宮崎市情報セキュリティポリシー

令和８年５月２５日改定

宮　崎　市

目次

宮崎市情報セキュリティポリシーの構成 1
第１章　情報セキュリティ基本方針 2
１．　目的 2
２．　定義 2
３．　対象とする脅威 3
４．　適用範囲 3
５．　職員等の遵守義務 3
６．　情報セキュリティ対策 3
７．　情報セキュリティ監査及び自己点検の実施 4
８．　情報セキュリティポリシーの見直し 4
９．　情報セキュリティ対策基準の策定 4
１０．　情報セキュリティ実施手順の策定 4
第２章　情報セキュリティ対策基準 5
１．　対象範囲 5
２．　組織体制 5
３．　情報資産の分類と管理方法 7
４．　情報システム全体の強靭性の向上 9
５．　物理的セキュリティ 10
５．１．　サーバ等の管理 10
５．２．　管理区域（情報システム室等）の管理 12
５．３．　通信回線及び通信回線装置の管理 12
５．４．　職員等の利用する端末や電磁的記録媒体等の管理 12
６．　人的セキュリティ 13
６．１．　職員等の遵守事項 13
６．２．　研修・訓練 14
６．３．　情報セキュリティインシデントの報告 14
６．４．　ＩＤ及びパスワード等の管理 15
７．　技術的セキュリティ 16
７．１．　コンピュータ及びネットワークの管理 16
７．２．　アクセス制御 19
７．３．　システム開発、導入、保守等 20
７．４．　不正プログラム対策 22
７．５．　不正アクセス対策 23
７．６．　セキュリティ情報の収集 24
８．　運用 25
８．１．　情報システムの監視 25
８．２．　情報セキュリティポリシーの遵守状況の確認 25
８．３．　侵害時の対応 26
８．４．　例外措置 26
８．５．　法令遵守 26
８．６．　懲戒処分等 27
９．　業務委託と外部サービスの利用 27
９．１．　業務委託 27
９．２．　外部サービスの利用（機密性２以上の情報を取り扱う場合） 28
９．３．　外部サービスの利用（機密性２以上の情報を取り扱わない場合） 30
９．４．　ソーシャルメディアサービスの利用 31
１０．　評価・見直し 31
１０．１．　監査 31
１０．２．　自己点検 32
１０．３．　情報セキュリティポリシー及び関係規定等の見直し 32

宮崎市情報セキュリティポリシーの構成

宮崎市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、宮崎市が管理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。セキュリティポリシーは、宮崎市が管理する情報資産に関する業務に携わる職員（非常勤職員・会計年度任用職員を含む。以下「職員等」という。）及び委託事業者や公の施設の指定管理者（以下「委託事業者等」という。）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。一方では、技術の進歩などに伴う情報セキュリティを取り巻く状況の急速な変化に柔軟に対応することも必要である。

このようなことから、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、セキュリティポリシーを、

情報セキュリティ基本方針
情報セキュリティ対策基準

の２階層に分け、それぞれを策定している。

また、情報セキュリティ対策基準に基づく、ネットワーク・情報システムごとの具体的な情報セキュリティ対策の実施手順を、情報セキュリティ実施手順として別途策定するとともに、Google Workspace（以下「GWS」という。）を利用するにあたり運用に伴う実施手順書を、Chromebook・Google Workspace実施手順書として別途策定することとしている（下表参照）。なお、情報セキュリティ実施手順書は、公にすることにより宮崎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。

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すべてのネットワークと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書		情報セキュリティ対策基準に基づく、ネットワーク・情報システムごとの具体的な情報セキュリティ対策の実施手順
Chromebook・ Google Workspace 実施手順書		情報セキュリティ対策基準に基づく、GWS の各アプリケーション単位の具体的な運用の実施手順

第１章　情報セキュリティ基本方針

１．　目的

情報セキュリティ基本方針（以下「本基本方針」という。）は、宮崎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、宮崎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

情報にアクセスすることを認められた者だけが、情報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（主として社会保障、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その情報システムで取り扱うデータをいう。

（9）LGWAN接続系（総合行政ネットワーク接続系）

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。

（１３）クラウドサービス

Web会議サービス、SNS、検索サービス、翻訳サービス、地図サービス、ホスティングサービスなど、庁外の通信回線やシステムを利用して委託事業者等が提供するサービスをいう。

（１４）自治体情報セキュリティクラウド

都道府県と市区町村がWebサーバー等を集約し、監視及びログ分析・解析をはじめ高度なセキュリティ対策を実施することをいう。

（１５）ゼロトラストセキュリティ

接続元のネットワークを問わず、全てのアクセスを信頼せず検証するセキュリティモデルをいう。

（１６）Google WorkSpace

Googleが提供しているクラウドツール、及びソフトウェアであり、宮崎市として利用しているグループウェアをいう。

３． 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、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、市長部局、行政委員会、議会事務局、消防局、上下水道局、教育機関（事務室のみ）とする（以下「部局等」という。）。

（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、情報システム及びこれらに関する設備、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、ネットワーク図等のシステム関連文書

エ．職員がGWSを利用するために使用する全ての情報端末

５． 職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって情報セキュリティポリシー、情報セキュリティ実施手順書及びChromebook・Google Workspace実施手順書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、次の情報セキュリティ対策を講じる。

（1）組織体制

宮崎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

宮崎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行う。

（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。

①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。

②LGWAN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、インターネット接続系からLGWAN接続系へ通信する場合には、無害化通信を実施する。

③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、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

サーバ等、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。）等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

（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、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。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(8)業務委託とクラウドサービスの利用

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。クラウドサービスを利用する場合には、利用に関す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る。

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、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宮崎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。

１１． Chromebook・Google Workspace 実施手順書の策定

情報セキュリティ対策基準に基づく、GWS の各アプリケーション単位の具体的な運用の実施手順を定めた Chromebook・Google Workspace 実施手順書を策定するものとする。

なお、Chromebook・Google Workspace 実施手順書は、公にすることにより宮崎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。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準（以下「本対策基準」という。）とは、宮崎市の全ての情報資産に関して情報セキュリティ基本方針を実行に移すための基準である。

１．対象範囲

（１）行政機関の範囲

本対策基準が対象とする行政機関は、基本方針に規定するものと同様とする。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、基本方針に規定するものと同様とする。

２．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。）

宮崎市の情報政策を担当する副市長を、ＣＩＳＯとする。ＣＩＳＯは、宮崎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。

（２）統括情報セキュリティ責任者

①情報政策担当部長を、ＣＩＳＯ直属の統括情報セキュリティ責任者とする。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。

②統括情報セキュリティ責任者は、宮崎市の全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。

③統括情報セキュリティ責任者は、宮崎市の全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。

④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。

⑤統括情報セキュリティ責任者は、宮崎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行う権限及び責任を有する。

⑥統括情報セキュリティ責任者は、宮崎市の共通的なネットワーク、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・管理を行う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、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、情報システム担当者を網羅する連絡体制を整備しなければならない。

⑧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。

⑨統括情報セキュリティ責任者は、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。

（３）情報セキュリティ責任者

①市長部局の部局長、行政委員会の長、議会事務局長、消防局長、上下水道局長を情報セキュリティ責任者とする。

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及び職員等に対する教育、訓練、助言及び指示を行う。

（４）情報セキュリティ管理者

①課・室の長、地域センター長、行政委員会の次長、議会事務局の次長、消防局の課長、上下水道局の課長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する課室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、その所掌する課室等において、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。

（５）情報システム管理者

①各情報システムの担当課・室の長を、当該情報システムに関する情報システム管理者とする。

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。

（６）情報システム担当者

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、情報システム担当者とする。

（７）宮崎市情報セキュリティ委員会

宮崎市の情報セキュリティ対策を統一的に行うため、宮崎市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等、情報セキュリティに関する重要な事項を決定する。

（８）兼務の禁止

①情報セキュリティ対策の実施において、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。

②監査を受ける者と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。

（９）情報セキュリティに関する統一的な窓口（ＣＳＩＲＴ：Computer Security Incident Response Team以下「ＣＳＩＲＴ」という。）の設置

①ＣＩＳＯは、情報セキュリティインシデントの統一的な窓口の機能を有するＣＳＩＲＴ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。

②ＣＩＳＯ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。

③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。また、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。

④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ＣＳＩＲＴ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。

（１０）クラウドサービス利用における組織体制

①統括情報セキュリティ責任者は、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。

【管理体制図】

最高情報セキュリティ責任者（ＣＩＳ	情報政策を担当する副市長

O）	
統括情報セキュリティ責任者	情報政策担当部長
情報セキュリティ責任者	市長部局の部局長、行政委員会の長、議会事務局長、消防局長、上下水道局長
情報セキュリティ管理者	市長部局の課・室の長、地域センター長、行政委員会の次長、議会事務局の次長、消防局の課長、上下水道局の課長
情報システム管理者	各情報システムの担当課・室の長
情報システム担当者	各情報システムの運用等を担当する職員
宮崎市情報セキュリティ委員会	委員長　情報政策担当部長 副委員長　情報政策課長、デジタル・行革推進課長 デジタル対策監 委員　情報政策課長補佐、情報政策課係長 デジタル・行革推進課係長、総務法制課係長 人材マネジメント課係長
情報セキュリティに関する統一的な窓口（ＣＳＩＲＴ）	統括情報セキュリティ責任者（情報政策担当部長）

３．　情報資産の分類と管理方法

（１）情報資産の分類

宮崎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。

機密性による情報資産の分類

分類	分類基準	取扱制限
自治体機密性３A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」(平成 23 年４月１日内閣総理大臣決定令和７年２月 14 日一部改正）に定める秘密文書に相当する文書又は個人番号利用事務系で取扱う情報資産	・支給、承認された端末以外及び信頼できるクラウドサービス以外での作業の原則禁止並びに・GWSへのアップロードの原則禁止（自治体機密性３A以上の情報資産に対して） ・庁外ネットワークでの作業の原則禁止（自治体機密性２以上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程 ・電磁的記録媒体の施錠可能な場所への保管
自治体機密性３B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性３C	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体機密性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	
自治体機密性１	機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
自治体 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	・許可された者以外による編集の制限 ・バックアップ、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程 ・電磁的記録媒体の施錠可能な場所への保管
自治体 完全性１	自治体完全性２の情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
自治体 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	・サーバやネットワーク等の冗長化 ・バックアップ、指定する時間以内での復旧 ・電磁的記録媒体の施錠可能な場所への保管
自治体 可用性１	自治体可用性２の情報資産以外の情報資産	

（２）情報資産の管理

①管理責任

（ア）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。

（イ）情報セキュリティ管理者は、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も（１）の分類に基づき管理しなければならない。

（ウ）情報セキュリティ管理者は、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）の取扱いを定めなければならない。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。

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切な管理を行わなければならない。

③情報の作成及び消去

（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、当該情報の分類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）情報が不要になった場合は、当該情報を速やかに消去しなければならない。

④情報資産の入手

（ア）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。

（イ）庁外の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、当該情報の分類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分類が不明な場合、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

（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、情報資産の分類に応じ、適切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分類が異なる情報が複数記録されている場合、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

（ア）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、情報資産を適切に保管しなければならない。
（イ）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。
（ウ）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や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。
（エ）情報セキュリティ管理者又は情報システム管理者は、自治体機密性２以上、自治体完全性２又は自治体可用性２の情報を記録した電磁的記録媒体を保管する場合、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。

⑦情報の送信

電子メールやクラウドサービスを利用して自治体機密性２以上の情報を送信する者は、情報セキュリティ管理者の許可を得た上で、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。

⑧情報資産の運搬

（ア）車両等により自治体機密性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。
（イ）自治体機密性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

（ア）自治体機密性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。
（イ）自治体機密性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。
（ウ）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

（ア）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、電磁的記録媒体の初期化等、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。
（イ）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とともに、処理委託業者へ産業廃棄物管理表（マニフェスト）の提出を求めなければならない。
（ウ）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。
（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取り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。

４． 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

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。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。

②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。

（イ）情報の持ち出し

業務遂行のために必要と認められる場合は、暗号化等の対策を行い、接続を許可されたUSBメモリ等の電磁的記録媒体を用いることができる。

③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取扱い

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取り扱い、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。

④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、その情報資産の自治体機密性を考慮し、暗号による対策を実施しなければならない。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

①LGWAN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を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

②LGWAN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取扱い

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接続系として取り扱い、マイナンバー利用事務系とネットワークを分離し、専用回線等のセキュリティが確保された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

①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に参加するとともに、関係省庁や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。

③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と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。

５． 物理的セキュリティ

５．１． 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、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切に固定する等、必要な措置を講じなければならない。

（２）サーバの冗長化

①情報システム管理者は、重要情報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及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。

②情報システム管理者は、基幹サーバに障害が発生した場合に、速やかに切り替えを行い、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。

（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、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。

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、可能な限り必要な措置を施さなければならない。

（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。

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切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。

（５）機器の定期保守及び修理

①情報システム管理者は、自治体可用性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、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、内容を消去した状態で行わせなければならない。内容を消去できない場合、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他、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、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。

（７）機器の廃棄等

①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、機器内部の記録装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

②機器の廃棄を行う者は、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とともに、処理委託業者から産業廃棄物管理表（マニフェスト）の提出を求めなければならない。

③職員等は、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）をする者が、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。

５．２．　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、情報システム室や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、管理区域を地階又は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。

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、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、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。

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、自治体機密性２以上の情報資産を取り扱うシステムを設置している管理区域について、原則として、当該情報システムに関連しない若しく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。

５．３．　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、適切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切に保管しなければならない。

②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。

③統括情報セキュリティ責任者は、自治体機密性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、適切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。

④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。

⑤統括情報セキュリティ責任者は、自治体可用性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。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。

５．４．　職員等の利用する端末や電磁的記録媒体等の管理

①情報システム管理者は、マイナンバー利用事務系について、執務時間外においては、執務室等の施錠管理やワイヤーによる固定等、端末や電磁的記録媒体等の盗難防止措置を講じなければならない。LGWAN接続系及びインターネット接続系については、各執務室の状況や職員配置状況を勘案し、必要に応じて盗難防止対策を講じなければならない。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、情報システムへのログインパスワード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、ゼロトラストセキュリティ対策を取っている場合を除き、端末の電源起動時のパスワード（ＢＩＯＳパスワード、ハードディスクパスワード等）を併用しなければならない。
④情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用しなければならない。
⑤情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、ＭＤＭ（ＭＤＭ：Mobile Device Management）等の遠隔消去機能を利用する等の措置を講じなければならない。

６． 人的セキュリティ

６．１． 職員等の遵守事項

（１）職員等の遵守事項

①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、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

②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。

③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

（ア）ＣＩＳＯは、自治体機密性２以上、自治体可用性２、自治体完全性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。

（イ）職員等は、宮崎市のモバイル端末、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。

（ウ）職員等は、外部で情報処理作業を行う場合には、情報セキュリティ管理者の許可を得なければならない。

（エ）職員等は、外部で情報処理作業を行う際は、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。

④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

（ア）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。

（イ）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、情報セキュリティ管理者の許可を得るものとし、外部で情報処理作業を行う際には安全管理措置を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、ＭＤＭ等の対策が取られていない端末等の外部への持ち出し及び外部から持ち込まれた端末等を市のネットワークに接続する場合、記録を作成し、保管しなければならない。

⑥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。

⑦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、適切な措置を講じなければならない。

⑧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。

⑨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、情報セキュリティポリシー及び本市が定めたクラウドサービスの利用に係る基本方針を遵守しなければならない。

（2）非常勤及び会計年度任用職員への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び会計年度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。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び会計年度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。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び会計年度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。

（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）委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、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。

6．2．　研修・訓練

（1）情報セキュリティに関する研修・訓練

①ＣＩＳＯは、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

②ＣＩＳＯ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、研修又は訓練を実施するとともに、委託先を含む関係者についても委託先等で研修、訓練が行われていることを確認しなければならない。

（2）研修計画の立案及び実施

①ＣＩＳＯは、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定期的に立案しなければならない。

②研修計画において、職員等が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。

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。

（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。

（4）研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加しなければならない。

6．3．　情報セキュリティインシデントの報告

（1）庁内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、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に報告しなければならない。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場合

も同様とする。
②報告を受けた情報セキュリティ管理者は、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ＣＳＩＲＴに報告しなければならない。
③情報セキュリティ管理者は、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に報告しなければならない。
④情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ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、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、情報セキュリティ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に報告しなければならない。
④統括情報セキュリティ責任者は、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。

（3）情報セキュリティインシデントの原因の究明・記録、再発防止等
①統括情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者、情報システム管理者及びＣＳＩＲＴと連携し、これらの情報セキュリティインシデントの原因を究明し、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結果から、再発防止策を検討し、必要に応じてＣＩＳＯに報告しなければならない。
②ＣＩＳＯは、統括情報セキュリティ責任者から、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。

６．４．　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若しく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。
（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。
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、切替え前のカードを回収し、破砕する等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（アルファベットの大文字及び小文字の両方を用い、数字や番号を織り交ぜる等）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取り扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑥パソコン等の端末にパスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。
⑦共用ＩＤのパスワードを除いて、職員等間でパスワードを共有してはならない。

7． 技術的セキュリティ

7．1． コンピュータ及びネットワークの管理

（1）ファイルサーバ等の設定等
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等の容量を設定し、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、ファイルサーバ等を課室等の単位で構成し、職員等が他課室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、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、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
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、業務システムのデータベースや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。
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、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。なお、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。

（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、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切に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。
③統括情報セキュリティ責任者、情報システム管理者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 名以上で作業し、互いにその作業を確認しなければならない。

（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について、記録媒体に関わらず、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、適切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、ログ等が窃取、改ざん、誤消去等されないように必要な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、所管する情報システムから自動出力したログ等について、必要に応じ、外部記録媒体にバックアップ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、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、保存するログ等に関する改ざんの防止等について、ログ管理等に関する対策や機能に関する情報を確認し、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。
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、監査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ない場合は、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。

（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、適切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、ネットワークに適切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物理的に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。
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、破壊若しくは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。
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、次のセキュリティ対策を実施しなければならない。
（ア）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。
（イ）脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。
（ウ）ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。
（エ）情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならない。
（オ）インターネットを介して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なければならない。【推奨事項】
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物理的に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、複合機を調達する場合、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、適切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切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、複合機の持つ電磁的記録媒体の全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（IoT機器を含む）のセキュリティ管理

統括情報セキュリティ責任者は、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実施しなければならない。

（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、解読が困難な暗号化及び認証技術等の十分なセキュリティ対策の実施を義務づ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、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。

②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。

③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。

④統括情報セキュリティ責任者は、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、委託先との間で利用方法を取り決めなければならない。

（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、外部へ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、ＢＣＣの設定を行うなど、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職員等が、インターネットで利用できるフリーメールを使用する場合は、利用申請の許可権限者へ申請しなければならない。

（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の方法を使用して、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。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。

③ＣＩＳＯ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。

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。

（１８）機器構成の変更の制限
①職員等は、パソコンやモバイル端末に対し無断で機器の改造及び増設・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及び増設・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）業務外ネットワークへの接続の禁止
①職員等は、有線・無線を問わず、その端末を接続して利用するよう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。
②情報セキュリティ管理者は、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することが望ましい。

（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切な措置を求めなければならない。

（２１）Web 会議サービスの利用時の対策
①職員等は、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すること。
②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ずること。

７．２．　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必要最小限の範囲で適切に設定する等、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、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。
（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、職員等から対象に対する不要なアクセス権限が付与されていないか定期的に確認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、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は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び内部からの不正操作や誤操作を防止するための措置を講じなければならない。
（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の特権を代行する者は、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。
（エ）ＣＩＳＯは、代行者を認めた場合、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。
（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

ードの変更について、委託事業者に行わせてはならない。
（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、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、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、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、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パソコン等の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、ＯＳ等のセキュリティ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に接続することを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、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）自動識別の設定
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、ネットワークで使用される機器について、必要に応じ、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（4）ログイン時の表示等
情報システム管理者は、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、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システムを設定しなければならない。

（5）認証情報の管理
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。また、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場合は、これを有効に活用しなければならない。

（6）特権による接続時間の制限
情報システム管理者は、管理者権限等の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。

7．3．　システム開発、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。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載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、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。

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、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。

（イ）情報システム管理者は、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、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、それ以外のものを利用させてはならない。

（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、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。

④アプリケーション・コンテンツの開発時の対策

情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

（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移行手順の明確化

（ア）情報システム管理者は、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。

（イ）情報システム管理者は、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。

（ウ）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。

（エ）情報システム管理者は、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、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、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生データ（未加工のデータ）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、開発したシステムについて受け入れテストを行う場合、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。

（オ）情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

③機器等の納入時又は情報システムの受入れ時

（ア）情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

（イ）情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（４）システム開発・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、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切に整備・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切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、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

ウェブアプリケーションやウェブコンテンツにおいて、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、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、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。

7.4. 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統括情報セキュリティ責任者が認めた場合（ゼロトラストセキュリティ対策を取っている場合等）を除き、所掌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。

⑥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。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

⑧仮想マシンを設定する際には、不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。なお、SaaS 型のサービスを利用する場合は、これらのセキュリティ対策が、クラウドサービス事業者側でなされているのか、サービスを利用する前に確認し、サービス利用開始後にあっては、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報

告を求めなければならない。

（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、ゼロトラストセキュリティ対策を取っている場合を除き、その所掌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システムに常駐させなければならない。

②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。

③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。

④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、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。また、不正プログラムの感染、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。

⑤不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

（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ゼロトラストセキュリティ対策を取っている場合を除き、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。

⑤ゼロトラストセキュリティ対策を取っている場合を除き、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。

⑥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。

⑦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、次の対応を行わなければならない。

（ア）パソコン等の端末の場合

有線接続の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。無線接続の場合は、無線から切断しなければならない。

（イ）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。

（4）専門家の支援体制

統括情報セキュリティ責任者は、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。

7．5．　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、次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に、データの書換えを検出し、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、設定しなければならない。

④重要なシステムの設定を行った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

査しなければならない。
⑤ＣＳＩＲＴと連携し、監視、通知、外部連絡窓口及び適切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。
⑥本市が定めたクラウドサービスの利用に係る基本方針におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。
⑦クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合は、多要素認証を用いて認証させなければならない。
⑧パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本市が定めたクラウドサービスの利用に係る基本方針を満たすことを確認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、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等の情報セキュリティ管理者に通知し、適切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。

7．6．　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
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、サーバ装置、端末及び通信回線装置等における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。
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、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を行った上で、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。

（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、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、セキュリティ侵害等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。

8． 運用

8．1． 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。また、利用するクラウドサービスで使用する時刻の同期についても、適切になされているのか確認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、外部と常時接続するシステムを常時監視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、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに、監視により業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

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、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

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、クラウドサービス利用における重大なインシデントに繋がるおそれのある以次の重要な操作に関して、手順化し、確認しなければならない。

（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）クラウドサービス利用を終了する際の手順

（ウ）バックアップ及び復旧

8．2． 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情報セキュリティ管理者は、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。

②ＣＩＳＯは、発生した問題について、適切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切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。

②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は、緊急時対応計画に従って適切に対処しなければならない。

8．3． 侵害時の対応

（1）緊急時対応計画の策定

①ＣＩＳＯ又は宮崎市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切に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って適切に対処しなければならない。

②ＣＩＳＯ又は宮崎市情報セキュリティ委員会は、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。

（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、次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

宮崎市情報セキュリティ委員会は、自然災害、大規模・広範囲にわたる疾病等に備えて策定した業務継続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又は宮崎市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。

8．4． 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、例外措置を取ることができる。

（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切に保管しなければならない。

8．5． 法令遵守

（1）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地方自治法（昭和 22 年法律第 67 号）
②地方公務員法(昭和 25 年法律第 261 号)
③著作権法（昭和 45 年法律第 48 号）
④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）
⑤個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑥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）
⑦サイバーセキュリティ基本法（平成 26 年法律第 104 号）
⑧ 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和 7 年法律第 42 号）
⑨宮崎市個人情報の保護に関する法律施行条例（令和 4 年 12 月 19 日条例第 28 号）

（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、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場合（IaaS 等でアプリケーションを構築する場合）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。

8．6． 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は、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等の情報セキュリティ管理者に通知し、適切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は、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等の情報セキュリティ管理者に通知し、適切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若しく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若しくは剥奪した旨をＣＩＳＯ及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

9． 業務委託とクラウドサービスの利用

9．1． 業務委託

（1）委託事業者の選定基準

①情報セキュリティ管理者は、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、委託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。

（2）契約項目

情報システムの運用、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等に係る要件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
・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
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフ

サイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・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
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市によるセキュリティインシデント発生時の公表
・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)
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め

（3）確認・措置等

情報セキュリティ管理者は、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、（2）の契約項目に基づき措置しなければならない。また、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。

9.2. クラウドサービスの利用（自治体機密性２以上の情報を取り扱う場合）

（1）クラウドサービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下の内容を含むクラウドサービス（機密性２以上の情報を取り扱う場合に限る。）の利用に関する規定を整備しなくてはならない。

①クラウド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（以下この節において「クラウドサービス利用判断基準」という。）
②クラウドサービス提供者の選定基準
③クラウドサービスの利用申請の許可権限者と利用手続
④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
⑤クラウドサービスを利用する場合は、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

（2）クラウドサービスの選定

①情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従ってクラウドサービスの利用を検討しなければならない。
②情報セキュリティ管理者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また、必要に応じて以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。
③情報セキュリティ管理者は、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係る基本方針を満たしているか否かを評価すること。

（ア）クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止
（イ）クラウド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
（ウ）クラウドサービスの提供にあたり、クラウド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
（エ）クラウドサービス提供者の資本関係・役員等の情報、クラウド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
（オ）情報セキュリティインシデントへの対処方法
（カ）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

（キ）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

④情報セキュリティ管理者は、クラウド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、必要に応じてクラウドサービス提供者の選定条件に含めなければならない。

⑤情報セキュリティ管理者は、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しなければならない。

⑥情報セキュリティ管理者は、クラウドサービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めること。なお、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、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に鑑み、その規約内容が本市において受容可能か判断しなければならない。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑦情報セキュリティ管理者は、クラウド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による規制が適用されるリスクを評価してクラウド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。

⑧情報セキュリティ管理者は、クラウド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、クラウドサービス提供者の選定条件で求める内容をクラウド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、クラウドサービス提供者の選定条件に含めること。また、クラウドサービス利用判断基準及びクラウド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しなければならない。

⑨情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、クラウドサービスを選定しなくてはならない。また、クラウド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なければならない。【推奨事項】

⑩情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウド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。

⑪統括情報セキュリティ責任者は、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、クラウド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。

（3）クラウドサービスの利用に係る調達・契約

①情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウド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。

②情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウド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。

（4）クラウドサービスの利用承認

①情報セキュリティ管理者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

②利用申請の許可権限者は、職員等によるクラウド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。

③利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。

（5）クラウドサービスを利用した情報システムの導入・構築時の対策

①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、

以下の内容を含むクラウド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。
（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（ウ）開発時におけるセキュリティ対策
（エ）設計・設定時の誤りの防止
（オ）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
②クラウドサービス管理者は、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しなければならない。
③クラウドサービス管理者は、前２項において定める規定に対し、情報セキュリティに配慮した構築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、実施状況を確認及び記録しなければならない。

（6）クラウドサービスを利用した情報システムの運用・保守時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下の内容を含むクラウド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。
（ア）クラウドサービス利用方針の規定
（イ）クラウドサービス利用に必要な教育
（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）クラウドサービス内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）クラウドサービスを利用した情報システムの事業継続
（ケ）設計・設定変更時の情報や変更履歴の管理
②総括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、クラウド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。
③クラウドサービス管理者は、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しなければならない。
④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・保守の手順及びその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しなければならない。

（7）クラウドサービスを利用した情報システムの更改・廃棄時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下の内容を含むクラウド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。
（ア）クラウドサービスの利用終了時における対策
（イ）クラウドサービスで取り扱った情報の廃棄
（ウ）クラウドサービスの利用のために作成したアカウントの廃棄
②クラウドサービス管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認しなければならない。
③クラウドサービス管理者は、クラウドサービス上で住民情報その他機密性の高い情報を保存する場合は、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。

９．３．　クラウドサービスの利用（自治体機密性２以上の情報を取り扱わない場合）

（1）クラウドサービスの利用に係る規定の整備
①統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱わない場合、以下の内容を含むクラウドサービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性２以上の情報が取り扱われないように規定しなければならない。

（ア）クラウドサービスを利用可能な業務の範囲
（イ）クラウドサービスの利用申請の許可権限者と利用手続
（ウ）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
（エ）クラウドサービスの利用の運用手順

（2）クラウドサービスの利用における対策の実施
①職員等は、利用するサービスの約款、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自治体機密性２以上の情報を取り扱わない場合のクラウドサービスの利用を申請し、適切な措置を講じた上で利用しなければならない。
②情報セキュリティ責任者は、職員等によるクラウド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、承認したクラウドサービスを記録しなければならない。

９．４．　ソーシャルメディアサービスの利用
ソーシャルメディアサービスを利用する場合、宮崎市ソーシャルメディアの利用に関するガイドラインを遵守すること。

１０．評価・見直し

１０．１．　監査

（1）実施方法
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状況について、必要に応じて監査を行わせなければならない。

（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）監査実施計画の立案及び実施への協力
①情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実施計画を立案し、宮崎市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）委託事業者に対する監査
①委託事業者に委託している場合、情報セキュリティ監査統括責任者は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、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。
②クラウドサービスを利用している場合、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、監査を必要に応じて行わなければならない。なお、クラウドサービス事業者に監査実施の証拠の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

（5）報告
情報セキュリティ監査統括責任者は、監査結果を取りまとめ、宮崎市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
情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、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。

（7）監査結果への対応

①ＣＩＳＯは、監査結果を踏まえ、監査の指摘事項を、所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。
②ＣＩＳＯは、指摘事項を所管していない情報セキュリティ管理者に対しても、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
宮崎市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。

１０．２．　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、定期的に、又は必要に応じ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は、情報セキュリティ管理者と連携して、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状況について、毎年度又は必要に応じ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及び情報セキュリティ責任者は、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、宮崎市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宮崎市情報セキュリティ委員会は、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。

１０．３．　情報セキュリティポリシー及び関係規定等の見直し

宮崎市情報セキュリティ委員会は、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踏まえ、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（リスク評価を含む）を行い、必要があると認めた場合、改善を行うものとする。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてＣＩＳＯ に報告しなければならない。