全管理に関する基本方針（以下「基本方針」という。）に規定する情報セキュリティ対策及び特定個人情報の安全管理措置の実施について、必要な事項を定めることを目的とする。

１－２　定義

この基準において使用する用語の意義は、行政手続における特定の個人を識別する番号の利用等に関する法律（平成２５年法律第２７号。以下「番号法」という。）、横手市個人情報保護条例（平成１７年横手市条例第２４号）及び基本方針で使用する用語の例によるほか、次に定めるところによる。

用語	定義
情報セキュリティ事象	情報セキュリティポリシーへの違反若しくは管理策の不具合の可能性又は情報セキュリティに関係し得る未知の状況を示すシステム、サービス又はネットワークの状態に関連する事象
情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いもの（特定個人情報の漏えいその他の番号法違反の事案またはおそれのある事案を含む）
端末	情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボード、マウス等の周辺機器を含む。）
パソコン	端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないもの（形態は問わない。）
モバイル端末	端末のうち、業務上の必要に応じて移動させて使用することを目

	的としたもの（形態は問わない。）
電子署名	情報の正当性を保証するための電子的な署名情報
標的型攻撃	明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃
約款による外部サービス	民間事業者等の庁外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うもの（利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。）
ソーシャルメディアサービス	ツイッター、フェイスブック等のＳＮＳ（ソーシャル・ネットワーキング・サービス）、ブログ及び動画共有サイトに代表されるユーザによる情報発信と情報共有によるコミュニケーションを特徴とするインターネット上のサービス

１－３　対象範囲

（１）　実施機関の範囲

この基準が適用される実施機関は、基本方針３（１）の実施機関（学校及び病院事業を除く。）とする。

（２）　情報資産の範囲

この基準が対象とする情報資産は、基本方針３（２）に掲げる情報資産（学校及び病院事業に供するものを除く。）とする。

（３）　特定個人情報の範囲

この基準が対象とする特定個人情報は、基本方針３（３）に掲げる特定個人情報とする。

２　組織体制

２－１　最高情報セキュリティ責任者及び総括保護責任者

（１）　市に最高情報セキュリティ責任者を置き、横手市副市長事務担任規程（平成１９年横手市訓令第１６号）第２条第２項に規定する総務企画部に属する事務を担任する副市長をもって充てる。

（２）　最高情報セキュリティ責任者は、市におけるすべての情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（３）　市に特定個人情報の安全管理に係る総括保護責任者を置き、最高情報セキュリティ責任者をもって充てる（以下、最高情報セキュリティ責任者及び総括保護責任者を総称して「ＣＩＳＯ」という。）。

（４）　総括保護責任者は、市における特定個人情報の管理に関する事務を総括する任に当たる。

（５）　ＣＩＳＯは、情報セキュリティインシデントに対処するための体制（以下、「ＣＳＩＲＴ」という）を整備し、役割を明確化しなければならない。

２－２　統括情報セキュリティ責任者

（１）　市に統括情報セキュリティ責任者を置き、総務企画部長をもって充てる。

（２）　統括情報セキュリティ責任者は、ＣＩＳＯを補佐しなければならない。

（３）　統括情報セキュリティ責任者は、市のすべてのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

（４）　統括情報セキュリティ責任者は、市のすべてのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

（５）　統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、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。

（６）　統括情報セキュリティ責任者は、市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、ＣＩＳＯの指示に従い、ＣＩＳＯが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

（7）　統括情報セキュリティ責任者は、市の情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

（8）　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

（9）　統括情報セキュリティ責任者は、緊急時にはＣＩＳＯに早急に報告を行うとともに、回復のための対策を講じなければならない。

(10)　統括情報セキュリティ責任者は、自身の権限に属する事務を情報政策課長に処理させることができる。

２－３　情報セキュリティ責任者及び保護責任者

（1）　市に情報セキュリティ責任者を置き、市長事務部局の部長、議会事務局長、行政委員会事務局の部長・局長、消防長及び会計管理者をもって充てる。

（2）　情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

（3）　情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

（4）　情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。

（5）　市に特定個人情報の安全管理にかかる保護責任者を置き、特定個人情報を取り扱う部局等の情報セキュリティ責任者をもって充てる。

（6）　保護責任者は、当該部局等における特定個人情報の管理に関する事務を統括する任に当たる。

２－４　情報セキュリティ管理者及び保護管理者

（1）　市に情報セキュリティ管理者を置き、市長事務部局の課室所長、行政委員会事務局の課室所長、消防本部の課室長及び消防署長をもって充てる。

（2）　情報セキュリティ管理者は、その所管する課室所等の情報セキュリティ対策に関する権限及び責任を有する。

（3）　情報セキュリティ管理者は、その所管する課室所等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及びＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

（4）　市に特定個人情報の安全管理にかかる保護管理者を置き、特定個人情報を取り扱う課室所等の情報セキュリティ管理者をもって充てる。

（5）　保護管理者は、当該課室所等における特定個人情報を適切に管理する任に当たる。

（6）　保護管理者は、当該課室所等において特定個人情報を取り扱う職員等（以下「特定個人情報取扱者」という。）を指定し、当該特定個人情報取扱者の役割及び取り扱う特 定個人情報の範囲を明らかにしておかなければならない。

（7）　保護管理者は、特定個人情報を複数の部署で取り扱う場合の各部署の任務分担及び責任を明らかにしておかなければならない。

２－５　情報システム管理者

（1）　市に情報システム管理者を置き、各情報システムの担当課室所長をもって充てる。

（2）　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

（3）　情報システム管理者は、所管する情報システム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。

（4）　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

２－６　情報システム担当者

市に情報システム担当者を置き、情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者をもって充てる。

２－７　情報セキュリティ委員会

（１）　市の情報セキュリティ対策及び特定個人情報の安全管理措置を統一的に実施するため、市に情報セキュリティ委員会を置く。

（２）　情報セキュリティ委員会は、情報セキュリティポリシー等、情報セキュリティ及び特定個人情報の安全管理に関する重要な事項を決定する。

（３）　情報セキュリティ委員会は、毎年度、市における情報セキュリティ対策及び特定個人情報の安全管理措置の改善計画を策定し、その実施状況を確認しなければならない。

２－８　兼務の禁止

（１）　情報セキュリティ対策及び特定個人情報の安全管理措置の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者及びその承認者又は許可者は、同じ者が兼務してはならない。

（２）　監査を受ける者及びその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

２－９　ＣＳＩＲＴの設置・役割

（１）　ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化すること。

（２）　ＣＩＳＯは、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ責任者を置くとともに、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員を定めること。

（３）　ＣＩＳＯは、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備すること。

（４）　ＣＩＳＯによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供すること。

（５）　情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省、秋田県等へ報告すること。

（６）　情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知及び公表対応を行わなければならない。

（7）　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行うこと。

３　情報資産の分類と管理

３－１　情報資産の分類

市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

① 機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	･行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産 ・特定個人情報	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限及び保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信及び情報資産の運搬・提供時における暗号化又はパスワード設定及び鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	上記以外の情報資産	

② 完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ及び電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	上記以外の情報資産	

③ 可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ及び指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	上記以外の情報資産	

３－２　情報資産の管理

（１）　管理責任

① 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

② 情報資産が複製又は伝送された場合には、複製等された情報資産についても上記３－１の分類に基づき管理しなければならない。

（２）　情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情

報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

（３） 情報の作成

① 職員等は、業務上必要のない情報を作成してはならない。

② 情報を作成する者は、情報の作成時に上記３－１の分類に基づき管理しなければならない。

③ 情報を作成する者は、作成途上の情報についても、紛失、流出等を防止しなければならない。この場合において、情報の作成途上で不要になったときは、当該情報を消去しなければならない。

（４） 情報資産の入手

① 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

② 庁外の者が作成した情報資産を入手した者は、上記３－１の分類に基づき管理しなければならない。

③ 情報資産を入手した者は、入手した情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰がなければならない。

（５） 情報資産の利用

① 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

② 情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

③ 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合は、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（６） 情報資産の保管

① 情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

② 情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

③ 情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体又は情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

④ 情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合は、耐火、耐熱、耐水及び可能な限りの耐湿を講じた施錠可能な場所に保管しなければならない。

（７） 情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

（８） 情報資産の運搬

① 車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

② 機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

（９） 情報資産の提供・公表

① 機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

② 機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

③ 情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

(10)　情報資産の廃棄

① 機密性２以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合は、電磁的記録媒体の初期化等し、情報を復元できないように処置した上で廃棄しなければならない。

② 情報資産の廃棄を行う者は、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。

③ 情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

４　特定個人情報の取扱い

４－１　アクセス制限

（１）　保護管理者は、特定個人情報の秘匿性等その内容に応じて、当該特定個人情報にアクセスする（紙等に記録されている特定個人情報に接する行為を含む。以下同じ。）権限を有する職員等とその権限の内容を、当該職員等が業務を行う上で必要最小限の範囲に限らなければならない。

（２）　アクセス権限を有しない職員等は、特定個人情報にアクセスしてはならない。

（３）　職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で特定個人情報にアクセスしてはならない。

４－２　複製等の制限

職員等は、業務上の目的で特定個人情報を取り扱う場合であっても、次に掲げる行為については、保護管理者の指示に従い行わなければならない。

①　特定個人情報の複製

②　特定個人情報の送信

③　特定個人情報が記録されている媒体の外部への送付又は持出し

④　その他特定個人情報の適切な管理に支障を及ぼすおそれのある行為

４－３　誤りの訂正等

職員等は、特定個人情報の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行わなければならない。

４－４　媒体の管理等

（１）　職員等は、保護管理者の指示に従い、特定個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めたときは、耐火金庫への保管、施錠等を行わなければならない。

（２）　職員等は、特定個人情報が記録されている媒体を庁舎内で移動させる場合には、紛失・盗難等に留意するものとする。

４－５　廃棄等

職員等は、特定個人情報又は特定個人情報が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該特定個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行わなければならない。

４－６　特定個人情報の取扱状況の記録

保護管理者は、特定個人情報の秘匿性等その内容及び必要に応じて、台帳等を整備して、当該特定個人情報の利用及び保管等の取扱いの状況について記録しなければならない。

４－７　個人番号の利用の制限等

（１）　保護管理者は、個人番号の利用に当たり、番号法及び横手市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条例（平成２７年横手市条例第３７号。以下「番号条例」という。）があらかじめ限定的に定めた事務に限定しなければならない。

（２）　特定個人情報取扱者は、個人番号利用事務等を処理するために必要な場合その他番号法で定める場合を除き、個人番号の提供を求めてはならない。

（３）　特定個人情報取扱者は、個人番号利用事務等を処理するために必要な場合その他番号法で定める場合を除き、特定個人情報ファイルを作成してはならない。

（４）　特定個人情報取扱者は、番号法第１９条各号のいずれかに該当する場合を除き、他人の個人番号を含む個人情報を収集し、及び保管してはならない。

（５）　保護管理者は、特定個人情報を取り扱う事務を実施する区域を明確にし、書類等の盗難又は紛失等を防止するために施錠可能な場所への保管等の物理的な安全管理措置を講じなければならない。

５　情報システム全体の強靭性の向上

５－１　マイナンバー利用事務系

（１）　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(ＭＡＣアドレス、ＩＰアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、外部接続先もインターネット等と接続してはならない。

（２）　情報のアクセス及び持ち出しにおける対策

① 情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。

② 原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

５－２　ＬＧＷＡＮ接続系

ＬＧＷＡＮ接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。また、メールやデータをＬＧＷＡＮ接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア）　インターネット環境で受信したインターネットメールの添付ファイル、及びインターネットからダウンロードしたファイルを、サニタイズ処理を実施したうえでＬＧＷＡＮ接続系に取り込む方式

（イ）　インターネット接続系の端末から、ＬＧＷＡＮ接続系の端末へ画面を転送する方式

５－３　インターネット接続系

（１）　不正通信の監視の強化

インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通

信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びＬＧＷＡＮへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

（２）　自治体情報セキュリティクラウドの活用等

市区町村のインターネット接続口を集約する自治体情報セキュリティクラウドを活用するとともに、総務省や秋田県等と連携しながら、情報セキュリティ対策を推進しなければならない。

６　物理的セキュリティ

６－１　サーバ等の管理

（１）　機器の取付け

情報システム管理者は、サーバ等の機器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設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（２）　サーバの冗長化

情報システム管理者は、所管するサーバに格納している情報の重要性、可用性、停止することによる業務への影響度等を勘案し、必要に応じて冗長化を施し、サービス又は業務を停止させないよう努めなければならない。

（３）　機器の電源

① 情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、所管するサーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正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。

② 情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、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講じなければならない。

（４）　通信ケーブル等の配線

① 統括情報セキュリティ責任者及び情報システム管理者等は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② 統括情報セキュリティ責任者及び情報システム管理者等は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合は、連携して対応しなければならない。

③ 統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハ

ブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④　統括情報セキュリティ責任者、情報システム管理者は、自ら又は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講じなければならない。

（５）　機器の定期保守及び修理

①　情報システム管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

②　情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合は、内容を消去した状態で行わせなければならない。この場合において内容を消去できないときは、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（６）　庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合は、ＣＩＳＯの承認を得なければならない。この場合において、統括情報セキュリティ責任者及び情報システム管理者は、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（７）　機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合は、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

６－２　管理区域（情報システム室等）の管理

（１）　管理区域の構造等

① 管理区域とは、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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）及び電磁的記録媒体の保管庫をいう。

② 統括情報セキュリティ責任者及び情報システム管理者は、可能な限り管理区域を地階又は１階に設けてはならない。この場合において、統括情報セキュリティ責任者及び情報システム管理者は、管理区域を可能な限り無窓の外壁にする等外部からの侵入が容易にできないようにしなければならない。

③ 統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置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。

④ 統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、可能な限り転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤ 統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を可能な限り塞がなければならない。

⑥ 統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（２）　管理区域の入退室管理等

① 情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

② 職員等及び外部委託事業者は、管理区域に入室する場合は、身分証明書等を携帯し、求めにより提示しなければならない。

③ 情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き

添うものとし、外見上職員等と区別できる措置を講じなければならない。

④　情報システム管理者は、機密性２以上の情報資産を扱う情報システムを設置している管理区域について、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）　機器等の搬入出

①　情報システム管理者は、搬入する機器等が既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

②　情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

６－３　通信回線及び通信回線装置の管理

①　統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。

②　統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

③　統括情報セキュリティ責任者は、 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

④　統括情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。この場合において、統括情報セキュリティ責任者は、必要に応じ、送受信される情報の暗号化を行わなければならない。

⑤　統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、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を実施しなければならない。

⑥　統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。この場合において、統括情報セキュリティ責任者は、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

６－４　職員等のパソコン等の管理

① 情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。この場合において、電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

② 情報システム管理者は、所管する情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

③ 情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

④ 情報システム管理者は、パソコン、モバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。この場合において、端末にセキュリティチップが搭載されているときは、その機能を有効に活用しなければならない。

7　人的セキュリティ

7－1　職員等の遵守事項

（1）　職員等の遵守事項

① 職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。この場合において、情報セキュリティ対策及び特定個人情報の安全管理について不明な点、遵守することが困難な点等があるときは、速やかに情報セキュリティ管理者及び保護管理者に相談し、指示を仰がなければならない。

② 職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子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。

③ ＣＩＳＯは、機密性２以上、可用性２及び完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

④ 職員等は、市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

⑤ 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

⑥ 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

⑦ 職員等は、支給以外のパソコン、モバイル端末、電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑧ 情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑨ 職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

⑩ 職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報

を閲覧されることがないように、離席時のパソコン、モバイル端末のロック及び電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑪　職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。

⑫　職員等は、業務上知り得た情報を漏らしてはならない。その職を退いた後も同様とする。

（２）　非常勤及び臨時職員への対応

①　情報セキュリティ管理者及び保護管理者は、非常勤及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員が守るべき内容を理解させ、実施及び遵守させなければならない。

②　情報セキュリティ管理者及び保護管理者は、非常勤及び臨時職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③　情報セキュリティ管理者は、非常勤及び臨時職員にパソコン又はモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合は、これを利用できないようにしなければならない。

（３）　情報セキュリティポリシー等の掲示

情報セキュリティ管理者及び保護管理者は、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閲覧できるように掲示しなければならない。

（４）　外部委託事業者に対する説明

情報セキュリティ管理者及び保護管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

７－２　研修・訓練

（１）　情報セキュリティに関する研修・訓練等

ＣＩＳＯは、定期的に情報セキュリティに関する研修・訓練及び特定個人情報の安全管理に関する研修を実施しなければならない。

（２）　研修計画の策定及び実施

① ＣＩＳＯは、情報セキュリティに関する研修及び特定個人情報の安全管理に関する研修について、研修計画の策定及びその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

② 研修計画において、受講すべき職員等は毎年度最低１回は必要な研修を受講できるようにしなければならない。

③ 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④ 情報セキュリティ研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、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ものにしなければならない。

⑤ 特定個人情報の安全管理に関する研修は、保護責任者、保護管理者及び特定個人情報取扱者に対し、それぞれの役割等に応じて、特定個人情報の適正な取扱いについて理解を深め、特定個人情報の保護に関する意識の高揚を図るための啓発その他必要な事項に関するものでなければならない。

⑥ ＣＩＳＯは、毎年度１回、情報セキュリティ委員会に対して、情報セキュリティ研修及び特定個人情報の安全管理に関する研修の実施状況について報告しなければならない。

（３）　緊急時対応訓練

ＣＩＳＯは、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、又は効果的に実施できるようにしなければならない。

（４）　研修・訓練への参加

① 幹部を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

② 情報セキュリティ責任者及び保護責任者並びに情報セキュリティ管理者及び保護管理者は、受講すべき職員等に研修参加の機会を付与するなどの必要な措置を講じなければならない。

７－３　情報セキュリティインシデントの報告

（１）　庁内での情報セキュリティインシデントの報告

① 職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及、保護管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

② 報告を受けた情報セキュリティ管理者及び保護管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③ 情報セキュリティ管理者及び保護管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてＣＩＳＯ及び情報セキュリティ責任者及び保護責任者に報告しなければならない。

（２）　住民等外部からの情報セキュリティインシデントの報告

① 職員等は、市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者及び保護管理者に報告しなければならない。

② 報告を受けた情報セキュリティ管理者及び保護管理者は、速やかに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に関する統一的な窓口に報告しなければならない。

③ 情報セキュリティ管理者及び保護管理者は、当該情報セキュリティインシデントについて、必要に応じてＣＩＳＯ及び情報セキュリティ責任者及び保護責任者に報告しなければならない。

（3）　情報セキュリティインシデント原因の究明・記録、再発防止等

① ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

② ＣＳＩＲＴは、情報セキュリティインシデントであると評価した場合、ＣＩＳＯに速やかに報告しなければならない。

③ ＣＳＩＲＴは、情報セキュリティインシデントに関係する情報セキュリティ責任者及び保護責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

④ ＣＳＩＲＴは、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。この場合において、ＣＳＩＲＴは、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、ＣＩＳＯに報告しなければならない。

⑤ ＣＩＳＯは、ＣＳＩＲＴから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

７－４　ＩＤ及びパスワード等の管理

（1）　ＩＣカード等の取扱い

① 職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

（ア）　認証に用いるＩＣカード等を職員等間で共有してはならない。

（イ）　業務上必要のないときは、ＩＣカード等をカードリーダ、パソコン等の端末のスロット等から抜いておかなければならない。

（ウ）　ＩＣカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

② 統括情報セキュリティ責任者及び情報システム管理者は、ＩＣカード等の紛失等の通報があった場合は、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

③　統括情報セキュリティ責任者及び情報システム管理者は、ＩＣカード等を切り替える場合は、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（２）　ＩＤの取扱い

職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

①　自己が利用しているＩＤは、他人に利用させてはならない。

②　共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（３）　パスワードの取扱い

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。

①　パスワードは、他者に知られないように管理しなければならない。

②　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てはならない。

③　パスワードは、十分な長さとし、文字列は想像しにくいものにしなければならない。

④　パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑥　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

⑦　サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

⑧　職員等間でパスワードを共有してはならない（ただし共有ＩＤに対するパスワードは除く）。

８　技術的セキュリティ

８－１　コンピュータ及びネットワークの管理

（１）　ファイルサーバの設定等

① 情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

② 情報システム管理者は、ファイルサーバを課室所等の単位で構成し、職員等が他課室所等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③ 情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途フォルダを作成する等の措置を講じ、同一課室所等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（２）　バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について、必要に応じて定期的にバックアップを実施しなければならない。

（３）　他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェ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、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

（４）　システム管理記録及び作業の確認

① 情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

② 統括情報セキュリティ責任者及び情報システム管理者は、所管する情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

③ 統括情報セキュリティ責任者及び情報システム管理者は、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がシステム変更等の作業を行う場合は、必要に応じて２名以上で作業させ、互いにその作業を確認させなければならない。

（５） 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等の情報資産について、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

（６） ログの取得等

① 統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③ 統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（７） 障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を障害記録として記録し、適正に保存しなければならない。

（８）　ネットワークの接続制御、経路制御等

① 統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

② 統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（９）　外部の者が利用できる情報システムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できる情報システムについて、必要に応じ他のネットワーク及び情報システムと分離する等の措置を講じなければならない。

(10)　外部ネットワークとの接続制限等

① 情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、ＣＩＳＯ及び統括情報セキュリティ責任者の許可を得なければならない。

② 情報システム管理者は、接続しようとする外部ネットワークに係るセキュリティ技術等を詳細に調査し、庁内のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ 情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん、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、必要に応じて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。

④ 統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤ 情報システム管理者は、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、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを遮断しなければならない。

(11)　複合機のセキュリティ管理

① 統括情報セキュリティ責任者は、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器（以下「複合機」という。）を調達する場合は、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

② 統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③ 統括情報セキュリティ責任者は、複合機の運用を終了する場合は、複合機の持つ電磁的記録媒体のすべての情報を抹消又は再利用できないようにする対策を講じなければならない。

(12)　特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、ＩＰ電話システム、ネットワークカメラシステム等の特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(13)　無線ＬＡＮ及びネットワークの盗聴対策

① 統括情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合は、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

② 統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(14)　電子メールのセキュリティ管理

① 統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

② 統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③　統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④　統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤　統括情報セキュリティ責任者は、情報システムの開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

⑥　統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じなければならない。

(15)　電子メールの利用制限

①　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

⑤　職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。

(16)　電子署名・暗号化

①　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、ＣＩＳＯが定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

②　職員等は、暗号化を行う場合にＣＩＳＯが定める以外の方法を用いてはならない。この場合において、職員等は、ＣＩＳＯが定めた方法で暗号のための鍵を管理しなければならない。

③　ＣＩＳＯは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17)　無許可ソフトウェアの導入等の禁止

① 職員等は、パソコン及びモバイル端末に無断でソフトウェアを導入してはならない。

② 職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。

③ 情報セキュリティ管理者又は情報システム管理者は、導入するソフトウェアのライセンスを管理しなければならない。

④ 職員等は、不正にコピー、改ざん等されたソフトウェアを利用してはならない。

(18)　機器構成の変更の制限

① 職員等は、パソコン及びモバイル端末に対し無断で機器の改造、増設及び交換を行ってはならない。

② 職員等は、業務上、パソコンやモバイル端末に対し機器の改造、増設及び交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

(19)　無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコン及びモバイル端末をネットワークに接続してはならない。

(20)　業務以外の目的でのウェブ閲覧の禁止

① 職員等は、業務以外の目的でウェブを閲覧してはならない。

② 統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

８－２　アクセス制御

（１）　アクセス制御

①　アクセス制御等

統括情報セキュリティ責任者又は情報システム管理者等は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

②　利用者ＩＤの取扱い

(ア)　統括情報セキュリティ責任者及び情報システム管理者は、所管する情報システムに係る利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

(イ)　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

(ウ)　統括情報セキュリティ責任者及び情報システム管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

③　特権を付与されたＩＤの管理等

(ア)　統括情報セキュリティ責任者及び情報システム管理者は、所管する情報システムに係る管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

(イ)　統括情報セキュリティ責任者及び情報システム管理者の特権を付与されたＩＤを利用する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、ＣＩＳＯが認めた者でなければならない。

(ウ)　ＣＩＳＯは、特権を付与されたＩＤを利用する者を認めた場合は、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

(エ)　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ）　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等のパスワードよりも入力回数制限等のセキュリティ機能を強化しなければならない。

（カ）　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

（２）　職員等による外部からのアクセス等の制限

①　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

②　統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③　統括情報セキュリティ責任者は、外部からのアクセスを認める場合は、システム上利用者の本人確認を行う機能を確保しなければならない。

④　統括情報セキュリティ責任者は、外部からのアクセスを認める場合は、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤　統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合は、セキュリティ確保のために必要な措置を講じなければならない。

⑥　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑦　統括情報セキュリティ責任者は、公衆通信回線（公衆無線ＬＡＮ等）の庁外通信回線を庁内ネットワーク（住民開放系ネットワークを除く）に接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等の情報セキュリティ確保のために必要な措置を講じなければならない。

（３）　ログイン時の表示等

情報システム管理者は、所管する情報システムについて、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、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よう情報システムを設定しなければならない。

（４）　認証情報の管理

① 統括情報セキュリティ責任者又は情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。この場合において、認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能があるときは、これを有効に活用しなければならない。

② 統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回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。

③ 統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（５）　特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

８－３　情報システムの開発、導入、保守等

（１）　情報システムの調達

① 統括情報セキュリティ責任者及び情報システム管理者は、情報システムの開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）　情報システムの開発

①　システム開発における責任者及び作業者の特定

情報システム管理者は、情報システムの開発の責任者及び作業者を特定するとともに、開発のための規則を確立しなければならない。

②　システム開発における責任者、作業者のＩＤの管理

（ア）　情報システム管理者は、情報システムの開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）　情報システム管理者は、情報システムの開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③　システム開発に用いるハードウェア及びソフトウェアの管理

（ア）　情報システム管理者は、情報システムの開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）　情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合は、当該ソフトウェアを情報システムから削除しなければならない。

（３）　情報システムの導入

①　開発環境と運用環境の分離及び以降手順の明確化

（ア）　情報システム管理者は、情報システムの開発・保守及びテスト環境から情報システムの運用環境への移行について、情報システムの開発・保守計画の策定時に手順を明確にしなければならない。

（イ）　情報システム管理者は、移行の際、情報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、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（ウ）　情報システム管理者は、導入する情報システムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

②　テスト

（ア）　情報システム管理者は、新たに情報システムを導入する場合は、既に稼働している情報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）　情報システム管理者は、運用テストを行う場合は、あらかじめ擬似環境に

よる操作確認を行わなければならない。

（ウ）　情報システム管理者は、個人情報及び機密性の高いデータを、テストデータに使用してはならない。

（エ）　情報システム管理者は、開発した情報システムについて受け入れテストを行う場合は、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（４）　情報システムの開発・保守に関連する資料等の整備・保管

① 情報システム管理者は、情報システムの開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

② 情報システム管理者は、テスト結果を一定期間保管しなければならない。

③ 情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

（５）　情報システムにおける入出力データの正確性の確保

① 情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② 情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③ 情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（６）　情報システムの変更管理

情報システム管理者は、情報システムを変更した場合は、プログラム仕様書等の変更履歴を作成しなければならない。

（７）　開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新、又はパッチの適用

をする場合は、他の情報システムとの整合性を確認しなければならない。

（８）　システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

８－４　不正プログラム対策

（１）　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

① 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの情報システムへの侵入を防止しなければならない。

② 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③ コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④ 所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑥ 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

（２）　情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

① 情報システム管理者は、その所管するサーバ及びパソコン等の端末にコンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

② 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

③　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

④　電磁的記録媒体を使う場合は、コンピュータウイルス等の感染を防止するため、市が管理している媒体以外を職員等に利用させてはならない。

⑤　インターネットに接続していない情報システムにおいて、不正プログラムの感染又は侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

（３）　職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

②　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを、ＬGWAN接続系に取込む場合は無害化しなければならない。

⑤　統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑥　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

（ア）　パソコン等の端末の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。

（イ）　モバイル端末の場合は、直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

８－５　不正アクセス対策

（１）　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

① 使用されていないポートを閉鎖しなければならない。

② 不要なサービスについて、機能を削除又は停止しなければならない。

③ 不正アクセスによるウェブページの改ざんを防止するため、データの書き換えを検出した場合に、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、必要な設定を行わなければならない。

④ 情報システムの設定に係る重要なファイルについて、定期的に当該ファイルの改ざんの有無を検査しなければならない。

⑤ 統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（２）　攻撃への対処

ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、情報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、ＣＩＳＯ及び統括情報セキュリティ責任者は、総務省、秋田県等と連絡を密にして情報の収集に努めなければならない。

（３）　記録の保存

ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（４）　内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５）　職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室所等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

（６）　サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（７）　標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育、自動再生無効化等の人的対策及び入口対策を講じなければならない。この場合において、統括情報セキュリティ責任者及び情報システム管理者は、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

８－６　セキュリティ情報の収集

（１）　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。この場合において、統括情報セキュリティ責任者及び情報システム管理者は、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（２）　不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（３）　情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識したときは、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

９　運用

９－１　情報システムの監視

① 統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

② 統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③ 統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続する情報システムを常時監視しなければならない。

９－２　情報セキュリティポリシーの遵守状況の確認

（１）　遵守状況の確認及び対処

① 情報セキュリティ責任者及び保護責任者並びに情報セキュリティ管理者及び保護管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにＣＩＳＯ及び統括情報セキュリティ責任者に報告しなければならない。

② ＣＩＳＯは、発生した問題について、適正かつ速やかに対処しなければならない。

③ 統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（２）　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

ＣＩＳＯ及びＣＩＳＯが指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３）　職員等の報告義務

① 職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに

統括情報セキュリティ責任者並びに情報セキュリティ管理者及び保護責任者に報告を行わなければならない。

② 当該違反行為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統括情報セキュリティ責任者が判断した場合において、職員等は緊急時対応計画に従って適正に対処しなければならない。

９－３ 侵害時の対応等

（１） 緊急時対応計画の策定

ＣＩＳＯ又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（２） 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

① 関係者の連絡先

② 発生した事案に係る報告すべき事項

③ 発生した事案への対応措置

④ 再発防止措置の策定

（３） 業務継続計画との整合性確保

市が自然災害等に備えて業務継続計画を策定する場合、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（４） 緊急時対応計画の見直し

ＣＩＳＯ又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

９－４　例外措置

（１）　例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、ＣＩＳＯの許可を得て、例外措置を講じることができる。

（２）　緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにＣＩＳＯに報告しなければならない。

（３）　例外措置の申請書の管理

ＣＩＳＯは、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

９－５　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及び特定個人情報を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

① 地方公務員法（昭和２５年法律第２６１号）
② 著作権法（昭和４５年法律第４８号）
③ 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）
④ 個人情報の保護に関する法律（平成１５年法律第５７号）
⑤ 番号法
⑥ サイバーセキュリティ基本法（平成２８年法律第３１号）
⑦ 横手市個人情報保護条例（平成１７年横手市条例第２４号）

９－６　懲戒処分等

（１）　懲戒処分

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。

（２）　違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

① 統括情報セキュリティ責任者が違反を確認した場合、統括情報セキュリティ責任者は、当該職員等が所属する課室所等の情報セキュリティ管理者及び保護管理者に通知し、適正な措置を求めなければならない。

② 情報システム管理者等が違反を確認した場合、違反を確認した者は、速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室所等の情報セキュリティ管理者及び保護管理者に通知し、適正な措置を求めなければならない。

③ 情報セキュリティ管理者及び保護管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用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、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨をＣＩＳＯ及び当該職員等が所属する課室所等の情報セキュリティ管理者及び保護管理者に通知しなければならない。

１０　外部サービスの利用

１０－１　外部委託

（１）　外部委託事業者の選定基準

① 情報セキュリティ管理者及び保護管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策及び特定個人情報の安全管理措置の実施が確保されることを確認しなければならない。

② 情報セキュリティ管理者及び保護管理者は、機密性２以上の情報資産を取り扱う業務を委託する場合は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

③ 情報セキュリティ管理者及び保護管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

④ 保護管理者は、特定個人情報の取扱いに係る業務を外部に委託する場合には、特定個人情報の適切な管理を行う能力を有しない者を選定することがないようにしなければならない。

（２）　契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

① 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

② 外部委託事業者の責任者、委託内容、作業者の所属及び作業場所の特定

③ 提供されるサービスレベルの保証

④ 外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法

⑤ 外部委託事業者の従業員に対する教育の実施

⑥ 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の禁止

⑦ 業務上知り得た情報の守秘義務

⑧ 再委託の制限又は事前承認等の再委託に係る条件に関する事項の遵守

⑨ 委託業務終了時の情報資産又は特定個人情報の返還、廃棄等

⑩　委託業務の定期報告及び緊急時報告義務

⑪　市による監査及び検査

⑫　市による情報セキュリティインシデント発生時の公表

⑬　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）

（３）　再委託等

保護管理者は、委託先において、特定個人情報の取扱いに係る業務が再委託される場合には、委託先に上記１０－１（２）に規定する措置を講じさせるとともに、再委託される業務に係る特定個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが上記１０－１（２）に規定する措置を実施するものとする。特定個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

（４）　確認・措置等

情報セキュリティ管理者及び保護管理者は、外部委託事業者において必要なセキュリティ対策及び特定個人情報の適正な管理が確保されていることを定期的に確認し、必要に応じ、上記１０－１（２）の契約に基づき措置を実施しなければならない。この場合において、情報セキュリティ管理者及び保護管理者は、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

１０－２　約款による外部サービスの利用

（１）　約款による外部サービスの利用に係る規定の整備等

情報セキュリティ管理者は、約款による外部サービスを利用する場合は、当該利用にかかる次の項目を含む規定をあらかじめ整備し、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

①　約款によるサービスを利用して良い範囲

②　業務により利用する約款による外部サービス

③　利用手続及び運用手順

④　機密性２以上の情報を取り扱わないこと。

（２）　約款による外部サービスの利用における対策の実施

職員等は、上記１０－２（１）の規定に基づき約款による外部サービスを利用する場合は、当該サービスの約款その他提供条件から、利用にあたってのリスクが許容できることを確認した上で当該サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

（３）　ソーシャルメディアサービスの利用

① 情報セキュリティ管理者は、市が管理するアカウントでソーシャルメディアサービスを利用する場合は、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ア）　市のアカウントによる情報発信が、実際に市が行うものであることを明らかにするため、市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

（イ）　パスワード、認証のためのコード等の認証情報及びこれを記録した媒体（ＩＣカード等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

② 機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

③ 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

１１　評価・見直し

１１－１　監査

（１）　実施方法

① ＣＩＳＯは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策の状況について、毎年度及び必要に応じて監査を行わせなければならない。

② ＣＩＳＯは、特定個人情報に関する監査統括責任者を指名し、特定個人情報の安全管理の状況について、毎年度及び必要に応じて監査を行わせなければならない。

③ 情報セキュリティ監査統括責任者と特定個人情報に関する監査統括責任者は、同じ者が兼務することができる。

（２）　監査を行う者の要件

① 情報セキュリティ監査統括責任者及び特定個人情報に関する監査統括責任者（以下、「監査統括責任者」という。）は、監査を実施する場合には、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。

② 情報セキュリティ監査を行う者は、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。

③ 特定個人情報に関する監査を行う者は、監査及び特定個人情報の安全管理に関する専門知識を有する者でなければならない。

（３）　監査実施計画の立案及び実施への協力

① 監査統括責任者は、監査を行うにあたって、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。

② 被監査部門は、監査の実施に協力しなければならない。

（４）　外部委託事業者に対する監査

① 監査統括責任者は、情報セキュリティ対策を要する業務を外部委託する場合、外部委託事業者及び再委託を認める場合の再委託先事業者において、必要な情報セキュリティ対策が確保されていることを確認するため、定期的に又は必要に応じて監

査を実施しなければならない。

② 監査統括責任者は、特定個人情報を取り扱う業務を外部委託する場合は、外部委託事業者及び再委託を認める場合の再委託先事業者において、番号法に基づき市が果たすべき安全管理措置と同等の措置が講じられていることを確認するため、定期的に又は必要に応じて監査を実施しなければならない。

（５） 報告

監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（６） 保管

監査統括責任者は、監査の実施を通して収集した監査証拠及び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正に保管しなければならない。

（７） 監査結果への対応

① ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者及び保護管理者に対し、当該事項への対処を指示しなければならない。

② ＣＩＳＯは、指摘事項を所管していない情報セキュリティ管理者及び保護管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（８） 情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策及び特定個人情報の安全管理の見直し時に活用しなければならない。

１１－２ 自己点検

（１） 実施方法

① 統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク

及び情報システムについて、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。

② 情報セキュリティ責任者及び保護責任者は、情報セキュリティ管理者及び保護管理者と連携して、所管する部局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及び特定個人情報の安全管理の状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（２） 報告

統括情報セキュリティ責任者、情報システム管理者並びに情報セキュリティ責任者及び保護責任者は、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。

（３） 自己点検結果の活用

① 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。

② 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及び特定個人情報の安全管理の見直し時に活用しなければならない。

１１－３ 情報セキュリティポリシー及び関係規程等の見直し等

情報セキュリティ委員会は、情報セキュリティポリシー及び関係規程等について、情報セキュリティ監査、特定個人情報に関する監査及び自己点検の結果並びに情報セキュリティ及び特定個人情報の安全管理に関する状況の変化等を踏まえて定期的に見直しを行い、必要があると認めた場合、その改定を行うものとする。ただし、緊急を要する場合又は軽微な改定については、ＣＩＳＯの判断で改定を行い、事後速やかに情報セキュリティ委員会に報告するものとする。

附　則

この基準は、平成３０年８月１日から施行する。

附　則（令和元年７月２２日横手市情報セキュリティ委員会決定）

この基準は、令和元年８月１日から施行する。