吹田市情報セキュリティポリシー

この情報セキュリティポリシーは、吹田市情報システム等管理運営要領（平成30年9月1日制定）第4条に基づき、情報セキュリティ対策について総合的かつ具体的に取りまとめたものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

Ⅰ　情報セキュリティ基本方針

1　目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2　定義

（1）　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（2）　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（3）　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（4）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5）　機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

（6）　完全性

情報資産が破壊、改ざん又は消去されていない状態を確保することをいう。

（7）　可用性

情報資産にアクセスすることを認められた者が、必要なときに中断されることなく、情報資産にアクセスできる状態を確保することをいう。

（8）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（9）　LGWAN 接続系

LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（１０）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１１）通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１２）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）地震、落雷、火災、停電等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

４　適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、市長、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、議会事務局、水道事業管理者及び消防長をいう。適用行政機関の範囲外であっても、本基本方針の対象となる情報システムを利用する場合にあっては、本基本方針の適用範囲とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　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。)

ウ　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

５　職員等の遵守義務

常勤職員、会計年度任用職員及び臨時的任用職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって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を遵守しなければならない。

６　情報セキュリティ対策

上記３の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。

（1） 組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（2） 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（3） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

ア　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

イ　LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、大阪府と府下市町村のインターネット接続口を集約した大阪版自治体情報セキュリティクラウドの導入等を実施する。

（4） 物理的セキュリティ

情報処理機器、通信回線及びそれらを設置している施設等の管理について、物理的な対策を実施する。

（5） 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（6） 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。

（8） 業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者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、必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービス

の運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

（9） 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7　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の遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

上記6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた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、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから、非公開とする。

Ⅱ 情報セキュリティ対策基準

1 組織体制

（1） 最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

ア 吹田市情報システム等管理運営要領（平成 30 年 9 月 1 日制定。以下「要領」という。）第 3 条に定める CISO を CISO とする。CISO は、本市における全てのネットワーク、情報システム等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。

イ CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

ウ 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（CSIRT: Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

エ CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。）１人を必要に応じて置く。

オ CISO は、本対策基準に定められた自らの担務を、副 CISO、統括管理者及び情報セキュリティ責任者に担わせることができる。

（2） 統括管理者

ア 要領第 3 条に定める統括管理者を、CISO 直属の統括管理者とする。統括管理者は CISO 及び副 CISO を補佐するものとする。

イ 統括管理者は、本市の全てのネットワーク、情報システム等における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ 統括管理者は、本市の全てのネットワーク、情報システム等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。

（3） 情報セキュリティ責任者

ア 要領第 3 条に定める情報セキュリティ責任者を、情報セキュリティ責任者とする。

イ 情報セキュリティ責任者は、その所管する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。

ウ 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。

エ 情報セキュリティ責任者は、外部サービス（後述する重要性区分Ⅰ又はⅡの

情報を取り扱わない場合）の利用申請を審査し、利用の可否を決定する権限及び責任を有する。

（4） ネットワーク管理者

ア　要領第3条に定めるネットワーク管理者をネットワーク管理者とする。

イ　ネットワーク管理者は、管理責任者及びシステムマネージャに対して、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。

ウ　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、必要に応じ本対策基準、実施手順その他の関連文書の維持、保守及び改訂を行わなければならない。

エ　ネットワーク管理者は、本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 及び統括管理者の指示に従い、両者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

オ　ネットワーク管理者は、本市の全てのネットワーク、情報システム等に関する実施手順の維持及び管理を行う権限並びに責任を有する。

カ　ネットワーク管理者は、緊急時等の円滑な情報共有を図るため、CISO、統括管理者、情報セキュリティ責任者、管理責任者及びシステムマネージャ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。

キ　ネットワーク管理者は、緊急時には CISO 及び統括管理者に早急に報告を行うとともに、回復のための対策を実施しなければならない。

ク　ネットワーク管理者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

（5） 利用申請の許可権限者

ア　要領第3条に定める利用申請の許可権限者を、利用申請の許可権限者とする。

イ　利用申請の許可権限者は、外部サービス（後述する重要性区分Ⅰ又はⅡの情報を取り扱う場合）の利用申請を審査し、利用の可否を決定する権限及び責任を有する。

（6） 管理責任者

ア　要領第3条に定める管理責任者を、管理責任者とする。

イ　管理責任者はその所管する室課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。

ウ　管理責任者は、その所管する室課等において、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

エ　管理責任者は、その所管する室課等において、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、CISO、統括管理者、情報セキュリティ責任者及びネットワーク管理者へ速やかに報告を行い、指示を仰がなければならない。

オ　管理責任者は、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。

カ　管理責任者は、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。

キ　管理責任者は、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策定、維持及び管理を行う。

（7） 外部サービス管理者

ア　要領第 3 条に定める外部サービス管理者を、外部サービス管理者とする。

イ　外部サービス管理者は､外部サービスを利用した情報システムの導入･構築、運用・保守、更改・廃棄において規定されたセキュリティ対策の実施状況を確認・記録する。

（8） クラウドサービス管理者

ア　要領第 3 条に定めるクラウドサービス管理者を、クラウドサービス管理者とする。

イ　クラウドサービス管理者は、クラウドサービスを利用した情報システムの導入・構築、運用・保守、更改・廃棄において規定されたセキュリティ対策の実施状況を確認・記録する。

（9） システムマネージャ

ア　管理責任者が指定する常勤職員を、システムマネージャとする。

イ　システムマネージャは、管理責任者の指示等に従い、情報システムの開発、設定の変更、運用、更新、システム利用のための申請手続き等の作業を行う。

（１０）兼務の禁止

ア　情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は､同じ者が兼務してはならない。

イ　情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

（１１）CSIRT の設置・役割

ア　CISO は、CSIRT を整備し、その役割を明確化しなければならない。

イ　CISO は、CSIRT に所属する職員を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

ウ　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しなければならない。

エ　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しなければならない。

オ　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、都道府県等へ報告しなければならない。

カ　　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・公表対応を行わなければならない。

キ　　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、委託事業者等との情報共有を行わなければならない。

（１２）クラウドサービス利用における組織体制

統括管理者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

２　情報資産の分類と管理

（１）　情報資産の分類

管理責任者は、情報資産を機密性、完全性、可用性の３つの側面から分析し、重要性に応じ次のとおり分類し、必要に応じ取扱制限を行うものとする。

重要性区分	内容	具体例	取扱制限
Ⅰ	セキュリティ侵害が、市民の権利、利益等へ重大な影響を及ぼす情報資産	・マイナンバー利用事務系で扱う情報や個人情報等 ・マイナンバー利用事務系を構成するサーバ等	・支給以外の端末での作業の原則禁止（重要性区分Ⅰ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、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、情報資産の運搬・提供時における暗号化・パスワード設定や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 ・バックアップ、指定する時間以内の復旧
Ⅱ	セキュリティ侵害が、事務の執行等に重大な影響を及ぼす情報資産	・非公開の入札情報、情報システムの手順書、マニュアル等 ・マイナンバー利用事務系以外のネットワークを構成するサーバ等	
Ⅲ	セキュリティ侵害が、事務の執行等に軽微な影響を及ぼす情報資産	・通常業務で扱う事務に関する情報資産	

（２）　情報資産の管理

ア　管理責任

（ア）　管理責任者は、その所管する情報資産について管理責任を有する。

（イ）　情報資産が複製又は伝送された場合には、複製された情報資産も（１）の分類に基づき管理しなければならない。

（ウ）　管理責任者は、クラウドサービスの環境に保存される情報資産についても（１）の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

イ　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、情報資産の重要性区分を表示し、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。

ウ　情報の作成

（ア）　職員等は、業務上必要のない情報を作成してはならない。

（イ）　情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の重要性区分と取扱制限を定めなければならない。

（ウ）　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

エ　情報資産の入手

（ア）　職員等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重要性区分に基づいた取扱いをしなければならない。

（イ）　職員等でない者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報資産の重要性区分と取扱制限を定めなければならない。

（ウ）　情報資産を入手した者は、入手した情報資産の重要性区分が不明な場合、管理責任者に判断を仰がなければならない。

オ　情報資産の利用

（ア）　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。

（イ）　情報資産を利用する者は、情報資産の重要性区分に応じ、適正な取扱いをしなければならない。

（ウ）　情報資産を利用する者は、電磁的記録媒体に情報資産の重要性区分が異なる情報が複数記録されている場合、記録されている情報のうち重要性区分が最も高いものの分類に従って、当該電磁的記録媒体を取り扱わなければならない。

カ　情報資産の保管

（ア）　管理責任者は、情報資産の重要性区分に従って、情報資産を適正に保管しなければならない。

（イ）　管理責任者は、情報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。

（ウ）　管理責任者は、重要性区分Ⅰ又はⅡの情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び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。

キ　情報の送信

電子メール等により重要性区分Ⅰ又はⅡの情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

ク　情報資産の運搬

（ア）　車両等により重要性区分Ⅰ又はⅡ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、パスワード等による暗号化を行う等、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。

（イ）　重要性区分Ⅰ又はⅡの情報資産を運搬する者は、管理責任者に許可を得なければならない。

ケ　情報資産の提供・公表

（ア）　重要性区分Ⅰ又はⅡの情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）　重要性区分Ⅰ又はⅡの情報資産を外部に提供する者は、管理責任者に許可を得なければならない。

（ウ）　管理責任者は、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。

コ　情報資産の廃棄等

（ア）　情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報資産の分類に応じ、情報を復元できないように処置しなければならない。

（イ）　情報資産の廃棄やリース返却等を行う者は、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。

（ウ）　情報資産の廃棄やリース返却等を行う者は、管理責任者の許可を得なければならない。

（エ）　クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

3　情報システム全体の強靭性の向上

（1）　マイナンバー利用事務系

ア　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、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

イ　情報のアクセス及び持ち出しにおける対策

（ア）　情報のアクセス対策

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。また、業務毎に専用端末を設置することが望ましい。

（イ）　情報の持ち出し不可設定

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。

ウ　マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

エ　マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

（２）　LGWAN 接続系

ア　LGWAN 接続系 とインターネット接続系の分割

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。なお、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本文のみLGWAN 接続系に転送するメールテキスト化方式

（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

（ウ）　危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

イ　LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

（3）　インターネット接続系

ア　　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。

イ　　府下市町村のインターネットとの通信を集約する大阪版自治体情報セキュリティクラウドに参加するとともに、関係省庁や大阪府と連携しながら、情報セキュリティ対策を推進しなければならない。

ウ　業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末もしくは入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

4　物理的セキュリティ

（1）　サーバ等の管理

ア　機器の取付け

管理責任者は、サーバ等の機器の取付けを行う場合、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。

イ　サーバの冗長化

管理責任者は、重要性区分Ⅰ又はⅡの情報を格納しているサーバについては、データを二重化する等障害時にシステムの運用停止時間を最小限にしなければならない。

ウ　機器の電源

（ア）　管理責任者は、ネットワーク管理者及び施設管理部門と連携し、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。

（イ）　管理責任者は、ネットワーク管理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。

エ　通信ケーブル等の配線

（ア）　ネットワーク管理者及び管理責任者は、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、必要な措置を実施しなければならない。

（イ）　ネットワーク管理者及び管理責任者は、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、連携して対応しなければならない。

（ウ）　ネットワーク管理者及び管理責任者は、ネットワーク接続口（ハブのポート等）を職員等でない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。

（エ）　ネットワーク管理者及び管理責任者は、システムマネージャ及び契約により操作を認められた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。

オ　機器の定期保守及び修理

（ア）　管理責任者は重要性区分Ⅰ又はⅡ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。

（イ）　管理責任者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、設置場所で行わせなければならない。設置場所から持ち出す場合、管理責任者は、事業者に故障を修理させるにあたり、当該事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

カ　庁外への機器の設置

ネットワーク管理者及び管理責任者は、本対策基準が適用される実施機関が管理する施設以外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、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。

キ　機器の廃棄等

（ア）　管理責任者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を実施しなければならない。

（イ）　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用で

きる。

（２） 管理区域（サーバ室等）の管理

ア　管理区域の構造等

（ア）　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、当該機器等の管理及び運用を行うための部屋（以下「サーバ室」という。）や電磁的記録媒体の保管庫が設定された部屋をいう。

（イ）　ネットワーク管理者及び管理責任者は、管理区域を原則として地階又は１階に設けてはならない。また、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。

（ウ）　ネットワーク管理者及び管理責任者は、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、電子錠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。

（エ）　ネットワーク管理者及び管理責任者は、サーバ室内の機器等に、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。

（オ）　ネットワーク管理者及び管理責任者は、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等に影響を与えないようにしなければならない。

イ　管理区域の入退室管理等

（ア）　管理責任者は、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。

（イ）　職員等及び委託事業者は、管理区域に入室する場合、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。

（ウ）　管理責任者は、外部からの訪問者が管理区域に入る場合には、名札の着用等を求め、必要に応じて立入区域を制限したうえで、管理区域への入退室を許可された常勤職員を付き添わせなければならない。

（エ）　管理責任者は、重要性区分Ⅰ又はⅡの情報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、電磁的記録媒体等の持込みを管理しなければならない。

ウ　機器等の搬入出

（ア）　管理責任者は、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事業者に確認を行わせなければならない。

（イ）　管理責任者は、管理区域内で機器等を搬入出する場合は、その安全性について確認し、常勤職員を立会わせなければならない。

（３） 通信回線及び通信回線装置の管理

ア　ネットワーク管理者は、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。また、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。

イ　ネットワーク管理者は、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。

ウ　ネットワーク管理者は、行政系のネットワークを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。

エ　ネットワーク管理者は、重要性区分Ⅰ又はⅡ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。また、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。

オ　ネットワーク管理者は、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。

カ　ネットワーク管理者は、重要性区分Ⅰ又はⅡ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。また、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。

（4）　職員等の利用する端末や電磁的記録媒体等の管理

（非公開）

5　人的セキュリティ

（1）　職員等の遵守事項

ア　職員等の遵守事項

（ア）　情報セキュリティポリシー等の遵守

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。また、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がある場合は、速やかに管理責任者に相談し、指示を仰がなければならない。

（イ）　業務以外の目的での使用の禁止

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。

（ウ）　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

a　CISO は、重要性区分Ⅰ又はⅡ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。

b　職員等は、本市のモバイル端末、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、管理責任者の許可を得なければならな

い。

c　職員等は、外部で情報処理業務を行う場合には、管理責任者の許可を得なければならない。

（エ）　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の業務利用

a　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、支給以外の端末の業務利用の可否判断を CISO が行った後に、業務上必要な場合は、実施手順に従い、管理責任者の許可を得て利用することができる。

b　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用いる場合には、管理責任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。

（オ）　持ち出し及び持ち込みの記録

管理責任者は、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。

（カ）　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

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管理責任者の許可なく変更してはならない。

（キ）　机上の端末等の管理

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管理責任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や電磁的記録媒体、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。

（ク）　退職時等の遵守事項

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。また、その後も、業務上知り得た情報を漏らしてはならない。

（ケ）　クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

イ　会計年度任用職員及び臨時的任用職員への対応

（ア）　情報セキュリティポリシー等の遵守

管理責任者は、会計年度任用職員及び臨時的任用職員に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員及び臨時的任用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。

（イ）　情報セキュリティポリシー等の遵守に対する同意

管理責任者は、会計年度任用職員及び臨時的任用職員の採用の際、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。

（ウ）　インターネット接続及び電子メール使用等の利用制限

管理責任者は、会計年度任用職員及び臨時的任用職員にパソコンや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、これを利用できないようにしなければならない。

ウ　情報セキュリティポリシー等の掲示

管理責任者は、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。

エ　委託事業者に対する説明

管理責任者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち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。

（２）　情報セキュリティに関する研修・訓練

ア　研修計画の策定及び実施

（ア）　CISO は、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。また、幹部を含め全ての職員等は、定められた研修及び訓練に参加しなければならない。

（イ）　CISO は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

イ　研修計画の策定及び実施

（ア）　CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画を策定しなければならない。

（イ）　研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

（ウ）　研修計画において、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するようにしなければならない。

（エ）　研修は、統括管理者、情報セキュリティ責任者、ネットワーク管理者、管理責任者、システムマネージャ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。

（オ）　管理責任者は、所管する課室等の研修の実施状況を記録し、統括管理者及び情報セキュリティ責任者に対して、報告しなければならない。

（カ）　統括管理者は、研修の実施状況を分析、評価し、CISO に情報セキュリティ対策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。

（キ）　統括管理者は、毎年度１回、CISO に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

ウ　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、また、効果的に実施できるようにしなければならない。

（３）　情報セキュリティインシデントの報告

ア　庁内からの情報セキュリティインシデントの報告

（ア）　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、速やかにシステムマネージャ及び管理責任者に報告しなければならない。

（イ）　報告を受けたシステムマネージャ及び管理責任者は、速やかに情報セキュリティ責任者及び CSIRT に報告しなければならない。

（ウ）　システムマネージャ及び管理責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

イ　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

（ア）　職員等は、本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、速やかに管理責任者に報告しなければならない。

（イ）　報告を受けた管理責任者は、速やかに情報セキュリティ責任者及び CSIRT に報告しなければならない。

（ウ）　CISO は、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るための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（エ）　統括管理者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

ウ　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

（ア）　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。

（イ）　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。

（ウ）　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。

（エ）　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。また、情報セキュリティインシデントの原因究

明の結果から、再発防止策を検討し、CISO に報告しなければならない。

（オ）　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。

（4）　ID 及びパスワード等の管理

ア　IC カード等の取扱い

（ア）　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。

a　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。

b　業務上必要のないときは、IC カード等をカードリーダ又は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。

c　IC カード等を紛失した場合には、速やかに統括管理者及び管理責任者に通報し、指示に従わなければならない。

（イ）　統括管理者及び管理責任者は、IC カード等の紛失等の通報があり次第、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。

（ウ）　統括管理者及び管理責任者は、IC カード等を切り替える場合、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。

イ　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。

（ア）　職員等は、自己が利用している ID を、他人に利用させてはならない。

（イ）　職員等は、複数の利用者が共通で利用できる ID（以下、「共用 ID」という。）を利用する場合は、共用　ID　の利用許可者以外に利用させてはならない。

ウ　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。

（ア）　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。

（イ）　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。

（ウ）　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。

（エ）　パスワードが流出したおそれがある場合には、管理責任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。

（オ）　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異なる情報システム間で用いてはならない。

（カ）　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。

（キ）　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。

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

6　技術的セキュリティ

（1）　コンピュータ及びネットワークの管理

ア　共有フォルダの設定等

（ア）　管理責任者は、職員等が使用できる共有フォルダの容量を設定し、職員等に周知しなければならない。

（イ）　管理責任者は、共有フォルダを原則として室課等の単位で構成し、職員等が他室課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。

（ウ）　管理責任者は、住民の個人情報、人事記録等、特定の職員等しか取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、同一室課等であっても、担当者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。

（エ）　その他共有フォルダに関する事項は、実施手順等に定める。

イ　バックアップの実施

（ア）　管理責任者は、サーバ等に記録された情報について、サーバの冗長化対策に関わらず、定期的にバックアップを実施しなければならない。

（イ）　管理責任者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本市の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

ウ　他団体との情報システムに関する情報等の交換

管理責任者は、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、その取扱いに関する事項をあらかじめ定め、情報セキュリティ責任者の許可を得なければならない。また、統括管理者にその旨を報告しなければならない。

エ　システム管理記録及び作業の確認

（ア）　管理責任者は、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。

（イ）　管理責任者は、所管するシステムにおいて、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。

（ウ）　管理責任者、システムマネージャ及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、2 名以上で作業する等、作業ミスをしないように努めなければならない。

オ　情報システム仕様書等の管理

管理責任者は、ネットワーク構成図及び情報システム仕様書について、記録媒体の種類に関わらず、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。

カ　ログの取得等

（ア）　管理責任者は、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。

（イ）　管理責任者は、ログとして取得する項目、保存期間、取扱方法等について定め、消去又は改ざんされることがないように適正にログを管理しなければならない。

（ウ）　管理責任者は、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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

（エ）　管理責任者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

キ　障害記録

管理責任者は、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、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。

ク　ネットワークの接続制御、経路制御等

（ア）　管理責任者は、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。

（イ）　管理責任者は、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。

ケ　外部の者が利用できるシステムの分離等

管理責任者は、来庁者向けのタブレットによる庁舎案内システム等、住民等外部の者が利用できるシステムについて、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。

コ　外部ネットワークとの接続制限等

（ア）　管理責任者は、所管するネットワーク及びシステムを外部ネットワークと接続しようとする場合には、CISO の許可を得なければならない。

（イ）　管理責任者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、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。

（ウ）　管理責任者は、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。

（エ）　管理責任者は、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。

（オ）　管理責任者は、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、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遮断しなければならない。

サ　ネットワークに接続するその他機器

（ア）　管理責任者は、複合機、プリンタ、ファクシミリ、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、その他 IoT 関連機器等（以下「複合機等」という。）を調達する場合、当該複合機等が備える機能、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対策を実施しなければなければならない。

（イ）　管理責任者は、複合機等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等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。

（ウ）　管理責任者は、複合機等の運用を終了する場合、複合機等の持つ電磁的記録媒体の全ての情報を抹消する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。

（エ）　管理責任者は、複合機等について、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。

シ　無線 LAN 及びネットワークの盗聴対策

（ア）　管理責任者は、無線 LAN の利用を認める場合、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。

（イ）　管理責任者は、重要性区分Ⅰ又はⅡの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。

ス　電子メールのセキュリティ管理

（ア）　ネットワーク管理者は、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。

（イ）　ネットワーク管理者は、スパムメール等の受信対策を適正に実施しなければならない。また、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止する等適正に対処しなければならない。

（ウ）　ネットワーク管理者は、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制限しなければならない。

（エ）　ネットワーク管理者は、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について職員等に周知しなければならない。

（オ）　ネットワーク管理者は、システム開発や運用、保守等のため庁舎内に常駐している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、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。

（カ）　ネットワーク管理者は、職員等によるメールの送受信を管理責任者が確認できるような対策を実施しなければならない。

（キ）　管理責任者は、情報資産の外部への送信が適正であることを確認するため、職員等が送付するメールを管理しなければならない。

（ク）　その他メールサーバの運用に関する事項は、実施手順に定める。

セ　電子メールの利用制限

（ア）　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。

（イ）　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。

（ウ）　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。

（エ）　職員等は、重要な電子メールを誤送信した場合、管理責任者に報告しなければならない。

（オ）　職員等は、許可されていないフリーメール、フリー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。

ソ　電子署名・暗号化

（ア）　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、電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

（イ）　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。また、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。

（ウ）　統括管理者は、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。

タ　無許可ソフトウェアの導入等の禁止

（ア）　職員等は、パソコンや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。

（イ）　職員等は、業務上の必要がある場合は、管理責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は管理責任者は、ソフトウェアのライセンスを管理しなければならない。

（ウ）　職員等は、不正にコピーしたソフトウェアを利用してはならない。

（エ）　ネットワーク管理者は、アプリケーションソフト等の端末へのインストールが許可なく行われたことを発見した場合は、そのアプリケーションソフト等の使用を停止することができる。

チ　機器構成の変更の制限

（ア）　職員等は、パソコン、モバイル端末及びネットワーク機器に対し機器の改造、増設及び交換を行ってはならない。

（イ）　職員等は、業務上、パソコン、モバイル端末及びネットワーク機器の改造、増設及び交換を行う必要がある場合には、ネットワーク管理者の許可を得なければならない。

（ウ）　ネットワーク管理者は、パソコン、モバイル端末及びネットワーク機器の改造、増設及び交換が許可なく行われたことを発見したときは、その使用を停止することができる。

ツ　　無許可での庁内ネットワーク接続の禁止

（ア）　職員等は、許可なくネットワーク環境の変更を行ってはならない。業務上、ネットワーク機器の増設等の必要が生じたときは、ネットワーク管理者の許可を得なければならない。

（イ）　職員等は、ネットワーク管理者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

（ウ）　ネットワーク管理者は、ネットワーク環境の変更やネットワーク機器の増設が許可なく行われたことを発見したときは、その使用を停止することができる。

テ　　業務外ネットワークへの接続の禁止

（ア）　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう管理責任者によって定められたネットワークと異なるネットワークに接続してはならない。

（イ）　管理責任者及びネットワーク管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限しなければならない。

ト　　業務以外の目的でのウェブ閲覧の禁止

（ア）　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。

（イ）　ネットワーク管理者は、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、管理責任者に通知し適正な措置を求めなければならない。

ナ　Web 会議サービスの利用時の対策

（ア）　統括管理者は、Web 会議を適切に利用するための利用手順を定めなければならない。

（イ）　職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

（ウ）　職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

（エ）　職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

ニ　ソーシャルメディアサービスの利用

（非公開）

（２）　アクセス制御

（非公開）

（３）　システム開発、導入、保守等

ア　情報システムの調達

（ア）　管理責任者は、情報システム開発、導入、保守等の調達に当たっては、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。

（イ）　管理責任者は、機器及びソフトウェアの調達に当たっては、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。

イ　情報システムの開発

（ア）　システム開発における責任者及び作業者の特定

管理責任者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

（イ）　システム開発における責任者、作業者の ID の管理

a　管理責任者は、システム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。

b　管理責任者は、システム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。

（ウ）　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

a　管理責任者は、システム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。

b　管理責任者は、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、当該ソフトウェアをシステムから削除しなければならない。

ウ　情報システムの導入

（ア）　開発環境と運用環境の分離及び移行手順の明確化

a　管理責任者は、原則としてシステム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

b　管理責任者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

c　管理責任者は、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。

d　管理責任者は、導入する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うえで導入しなければならない。

（イ）　テスト

a　管理責任者は、新たに情報システムを導入する場合、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。

b　管理責任者は、運用テストを行う場合、原則としてあらかじめテスト環境による操作確認を行わなければならない。

c　管理責任者は、重要性区分Ⅰ又はⅡのデータを、テストデータに使用してはならない。ただし、情報セキュリティ責任者の許可を得た場合はこの限りではない。

d　管理責任者は、開発したシステムについて受入テストを行う場合、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。

（ウ）　システム開発・保守に関連する資料等の整備・保管

a　管理責任者は、システム開発・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。

b　管理責任者は、テスト結果を一定期間保管しなければならない。

c　管理責任者は、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。

（エ）　情報システムにおける入出力データの正確性の確保

a　管理責任者は、情報システムに入力されるデータについて、必要に応じて範囲、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。

b　管理責任者は、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。

c　管理責任者は、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。

d　インターネットに公開するウェブサイトにおいては、転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じることが望ましい。

（オ）　情報システムの変更管理

管理責任者は、情報システムを変更した場合、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。

（カ）　開発・保守用のソフトウェアの更新等

管理責任者は、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、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。

（キ）　システム更新又は統合時の検証等

管理責任者は、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。

（4）　不正プログラム対策

ア　管理責任者の措置事項

（非公開）

イ　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。

（ア）　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。

（イ）　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。

（ウ）　差出人が不明又は不自然な添付ファイルを受信した場合は速やかにネットワーク管理者に報告し、その指示に従い処理しなければならない。

（エ）　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

（オ）　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 接続系に取り込む場合は無害化しなければならない。

（カ）　ネットワーク管理者が提供するウイルス情報を、常に確認しなければならない。

（キ）　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、次の対応を行ったうえ、ネットワーク管理者及び管理責任

者に報告し、その指示に従わなければならない。

a　パソコン等の端末の場合

LAN ケーブルの即時取外しを行わなければならない。

b　モバイル端末の場合

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。

ウ　専門家の支援体制

統括管理者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（5） 不正アクセス対策

ア　管理責任者の措置事項

（非公開）

イ　攻撃への対処

CISO 及び統括管理者は、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、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、総務省、都道府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。

ウ　記録の保存

CISO 及び統括管理者は、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。

エ　内部からの攻撃

管理責任者は、職員等及び委託事業者が使用しているパソコン等の端末から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。

オ　職員等による不正アクセス

システムを所管する管理責任者は、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室課等の管理責任者に通知し、適正な処置を求めるとともに、ネットワーク管理者に報告しなければならない。

カ　サービス不能攻撃

管理責任者は、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。

キ　標的型攻撃

ネットワーク管理者及び管理責任者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知し

て対処する対策（内部対策及び出口対策）を講じなければならない。

（６） セキュリティ情報の収集

ア　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

（ア）　ネットワーク管理者及び管理責任者は、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。また、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。

（イ）　ネットワーク管理者及び管理責任者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

イ　不正プログラム等のセキュリティ情報の収集・周知

ネットワーク管理者は、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。

ウ　情報セキュリティに関する情報の収集及び共有

ネットワーク管理者及び管理責任者は、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、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場合は、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。

７　運用

（１） 情報システムの監視

（非公開）

（２） 情報セキュリティポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

（ア）　管理責任者は、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 、統括管理者、情報セキュリティ責任者及びネットワーク管理者に報告しなければならない。

（イ）　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。

（ウ）　ネットワーク管理者及び管理責任者は、ネットワーク、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。

イ　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 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、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。

ウ　職員等の報告義務

（ア）　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、直ちに管理責任者に報告を行わなければならない。管理責任者は、必要に応じて統括管理者、情報セキュリティ責任者及びネットワーク管理者に報告を行わなければならない。

（イ）　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管理者が判断した場合は、適正かつ速やかに対処しなければならない。

（３）　侵害時の対応等

ア　緊急時対応計画の策定

（ア）　CISO 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。

（イ）　CISO は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した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。

イ　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。

（ア）　関係者の連絡先

（イ）　発生した事案に係る報告すべき事項

（ウ）　発生した事案への対応措置

（エ）　再発防止措置の策定

ウ　業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、CISO 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。

エ　緊急時対応計画の見直し

CISO 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。

（４） 例外措置

ア　例外措置の許可

管理責任者は、情報セキュリティポリシー及び関係規定等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する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。

イ　緊急時の例外措置

管理責任者は、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、統括管理者、情報セキュリティ責任者及びネットワーク管理者に報告しなければならない。

ウ　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。

（５） 法令遵守

ア　職員等は、職務の遂行において使用する情報資産を保護するために、次の法令等のほか関係法令等を遵守し、これに従わなければならない。

（ア）　地方公務員法（昭和 25 年法律第 261 号）

（イ）　著作権法（昭和 45 年法律第 48 号）

（ウ）　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）

（エ）　個人情報の保護に関する法律（平成 15 年法律第 57 号）

（オ）　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）

（カ）　サイバーセキュリティ基本法（平成 26 年法律第 104 号）

イ　管理責任者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

（６） 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。

ア　統括管理者が違反を確認した場合は、当該職員等が所属する室課等の管理責任者に通知し、適正な措置を求めなければならない。

イ　システムを所管する管理責任者が違反を確認した場合は、速やかに統括管理者及び当該職員等が所属する室課等の管理責任者に通知し、適正な措置を求めなければならない。

ウ　管理責任者の指導によっても改善されない場合、統括管理者は、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。統括管理者は職員等の権利を停止あるいは剥奪した旨を CISO に報告し、当該職員等が所属する室課等の管理責任者に通知しなければならない。

8　業務委託と外部サービスの利用

（1）　業務委託

ア　委託事業者の選定基準

（ア）　管理責任者は、委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（イ）　管理責任者は、必要に応じて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等を参考にして、委託事業者を選定しなければならない。

イ　契約項目

情報システムの開発、運用、保守等を業務委託する場合には、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。

（ア）　情報セキュリティポリシー及び実施手順の遵守

（イ）　外部サービスの利用に係る規定の遵守（委託事業者が外部サービスを利用する場合）

（ウ）　委託事業者の責任者、委託内容、作業者及び作業場所の特定

（エ）　提供されるサービスレベルの保証

（オ）　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

（カ）　委託事業者の従業員に対する教育の実施

（キ）　提供された情報の目的外利用及び委託事業者以外の者への提供の禁止

（ク）　業務上知り得た情報の守秘義務

（ケ）　再委託に関する制限事項の遵守

（コ）　委託業務終了時の情報資産の返還、廃棄等

（サ）　委託業務の定期報告及び緊急時報告義務

（シ）　市による監査、検査

（ス）　市による情報セキュリティインシデント発生時の公表

（セ）　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）

ウ　確認、措置等

管理責任者は、委託事業者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定期的に確認し、必要に応じ、イの契約に基づき措置しなければならない。また、その内容を重要度に応じて CISO、統括管理者、情報セキュリティ責任者及びネットワーク管理者に報告しなければならない。

（2）　外部サービスの利用（重要性区分Ⅰ又はⅡの情報を取り扱う場合）

ア　外部サービスの利用に係る規定の整備

統括管理者は、以下を含む外部サービスの利用（重要性区分Ⅰ又はⅡの情報を取り扱う場合）に関する規定を整備しなければならない。

（ア）　外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「外部サービス利用判断基準」という。）

（イ）　外部サービス提供者の選定基準

（ウ）　外部サービスの利用手続

（エ）　外部サービスの利用状況の管理

（オ）　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

イ　外部サービスの選定

（ア）　情報セキュリティ責任者は、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討しなければならない。

（イ）　情報セキュリティ責任者は、外部サービスで取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定しなければならない。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めるものとする。

（ウ）　情報セキュリティ責任者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価すること。

a　外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止

b　外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

c　外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

d　外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

e　情報セキュリティインシデントへの対処方法

f　情報セキュリティ対策その他の契約の履行状況の確認方法

g　情報セキュリティ対策の履行が不十分な場合の対処方法

（エ）　情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めなけ

ればならない。

（オ）　情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。

（カ）　情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報資産の分類等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めなければならない。（注）クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が本市によって受容可能か判断すること。

a　情報セキュリティ監査の受入れ

b　サービスレベルの保証

（キ）　情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

（ク）　情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めなければならない。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断するものとする。

（ケ）　情報セキュリティ責任者は、取り扱う情報資産の分類及び分類に応じた取扱制限に応じてセキュリティ要件を定め、外部サービスを選定しなければならない。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めるものとする。

（コ）　情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めなければならない。

（サ）　統括管理者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

ウ　外部サービスの利用に係る調達・契約

（ア）　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

（イ）　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

エ　外部サービスの利用承認

（ア）　情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行わなければならない。

（イ）　利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定しなければならない。

（ウ）　利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録しなければならない。（クラウドサービスを利用する場合も同様の措置を行う。）

オ　外部サービスを利用した情報システムの導入・構築時の対策

（ア）　統括管理者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

a　不正なアクセスを防止するためのアクセス制御

b　取り扱う情報の機密性保護のための暗号化

c　開発時におけるセキュリティ対策

d　設計・設定時の誤りの防止

e　クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

（イ）　外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

（ウ）　クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

カ　外部サービスを利用した情報システムの運用・保守時の対策

（ア）　統括管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

a　外部サービス利用方針の規定

b　外部サービス利用に必要な教育

c　取り扱う資産の管理

d　不正アクセスを防止するためのアクセス制御

e　取り扱う情報の機密性保護のための暗号化

f　外部サービス内の通信の制御

g　設計・設定時の誤りの防止

h　外部サービスを利用した情報システムの事業継続

i　設計・設定変更時の情報や変更履歴の管理

（イ）　情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

（ウ）　外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

（エ）　クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

キ　外部サービスを利用した情報システムの更改・廃棄時の対策

（ア）　統括管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定しなければならない。

a　外部サービスの利用終了時における対策

b　外部サービスで取り扱った情報の廃棄

c　外部サービスの利用のために作成したアカウントの廃棄

（イ）　外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録しなければならない。

（ウ）　クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

（３）　外部サービスの利用（重要性区分Ⅰ又はⅡの情報を取り扱わない場合）

ア　外部サービスの利用に係る規定の整備

統括管理者は、以下を含む外部サービスの利用（重要性区分Ⅰ又はⅡの情報を取り扱わない場合）に関する規定を整備しなければならない。

（ア）　外部サービスを利用可能な業務の範囲

（イ）　外部サービスの利用手続

（ウ）　外部サービスの利用状況の管理

（エ）　外部サービスの利用の運用手順

イ　外部サービスの利用における対策の実施

（ア）　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で重要性区分Ⅰ又はⅡの

情報を取り扱わない場合の外部サービスの利用を申請しなければならない。また、外部サービス管理者は、当該外部サービスの利用において適切な措置を講じなければならない。

（イ）　情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認した外部サービスを記録するものとする。

9　評価・見直し

（1）　監査

（非公開）

（2）　自己点検

ア　実施方法

（ア）　CISO はネットワーク管理者及び管理責任者に、所管するネットワーク及び情報システムについて、定期的に自己点検を実施させなければならない。

（イ）　CISO は管理責任者に、所属する職員等の情報セキュリティ対策について、定期的に自己点検を行わせなければならない。

イ　報告

ネットワーク管理者及び管理責任者は、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、CISO 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）　CISO 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定等の見直し、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。

（3）　情報セキュリティポリシー及び関係規定等の見直し

CISO は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規定等について重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

（改正履歴）

平成２９年５月１８日　制定

平成２９年８月　２日　改正

平成３１年3月２８日　改正

令和　３年6月１６日　改正（令和3年8月1日　施行）

令和　４年１０月１２日　改正

令和　５年　３月３１日　改正

令和　６年　４月1日　改正