石垣市情報セキュリティ対策基準

第2版

令和7年12月

石　垣　市

〈 改 版 履 歴 〉

版　数	作成年月日	作成改訂理由
第1版	令和4年4月1日	新規制定
第2版	令和7年12月10日	全部改正

目次

第1章　総則

（趣旨）

第1条　この基準は、石垣市情報セキュリティ基本方針（令和4年4月1日市長決裁）第10条の規定に基づき、情報セキュリティ基本方針を実行に移すための、本市における情報資産に関する情報セキュリティ対策の基準について定めるものとする。

（定義）

第2条　この基準において使用する用語は、石垣市情報セキュリティ基本方針において使用する用語の例による。

第2章　組織体制

（最高情報セキュリティ責任者）

第3条　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責任者として、最高情報セキュリティ責任者(以下「CISO」という。)を設置し、副市長をもって充てる。

2　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する者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。

3　CISOは、情報セキュリティ上の脅威となる事象となる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、役割を明確化するものとする。

4　CISOは、本基準に定められた自らの職務を、本基準に定める各責任者に担わせることができる。

（統括情報セキュリティ責任者）

第4条　CISOを補佐する者として統括情報セキュリティ責任者を置き、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、次に掲げる事項に係る権限及び責任を有する。

(1)　本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行うこと。

(2)　本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こと。

(3)　第5条の情報セキュリティ責任者、第6条の情報セキュリティ管理者、第7条の情報システム責任者、第8条の情報システム管理者及び第9条の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こと。

(4)　本市の情報セキュリティの侵害が発生した場合又は侵害のおそれがある場合において、CISOの指示に従い、及びCISOが不在の場合にあっては自らの判断に基づき、必要かつ十分な措置を実施すること。

(5)　本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決定、維持及び管理を行うこと。

3　統括情報セキュリティ責任者は、情報セキュリティに係る緊急時、その他必要な場合における円滑な情報共有を図るため、CISO、副CISO、自己及び情報セキュリティ責任者らへの連絡体制を含む緊急連絡網を整備しなければならない。

4　統括情報セキュリティ責任者は、緊急時においては直ちにCISO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。

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係する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。

（情報セキュリティ責任者）

第5条　各部等における情報セキュリティを統括する責任者として情報セキュリティ責任者を置き、当該部等を所管する部長又は部長相当職の職にある者をもって充てる。

2　情報セキュリティ責任者は、次に掲げる事項に係る権限及び責任を有する。

(1)　所管する部等の統括的な情報セキュリティ対策に関すること。

(2)　所管する部等において所有する情報システムにおける開発、設定の変更、運用、見直し等を行うこと。

3　情報セキュリティ責任者は、その所管する部等において所有す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に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者）

第6条　情報システムを利用する課等における情報セキュリティを管理する責任者として情報セキュリティ管理者を置き、当該課を所管する課長又は課長相当職の職にある者をもって充てる。

2　情報セキュリティ管理者は、その所管する課等の情報セキュリティ対策に関する権限及び責任並びに情報資産の管理に関する責任を有する。

3　情報セキュリティ管理者は、その所掌する課等において、情報セキュリティの侵害が発生した場合又はそのおそれがある場合には、直ちに情報セキュリティ責任者へ報告を行い、指示を受けなければならない。

（情報システム責任者）

第7条　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開発、設定の変更、運用、見直し等及び情報セキュリティ対策に関する全庁的な調整を行う責任者として情報システム責任者を置き、DX課長をもって充てる。

（情報システム管理者）

第8条　各課等における情報システムの管理運用及び情報システムに係る情報セキュリティ対策の責任者として情報システム管理者を置き、当該課等を所管する課長又は課長相当職の職にある者をもって充てる。

2　情報システム管理者は、次に掲げる事項に係る権限及び責任を有する。

(1)　所管する情報システムにおける開発、設定の変更、運用、見直し等を行うこと。

(2)　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こと。

3　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及び管理を行う。

（情報システム担当者）

第9条　情報システム管理者の指示等に従い、各課等において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職員を情報システム担当者とする。

（石垣市情報セキュリティ委員会）

第10条　本市における情報セキュリティ対策を統一的に実施するため、別表第1に定める石垣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その他情報セキュリティに関する重要

な事項を決定する。

(兼務の禁止)

第11条　情報セキュリティ対策の実施においては、やむを得ない場合を除き、承認又は許可の申請と当該承認又は当該許可は、同じ者が行ってはならない。

(CSIRTの設置及び役割)

第12条　CSIRTに責任者を置き、総務部長をもって充てる。

2　CSIRTに管理者を置き、総務課長をもって充てる。

3　CSIRTに情報セキュリティの統一的な窓口(以下「PoC」という。)を置き、総務部総務課に設置する。

4　CSIRTは、CISOによる情報セキュリティに関する方針の決定が行われた場合は、その内容を関係部局等に提供しなければならない。

5　CSIRTは、情報セキュリティインシデントを認知した場合は、CISO、総務省、沖縄県その他関係機関へ報告しなければならない。

6　CSIRTは、前項に規定する場合において、その重要度や影響範囲等を勘案し、必要に応じ報道機関への通知その他公表に係る対応を行わなければならない。

7　CSIRTは、情報セキュリティに関して、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その他関係機関、外部の事業者等との情報共有に努めなければならない。

第3章　情報資産の分類と管理

(情報資産の分類)

第13条　本市の情報資産は、機密性、完全性及び可用性により別表第2から別表第4までに定めるとおり分類し、及び取扱いの制限を行うものとする。複製され、又は伝送された情報資産についても、同様とする。

(行政文書の分類及び管理)

第14条　職員は、本市の情報資産のうち行政文書については、石垣市文書取扱規程(昭和61年訓令第9号)及び石垣市文書編集保存規程(昭和61年11月21日訓令第10号)に規定するファイル基準に従って分類し、適正な管理を行わなければならない。

(情報の作成)

第15条　職員は、業務上必要のない情報を作成してはならない。

2　情報を作成する職員は、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ず、また、作成途上で当該情報が不要になった場合は、速やかに当該情報を消去しなければならない。

(情報資産の入手)

第16条　職員は、他の職員が作成した情報資産を入手した場合は、作成元の第13条の規定による情報資産の分類に基づく取扱いをしなければならない。

2　職員は、前項に規定する場合において、入手した情報資産の分類が不明であるときは、当該情報資産の分類について情報セキュリティ管理者の判断を受けなければならない。

(情報資産の利用)

第17条　情報資産を利用する職員は、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職員は、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　情報資産のうち電磁的記録媒体を利用する職員は、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、これらのうち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。

（情報資産の保管）

第18条　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及び情報システム管理者は、情報資産である電磁的記録媒体を長期にわたって保管する場合は、当該電磁的記録媒体への書き込みを禁止する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及び情報システム管理者は、別表第2に規定する機密性2若しくは機密性3、別表第3に規定する完全性2(以下「完全性2」という。)又は別表第4に規定する可用性2(以下「可用性2」という。)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。

（情報の送信）

第19条　電子メール等により機密性2以上の情報を送信しようとする職員は、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。

（情報資産の運搬）

第20条　車両等により機密性2以上の情報資産を運搬しようとする職員は、当該運搬について情報セキュリティ管理者の許可を受けなければならず、かつ、必要に応じ鍵付きのケース等に格納し、又は暗号化若しく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。

（情報資産の提供又は公開）

第21条　機密性2以上の情報資産を外部に提供しようとする職員は、当該提供について情報セキュリティ管理者の許可を受けなければならず、かつ、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　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。

（情報資産の廃棄）

第22条　情報資産の廃棄をしようとする職員は、当該廃棄について情報セキュリティ管理者の許可を受けなければならず、かつ、当該情報資産が電磁的記録媒体である場合は、記録されている情報の機密性に応じ当該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った職員は、当該廃棄の日時、担当者及び処理内容を記録しなければならない。

第4章　情報システム全体の強靭性の向上

（マイナンバー利用事務系と他の領域との分離）

第23条　マイナンバー利用事務系は、他の領域と通信できない領域に置かなければならない。

2　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、MACアドレス又はIPアドレスによる通信経路の限定及びポート番号の指定によるアプリケーションプロトコルのレベルでの限定

を行わなければならず、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、インターネット等からLGWAN-ASPを利用してマイナンバー利用事務系にデータの取り込みができるものとする。

（情報へのアクセス及び情報の持ち出しに係る対策）

第24条　情報システムが正規の利用者かどうかを判断する認証については、知識に係る情報、所持に係る情報及び生体に係る情報を利用する認証手段のうち二つ以上を併用する認証手段を利用しなければならない。

2　職員は、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の持ち出しを行ってはならず、端末についても当該手段による情報の持ち出しができないように設定しなければならない。

（LGWAN接続系とインターネット接続系の分割）

第25条　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、必要な通信のみを許可できるようにしなければならない。

（インターネット接続系）

第26条　インターネット接続系においては、沖縄県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、沖縄県等と連携しながら、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　マイナンバー利用事務系及びLGWANから完全に分離したインターネット接続系においては、通信パケットの監視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及びその対処等の情報セキュリティ対策を講じなければならない。

第5章　物理的セキュリティ

（機器の取付け）

第27条　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、湿度等の影響をできる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の必要な措置を講じなければならない。

（サーバの冗長化等）

第28条　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その他の基幹サーバを冗長化し、同一データを保持するよう努めなければならない。

2　情報システム管理者は、通常業務で稼働しているサーバ等に障害が発生した場合は、速やかに複製サーバを起動し、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。

（機器の電源）

第29条　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。

（通信ケーブル等の配線）

第30条　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、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、施設管理部門と連携し配線収納管を使用する等の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、施設管理部門から主要な箇所の通信ケーブル及び電源ケーブルの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、ハブのポート等のネットワーク接続口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及び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し、追加し、又は撤去することができないように必要な措置を講じなければならない。

（機器の定期保守及び修理）

第31条　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の修理を外部の事業者に行わせる場合は、あらかじめ記録した情報を消去した状態で引き渡さなければならない。

3　情報システム管理者は、前項に規定する場合において、当該情報を消去できないときは、当該事業者との間で当該修理に係る守秘義務契約を締結し、及び当該事業者の秘密保持に係る体制の確認等を行わなければならない。

（庁外における機器の設置）

第32条　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、庁外にサーバ又はネットワーク機器を設置する場合は、CISOの承認を得なければならない。

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、前項に規定する場合において、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。

（機器の廃棄等）

第33条　情報システム管理者は、機器の廃棄、リース返却等をする場合は、機器内部の記憶装置から全ての情報を消去し、及び復元不可能な状態にする措置を講じなければならない。

（管理区域の構造等）

第34条　統括情報セキュリティ責任者及び情報システム責任者は、管理区域（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区域）を2階以上に設置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責任者は、施設管理部門と連携し、管理区域から外部に通ずるドアは必要最小限の数とし、鍵、監視機能、警報装置等により入退室を許可された者以外の者の立入りを防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責任者は、情報システム室内の機器等に転倒及び落下の防止等の耐震対策、防火措置、防水措置等を講じなければならない。

4　統括情報セキュリティ責任者及び情報システム責任者は、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に影響を与えないようにしなければならない。

（管理区域の入退室管理等）
第35条　情報システム責任者は、管理区域への入退室を許可された者のみに制限し、ICカード又は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、身分証明書を携帯し、及び情報システム責任者の求めにより提示しなければならない。
3　情報システム責任者は、外部の者が管理区域に入室する場合は、必要に応じて立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を付き添わせ、及び当該外部の者と職員を区別できる外見上の措置を講じなければならない。
4　情報システム責任者は、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入室する者について、当該情報システムに関連しない機器等を持ち込ませないようにしなければならない。
（機器等の搬入出）
第36条　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外部委託事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、管理区域の機器等の搬入出が行われるときは、職員を立ち会わせなければならない。
（通信回線及び通信回線装置の管理）
第37条　統括情報セキュリティ責任者は、施設管理部門と連携して庁内の通信回線及び通信回線装置を適正に管理し、並びに当該通信回線及び通信回線装置に関する文書を適正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、行政系のネットワークをLGWANに集約するように努めなければならない。
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は、必要なセキュリティ水準を検討の上で適正な回線を選択し、及び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、及び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。
（市の職員が利用する端末や電磁的記録媒体等の管理）
第38条　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ずるものとし、かつ、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については、パスワードの入力、ICカード

の使用、生体認証等の複数の認証を必要とするよう設定しなければならない。
3　マイナンバー利用事務系における前項の複数の認証は、多要素認証としなければならない。

第6章　人的セキュリティ

(情報セキュリティポリシー等の遵守)

第39条　職員は、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。
2　職員は、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報告し、指示を受けなければならない。

(業務外における情報資産の持ち出し等の禁止)

第40条　職員は、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、市の電子メールアドレスの使用及び市のパソコン又はモバイル端末からのインターネットへのアクセスを行ってはならない。

(情報資産の持ち出し等の制限)

第41条　CISOは、職員が機密性2以上、可用性2又は完全性2の情報資産を外部で処理する場合は、当該情報資産に係る安全管理措置を定めなければならない。
2　職員は、情報資産を外部に持ち出し、又は外部で情報処理業務を行う場合は、あらかじめ情報セキュリティ管理者の許可を受けなければならない。

(配置外のパソコン等の使用)

第42条　職員は、原則として、配置されたパソコン、モバイル端末、電磁的記録媒体等以外のパソコン等を業務に使用してはならない。ただし、CISOが業務上必要と認める場合は、情報セキュリティ実施手順に従い、情報セキュリティ管理者の許可を得て使用することができる。
2　職員は、前項ただし書の場合において、外部で情報処理作業を行うときは、情報セキュリティ実施手順に定める安全管理に関する措置を実施しなければならない。

(持ち出し及び持込みの記録)

第43条　情報セキュリティ管理者は、情報資産の持ち出し及び持込みについて、記録を作成し、及び当該記録を保管しなければならない。

(セキュリティ設定変更の禁止)

第44条　職員は、配置されたパソコン及び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。

(離席時の端末等の管理)

第45条　職員は、配置されたパソコン等の使用中又は印刷された行政文書の閲覧中に離席するときは、当該パソコン若しくはモバイル端末が第三者に使用され、又は当該電磁的記録媒体若しくは行政文書に記録された情報が情報セキュリティ管理者の許可なく閲覧されることがないよう当該パソコン及びモバイル端末をロックし、並びに当該電磁的記録媒体及び行政文書を容易に閲覧されない場所へ保管する等の適正な措置を講じなければならない。

(退職時等の遵守事項)

第46条　職員は、異動、退職等により情報資産に係る業務を離れる場合は、当該情報資産を返却しなければならず、かつ、その後も業務上知り得た情報を漏らしてはならない。

（会計年度任用職員への対応）

第47条　情報セキュリティ管理者は、会計年度任用職員に対し、情報セキュリティポリシーその他本市の情報セキュリティに関する規程（以下「情報セキュリティ関係規程」という。）及び第122条に掲げる法令のうち会計年度任用職員が遵守すべき規定を教示し、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は、会計年度任用職員を任用するときは、必要に応じ、前項の遵守すべき規定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、会計年度任用職員に配置された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、電子メールの使用等が不要であるときは、これを利用できないようにしなければならない。

（情報セキュリティポリシー等の掲示）

第48条　情報セキュリティ管理者は、職員が常に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閲覧できるよう掲示しなければならない。

（外部委託事業者への対応）

第49条　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、保守等を外部委託事業者に委託する場合は、委託事業者が再委託を受ける事業者を含む当該外部委託事業者に対し、情報セキュリティ関係規程のうち外部委託事業者が守るべき規定を教示し、及び当該業務に係る機密事項の守秘義務について説明しなければならない。

（職員に対する研修及び訓練）

第50条　統括情報セキュリティ責任者は、職員に対し、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。

（研修計画の策定及び研修の実施）

第51条　統括情報セキュリティ責任者は、全ての職員に対する情報セキュリティに関する研修の計画の策定とその実施体制の構築を行い、最高情報セキュリティ責任者の承認を得なければならない。当該計画又は当該実施体制の変更を行ったときも、同様とする。

2　統括情報セキュリティ責任者は、新規採用の職員を対象とする研修を実施しなければならない。

3　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らその他職員のそれぞれの役割に応じた内容としなければならない。

4　統括情報セキュリティ責任者は、研修の実施状況の分析及び評価を行い、CISOに当該分析及び評価の結果を報告しなければならない。

5　CISOは、毎年度1回、石垣市情報セキュリティ委員会に対し、職員の研修の実施状況について報告しなければならない。

（緊急時対応訓練）

第52条　統括情報セキュリティ責任者は、緊急時対応を想定した情報セキュリティに関する訓練（以下「訓練」という。）を定期的に実施しなければならない。

2　訓練の計画は、ネットワーク及び各情報システムの規模等を考慮して実施の体制、範囲等を定めるものとし、かつ、効果的に実施できるものとしなければならない。

（研修及び訓練への参加）
第53条　全ての職員は、定められた研修及び訓練に参加しなければならない。
（庁内での情報セキュリティインシデントの報告）
第54条　職員は、情報セキュリティインシデントの可能性を認知した場合は、直ちに情報セキュリティ管理者及びPoCに報告しなければならない。
2　PoCの担当者は、前項の規定による報告を受けた場合は、当該報告の内容について、直ち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、第1項の規定による報告を受けた場合は、当該報告の内容について、直ちに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、第2項の規定による報告を受けた場合は、当該報告の内容について、必要に応じてCISOに報告しなければならない。
（外部の者からの情報セキュリティインシデントの報告）
第55条　職員は、住民等外部の者から情報セキュリティインシデントの可能性についての報告を受けた場合は、直ちに情報セキュリティ管理者及びPoCに報告しなければならない。
2　PoCの担当者は、前項の規定による報告を受けた場合は、当該報告の内容について、直ち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、第1項の規定による報告を受けた場合は、当該報告の内容について、直ちに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、第2項の規定による報告を受けた場合は、当該報告の内容について、必要に応じてCISOに報告しなければならない。
5　CISOは、住民等外部の者から情報セキュリティインシデントについての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。
（情報セキュリティインシデントへの対応）
第56条　CSIRTは、第54条第1項又は前条第1項の規定によりPoCに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、直ちに状況を確認し、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、前項の場合において、情報セキュリティインシデントであると評価したときは、直ちにCISOに報告しなければならない。
3　CSIRTは、第1項の情報セキュリティインシデントの内容に係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速やかに行わなければならない。
4　CSIRTは、第1項の情報セキュリティインシデントの原因を究明し、及びその記録を保存し、並びに当該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。
5　CISOは、前項の規定により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CSIRTに指示しなければならない。
（ICカードの取扱い）
第57条　職員は、自己の管理するICカードに関し、次に掲げる事項を遵守しなければならない。

(1)　認証に用いるICカードは、職員間で共有してはならない。
(2)　業務上必要のないときは、ICカード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。
(3)　ICカードを紛失した場合は、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、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、前項の規定による報告があった場合は、当該ICカード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カードを切り替える場合は、切替え前のICカードを回収し、破砕する等の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。
(IDの取扱い)
第58条　職員は、業務上管理するIDに関し、次の事項を遵守しなければならない。
(1)　自己のIDは、他人に利用させてはならない。
(2)　共用IDは、共用IDの利用者として登録された者以外の者に利用させてはならない。
(パスワードの取扱い)
第59条　職員は、業務上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、他人に知られないよう管理しなければならない。
(2)　パスワードは、秘密とし、そ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、その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、直ちに情報セキュリティ管理者に報告し、及びパスワードを変更しなければならない。
(5)　複数の情報システムにおいて同一のパスワードを設定してはならない。
(6)　仮のパスワード(初期パスワードを含む。)は、最初のログイン時点で変更しなければならない。
(7)　パスワードは、サーバ、ネットワーク機器及びパソコン等の端末に記憶させてはならない。
(8)　パスワード(共有IDに付随するパスワードを除く。)は、職員間で共有してはならない。

第7章　技術的セキュリティ

(文書サーバの設定等)
第60条　情報システム責任者は、職員が使用できる文書サーバの容量を設定し、職員に周知しなければならない。
2　情報システム責任者は、文書サーバを課等を単位として構成し、職員が他課のフォルダ及びファイルを閲覧し、及び使用することができないよう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、人事記録等の特定の職員のみが取り扱うデータについては、当該データを所管する課等においても当該特定の職員以外の職員の閲覧及び使用ができないよう別途ディレクトリを作成する等の措置を講じなければならない。
(バックアップの実施)
第61条　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、サーバの冗長化に係る対策の有無にかかわらず、必要に応じて定期的なバックア

ップを実施しなければならない。

（他団体との情報システムに関する情報等の交換）

第62条　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当該団体との間で定め、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承認を得なければならない。

（情報システムの作業記録の作成等）

第63条　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、当該作業の内容に係る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係る変更等の作業を行った場合は、当該作業の内容に係る記録を作成し、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、情報システム管理者若しくは情報システム担当者又は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、2名以上で作業するように努め、その作業を互いに確認しなければならない。

（情報システムの仕様書等の管理）

第64条　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、ネットワークの構成図及び情報システムの仕様書について、記録媒体の種類にかかわらず、紛失し、又は業務上必要とする者以外の者が閲覧すること等がないよう適正に管理しなければならない。

（ログの取得等）

第65条　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（情報システムの利用、情報機器の稼働、データ通信等の履歴の記録をいう。以下同じ。）その他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し、及び分析する機能をネットワーク及びサーバ上に設け、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確認しなければならない。

（障害記録）

第66条　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、職員からの情報システムの障害の報告、情報システムの障害に対する処理結果及び今後解決すべき障害の要因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。

（ネットワークの接続制御等）

第67条　統括情報セキュリティ責任者は、ネットワークの接続制御、経路制御等について、設定の不整合が発生しないようファイアウォール、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、ネットワークに係る適正なアクセス制御を行わなければならない。

（外部の者が利用できるシステムの分離等）

第68条　情報システム管理者は、電子申請の汎用受付システム等の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。

（外部ネットワークとの接続制限等）

第69条　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は、CISO及び統括情報セキュリティ責任者の承認を受けなければならない。

2　情報システム管理者は、前項に規定する場合において、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、第1項に規定する場合において、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は、外部の者が庁内ネットワークへ侵入することを防御するため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る場合において、情報資産に脅威が生じることが想定されるときは、統括情報セキュリティ責任者の指示に従い、直ち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。

（複合機のセキュリティ管理）

第70条　統括情報セキュリティ責任者は、複合機を調達する場合は、当該複合機が備える機能及び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、複合機が持つ電磁的記録媒体の全ての情報を抹消し、又は再利用できないようにする措置を講じなければならない。

（特定用途機器のセキュリティ管理）

第71条　統括情報セキュリティ責任者は、特定用途機器(IoT機器、テレビ会議システム、ネットワークカメラシステム、入退室管理システム等の特定の用途にのみ使用される機器をいう。)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。

（無線LAN及びネットワークの盗聴対策）

第72条　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。

（電子メールのセキュリティ管理）

第73条　統括情報セキュリティ責任者は、権限のない者により市の電子メールサーバを中継した外部から外部への電子メールの転送が行われることがない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、市の電子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と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、システムの開発、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の利用について、当該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。

（電子メールの利用制限）

第74条　職員は、統括情報セキュリティ責任者が必要と認める場合を除き、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　職員は、複数人に電子メールを送信する場合は、必要がある場合を除き、当該電子メールを受け取った者に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　職員は、重要な電子メールを誤送信した場合は、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。

5　職員は、統括情報セキュリティ責任者が必要と認める場合を除き、ウェブ上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。

（電子署名及び暗号化）

第75条　職員は、外部にデータを送信しようとする場合は、当該データに係る第13条の規定による取扱制限について確認し、当該データの機密性又は完全性を確保することが必要であるときは、CISOが定めた電子署名、暗号化、パスワード設定等のセキュリティ対策を行った上で送信しなければならない。

2　職員は、暗号化を行う場合は、CISOが定める方法以外の方法を用いてはならず、また、CISOが定めた方法により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(電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律(平成14年法律第153号)第17条第4項に規定する署名検証者をいう。)へ安全に提供しなければならない。

（無許可ソフトウェアの導入等の禁止）

第76条　職員は、配置されたパソコン及びモバイル端末(以下「業務用端末」という。)にソフトウェアを導入してはならない。

2　前項の規定にかかわらず、職員は、業務用端末にソフトウェアを導入する必要がある場合は、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、当該導入をすることができ

る。この場合において、情報セキュリティ管理者又は情報システム管理者は、当該ソフトウェアのライセンスを管理しなければならない。

3　職員は、業務用端末において、不正にコピーされたソフトウェアを利用してはならない。

（機器構成の変更の制限）

第77条　職員は、業務用端末の改造又は部品の増設若しくは交換(以下「改造等」という。)を行ってはならない。

2　前項の規定にかかわらず、職員は、業務用端末の改造等をする必要がある場合は、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受けて、当該改造等をすることができる。

（無許可でのネットワーク接続の禁止）

第78条　職員は、統括情報セキュリティ責任者の許可なく業務用端末を統括情報システム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。

（業務以外の目的でのウェブの閲覧の禁止）

第79条　職員は、業務以外の目的で業務用端末によりウェブサイト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、職員が明らかに業務に関係のないウェブサイトを業務用端末により閲覧していることを把握した場合は、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。

（Web会議サービスの利用時の対策）

第80条　統括情報セキュリティ責任者は、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。

2　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。

3　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。

4　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。

（ソーシャルメディアサービスの利用）

第81条　統括情報セキュリティ責任者は、本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、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。

(1)　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本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。

(2)　パスワードや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（ハードディスク、USBメモリ、紙等）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。

(3)　職員等は、統括情報セキュリティ責任者の許可なく第13条別表第２の機密性２以上の情報をソーシャルメディアサービスで発信してはならないこと。

(4)　情報セキュリティ責任者(管理者)は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こと。

(5)　統括情報セキュリティ責任者はアカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならないこと。

(アクセス制御)

第82条　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毎に、アクセスする権限のない職員がアクセスできないようシステム上の制限をしなければならない。

(利用者IDの取扱い)

第83条　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、情報システム等の利用に係るIDについて、利用者の登録、変更、抹消等の情報管理、職員の異動、出向又は退職に伴うIDの取扱い等の方法を定めなければならない。

2　職員は、情報システム等の利用に係るIDが必要なくなった場合は、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その旨を申し出なければならない。

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、前項の規定による申出があった場合は、当該申出に係るIDの登録を抹消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、利用されていないIDについて、人事管理部門と連携し放置されることのないよう管理しなければならない。

(特権を付与されたIDの管理等)

第84条　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(以下「代行者」という。)を必要最小限度の範囲とし、かつ、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及び付随するパスワードを厳重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、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搾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。

3　代行者は、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が承認した者でなければならない。

4　CISOは、前項の規定により代行者を承認した場合は、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。

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、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。

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、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。

(職員による外部からのアクセス等の制限)

第85条　職員は、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行うことができる職員については、外部からのアクセスが必要な合理的理由を有する必要最小限度の範囲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、職員による外部からのアクセスを認める場合は、情報システム上において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、前項に規定する場合において、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市の職員等に貸与する場合は、情報セキュリティの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、前項のモバイル端末を外部から持ち込み、又は外部から持ち帰った場合は、当該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、情報セキュリティ管理者の許可を得、又は情報セキュリティ管理者が定める手順に従って接続しなければならない。
7　統括情報セキュリティ責任者は、インターネット等の庁外ネットワークから庁内ネットワークに接続することを原則として禁止としなければならない。ただし、止むを得ず接続を許可する場合は、利用者のID、パスワード及び生体認証に係る情報等の認証情報並びに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。

（自動識別の設定）

第86条　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、機器の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。

（ログイン時の表示等）

第87条　情報システム管理者は、情報システムへのログイン時におけるメッセージの表示、ログイン試行回数の制限、アクセスタイムアウトの設定、ログインし、及びログアウトした時刻の表示等により正当なアクセスの権限を持つ職員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。

（認証情報の管理）

第88条　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、職員の認証情報を厳重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。
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、職員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から新しいパスワードに変更させなければならない。

（特権による情報システム等への接続の時間の制限）

第89条　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の時間を必要最小限に制限しなければならない。

（情報システムの調達）

第90条　情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、当該調達の方針について情報システム責任者と協議をした上で、当該調達に係る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　情報システム管理者は、機器又はソフトウェアの調達に当たっては、当該調達の方針について情報システム責任者と協議をした上で、調達しようとする機器又はソフトウェアのセキュリティ機能を調査し、情報セキュリティ上の問題がないことを確認しなければならない。

（情報システムの設計）

第91条　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。

2　情報システム管理者は、情報システムを設計する場合は、次に掲げる機能を組み込まなければならない。

(1)　情報システムに入力されるデータに係る範囲及び妥当性のチェック機能並びに不正な文字列等の入力を除去する機能

(2)　情報システム内の情報が改ざんされ、又は漏えいする可能性を検出する機能

（情報システムの開発）

第92条　情報システム管理者は、情報システムの開発を委託する場合は、当該開発に係る責任者及び担当者を特定しなければならない。

2　情報システム管理者は、情報システムの開発の責任者及び担当者が使用するIDを管理し、開発が完了した場合は、当該IDを削除しなければならない。

3　情報システム管理者は、情報システム開発の責任者及び担当者のネットワーク及び情報システムへのアクセスの権限を設定しなければならならない。

4　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担当者が使用するハードウェア及びソフトウェアを特定し、その使用を承認しなければならない。

5　情報システム管理者は、前項の規定により使用を承認し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システムから削除しなければならない。

（情報システムの導入）

第93条　情報システム管理者は、情報システムの開発、保守及び運用テスト環境と当該情報システムの運用環境を分離するよう努めなければならない。

2　情報システム管理者は、情報システムの開発、保守及び運用テスト環境から当該情報システムの運用環境への移行について、当該情報システムの開発及び保守に係る計画の策定時に手順を明確にしなければならない。

3　情報システム管理者は、前項の移行の際、移行を行う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度の範囲になるよう配慮しなければならない。

4　情報システム管理者は、情報システムを導入しようとする場合は、当該情報システムの可用性

が確保されていることを確認しなければならない。
5　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運用テストを行わなければならない。
6　情報システム管理者は、情報システムの運用テストを行う場合は、あらかじめ擬似環境における操作の確認を行わなければならない。
7　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前項の運用テストにおいて使用してはならない。
8　開発した情報システムに係る受入れテストを行う場合は、開発した者と導入する者が、それぞれ独立したテストを行わなければならない。

（情報システム開発に関する資料等の整備及び保管）

第94条　情報システム管理者は、情報システムの開発又は保守に関する資料その他情報システムに関する文書を適切に整備し、及び保管しなければならない。
2　情報システム管理者は、情報システムの開発に係る全てのテストの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。

（情報システムにおける入出力データの正確性の確保）

第95条　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　統括情報セキュリティ責任者は、情報システムにおいて、次のセキュリティ対策を実施しなければならない。
(1)　運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。
(2)　情報システムにおいて、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設計しなければならない。
3　統括情報セキュリティ責任者は、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。

（情報システムの変更管理）

第96条　情報システム管理者は、情報システムを変更した場合は、当該情報システムの仕様書等の変更の記録を作成しなければならない。

（ソフトウェアの更新等）

第97条　情報システム管理者は、情報システムの開発用若しくは保守用のソフトウェア等を更新し、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。

（情報システムの更新又は統合時の検証等）

第98条　情報システム管理者は、情報システムを更新し、又は統合する場合におけるリスク管理体制の構築、情報システムの更新又は統合の基準の明確化及び情報システムの更新又は統合後の業務運営体制の検証を行わなければならない。

（不正プログラムに対する統括情報セキュリティ責任者の措置事項）

第99条　統括情報セキュリティ責任者は、不正プログラムに係る対策として次に掲げる措置を講じなければならない。

(1)　外部ネットワークから受信したファイルについて、通信条件が異なるインターネットと庁内ネットワークの境界部分（以下「インターネットゲートウェイ」という。）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うこと。

(2)　外部ネットワークに送信するファイルについて、インターネット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うこと。

(3)　コンピュータウイルス等の不正プログラムに関する情報を収集し、必要に応じて職員に対する注意喚起を行うこと。

(4)　所掌するサーバ及び業務用端末にコンピュータウイルス等の不正プログラムに係る対策のためのソフトウェア(以下「不正プログラム対策ソフトウェア」という。)を常駐させること。

(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を常に最新の状態に保つこと。

(6)　不正プログラム対策ソフトウェアを常に最新の状態に保つこと。

(7)　更新パッチ、バージョンアップ等の開発元のサポートが終了したソフトウェアを業務において使用することを禁止すること(CISOがやむを得ない事情があると認める場合を除く。)。

（不正プログラムに対する情報システム管理者の措置事項）

第100条　情報システム管理者は、不正プログラムに係る対策にとして次に掲げる措置を講じなければならない。

(1)　所掌するサーバ及び業務用端末に不正プログラム対策ソフトウェアを常駐させること。

(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を常に最新の状態に保つこと。

(3)　不正プログラム対策ソフトウェアを常に最新の状態に保つこと。

(4)　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、市が管理する電磁的記録媒体以外の電磁的記録媒体の使用を禁止すること。

(5)　前号の情報システムにおいて、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すること。

(6)　不正プログラム対策ソフトウェア等の設定の変更に係る権限を一括管理し、情報システム管理者が必要と認める職員を除く職員等に当該権限を付与しないこと。

（不正プログラムに対する職員等の遵守事項）

第101条　職員等は、不正プログラムに係る対策として次に掲げる事項を遵守しなければならない。

(1)　業務用端末に導入されている不正プログラム対策ソフトウェアの設定を変更してはならない。

(2)　外部からデータを移入し、又はソフトウェアを導入する場合は、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)　差出人が不明であるファイル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PoCに報告しなければならない。

(4)　業務用端末に対して、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)　ファイルが添付され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によるチェックを行わなければならない。

(6)　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、所定の手順により無害化しなければならない。

(7)　統括情報セキュリティ責任者が提供するコンピュータウイルスに関する情報を常に確認しなければならない。

(8)　業務用端末がコンピュータウイルス等の不正プログラムに感染し、又は感染したことが疑われる場合は、直ちにPoCに報告し、その指示に従わなければならない。

(専門家の支援体制)

第102条　統括情報セキュリティ責任者は、前3条に規定する不正プログラムに係る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体制を整備しておかなければならない。

(不正アクセスに対する統括情報セキュリティ責任者の措置事項)

第103条　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に掲げる措置を講じなければならない。

(1)　使用されていないポートを閉鎖すること。

(2)　不要なサービスの機能を削除し、又は停止すること。

(3)　不正アクセスによるデータの書換えを検出し、及び当該検出につ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へ通報するためのシステムを機器に設定すること。

(4)　PoCと連携し、不正アクセスによるデータの書換えの監視、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対する当該書換えに係る通知、関係機関との連携、報道機関への情報提供等を適切に実施できる体制を構築すること。

(攻撃への対処)

第104条　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おそれがある場合は、情報システムの停止その他の必要な措置を講ずるとともに、総務省、沖縄県等と緊密に連携して当該攻撃に係る情報の収集に努めなければならない。

(違法行為への対応)

第105条　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において、当該攻撃が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)等に違反し、又は違反している可能性があるときは、当該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。

(内部からの攻撃への対策)

第106条　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、業務用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。

(職員等による不正アクセスへの処置)

第107条　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、当該職員が所属する課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。

（サービス不能攻撃への対策）

第108条　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、情報システムが外部から当該情報システムのサービスを停止させる攻撃を受け、当該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。

（標的型攻撃への対策）

第109条　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、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。

（セキュリティホールに係る対応）

第110条　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、及び必要に応じて関係者間で共有し、並びに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。

（不正プログラム等のセキュリティ情報の収集及び周知）

第111条　統括情報セキュリティ責任者は、不正プログラム等に係るセキュリティ情報を収集し、必要に応じて当該不正プログラム等への対応方法について職員等に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）

第112条　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、必要に応じて関係者間で共有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、情報セキュリティに関する社会環境又は技術環境の変化等による新たな脅威を認識した場合は、情報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。

第8章　運用

（情報システムの監視）

第113条　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の設定及びサーバ間の時刻の同期ができる措置を講じなければならない。

（情報セキュリティポリシー遵守状況の確認及び対処）

第114条　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、毎年度、情報セキュリティポリシーの遵守の状況について確認を行い、当該状況に問題を認めた場合は、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、前項の規定により報告を受けた問題について、適正かつ速やかに対処しなければならない。

（業務用端末等の利用状況の調査）

第115条　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、職員が使用している業務用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。

(職員の報告義務)

第116条　職員は、情報セキュリティポリシーに違反する行為(以下「違反行為」という。)を発見した場合は、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　職員は、前項に規定する場合において、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判断したときは、次条の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。

(緊急時対応計画の策定)

第117条　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に違反する行為等により情報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の対応計画(以下「緊急時対応計画」という。)を策定するとともに、情報セキュリティ侵害が発生したときは、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。

(緊急時対応計画に定める事項)

第118条　緊急時対応計画には、次に掲げる事項を定めるものとする。

(1)　情報セキュリティに係る関係者の連絡先

(2)　発生した情報セキュリティ侵害事案に係る報告すべき事項

(3)　発生した情報セキュリティ侵害事案への対応に係る措置

(4)　再発防止措置の決定

(業務継続計画との整合性の確保)

第119条　石垣市情報セキュリティ委員会では、石垣市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。

(緊急時対応計画の見直し)

第120条　CISOは、情報セキュリティを取り巻く状況の変化、組織体制の変動等に応じ、緊急時対応計画の規定を見直さなければならない。

(例外措置)

第121条　情報セキュリティ管理者及び情報システム管理者は、大規模な災害等により情報セキュリティ関係規程を遵守することが困難な状況において、行政事務の適正な遂行を継続するため、情報セキュリティ関係規程に定める方法とは異なる方法を採用し、又は情報セキュリティ関係規程に定める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は、CISOの許可を得て情報セキュリティ関係規程に定める措置以外の措置(以下「例外措置」という。)を講ずることができる。

2　情報セキュリティ管理者及び情報システム管理者は、例外措置を講ずる場合において、特に緊急を要するためCISOの許可を受ける時間的余裕がないと認めるときは、前項の規定にかかわらず、CISOの許可を得ずに例外措置を講ずることができる。この場合において、情報セキュリティ管理者

及び情報システム管理者は、当該例外措置の実施後速やかにCISOに当該例外措置についての報告をしなければならない。
3　CISOは、前2項の規定により例外措置が実施されたときは、その内容が適正であるかの審査を行うものとする。
4　CISOは、第1項又は第2項の規定による例外措置の実施に係る書類及び前項の審査の結果に係る書類を適正に保管し、定期的に実施状況を確認しなければならない。

(法令遵守)

第122条　職員は、職務の遂行において使用する情報資産を保護するため次に掲げる法令その他の関係法令を遵守しなければならない。

(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218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)　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2号)
(6)　サイバーセキュリティ基本法(平成28年法律第31号)
(7)　石垣市個人情報保護条例(平成13年12月21日条例第24号)

(懲戒処分)

第123条　違反行為を行った職員及びその監督責任者は、その行為の重大性、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。

(違反行為への対応)

第124条　統括情報セキュリティ責任者は、職員の違反行為を確認した場合は、当該職員が所属する課等の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。
2　職員は、違反行為を確認した場合は、速やかに統括情報セキュリティ責任者及び当該違反行為をした職員が所属する課等の情報セキュリティ管理者に通知するものとし、当該通知を受けた情報セキュリティ管理者は、当該違反行為に係る適正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は、違反行為が前2項の規定による情報セキュリティ管理者の指導等によっても改善されない場合は、当該職員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し、又は剥奪することができる。この場合において、統括情報セキュリティ責任者は、当該権利を停止し、又は剥奪した旨を速やかにCISO及び当該職員が所属する課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。

第9章　外部サービスの利用

(外部委託事業者の選定基準)

第125条　情報セキュリティ管理者は、外部委託事業者の選定にあたり、委託の内容に応じた情セキュリティ対策が実施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の取得状況、情報セキュリティ監査の実施状況等を考慮して外部委託事業者を選定しなければならない。

(契約項目)

第126条　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次に掲げる情報セキュリティに係る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及び範囲並びにアクセス方法

(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)　再委託に関する制限事項の遵守

(9)　委託業務終了時の情報資産の返還、廃棄等

(10)　委託業務に係る定期報告及び緊急時報告の義務

(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の違反に係る損害賠償責任その他当該違反があった場合の措置

(確認、措置等)

第127条　情報セキュリティ管理者は、外部委託の契約期間中において当該外部委託事業者が必要な情報セキュリティ対策を実施していることを定期的に確認し、必要に応じて前条の契約による措置を実施しなければならない。

2　情報セキュリティ管理者は、前項の規定により第126条の契約による措置を実施した場合は、当該措置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。

(約款による外部サービスの利用)

第128条　情報セキュリティ管理者は、約款による外部サービスの利用に関し、次に掲げる事項を規定する規程を整備しなければならない。

(1)　約款による外部サービスを利用してよい範囲

(2)　業務により利用する約款による外部サービス

(3)　外部サービスの利用に係る手続及び運用の手順

(4)　機密性2以上の情報の取扱いの禁止

2　職員は、約款による外部サービスの利用をする場合は、前項により定めた規程を遵守しなければならない。

3　職員は、約款による外部サービスの利用をしようとする場合は、当該サービスの約款その他当該外部サービスの提供の条件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、適切な措置を講じた上で当該外部サービスを利用しなければならない。

(ソーシャルメディアサービスの利用)

第129条　統括情報セキュリティ責任者は、本市が管理するアカウントでのソーシャルメディアサービスの利用に関し、情報セキュリティ対策に係る次に掲げる事項を規定するガイドラインを定めなければならない。

(1)　情報を発信したアカウントが本市のものであることを明らかにするため本市が自己で管理するウェブサイトに当該情報を掲載して参照可能な状態とするとともに、当該ソーシャルメディアサービスにおける自由記述欄等に当該アカウントを運用する課等を明示する等の方法によりなりすまし対策を実施すること。

(2)　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ICカード等の媒体を適正に管理するなどの方法により不正アクセス対策を実施すること。

2　情報システム責任者は、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。

3　職員は、機密性2以上の情報をソーシャルメディアサービスで発信してはならない。

4　職員は、第三者によるアカウントの乗っ取り又はなりすましを確認した場合は、第54条の規定の例により当該乗っ取り又はなりすましに係る報告を行い、及び被害を最小限にするために必要な措置を講じなければならない。

（クラウドサービスの選定に係る運用規程の整備）

第130条　統括情報セキュリティ責任者は、機密情報2以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定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判断する基準（以下「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

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クラウドサービス提供者の選定基準に含めなければならない。

(1)　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

(2)　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

(3)　クラウドサービスの提供に当たり、クラウドサービス提供者もしくはその従業員、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

(4)　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、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やリージョンの指定

(5)　情報セキュリティインシデントへの対処方法

(6)　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

(7)　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

(8)　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

(9)　情報セキュリティ監査の受入れ

(10)　サービスレベルの保証

3　情報セキュリティ責任者は、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及び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・裁判管轄を選定基準に含めなければならない。

4　情報セキュリティ責任者は、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基準に含めなければならない。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。

(クラウドサービスの利用に係る運用規程の整備)

第131条　統括情報セキュリティ責任者は、機密性2以上の情報を取り扱う場合、以下を含むクラウドサービスの利用に関する規程を整備しなければならない。

2　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、クラウドサービスを利用して情報システムを導入・構築及び運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

3　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、以下を全て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の基本方針を運用規程として整備しなければならない。

(1)　クラウドサービスの利用終了時における対策

(2)　クラウドサービスで取り扱った情報の廃棄

(3)　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

(クラウドセキュリティ要件の策定)

第132条　情報セキュリティ責任者は、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、以下を全て含むセキュリティ要件を定めなければならない。

(1)　クラウドサービスに求める情報セキュリティ対策

(2)　クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(3)　クラウドサービスに求めるサービスレベル

2　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。

(クラウドサービスの利用に係る調達・契約)

第133条　情報セキュリティ責任者は、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　情報セキュリティ責任者は、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、利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。

（クラウドサービスの利用申請）

第134条　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。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。

（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）

第135条　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。
(1)　不正なアクセスを防止するためのアクセス制御
(2)　取り扱う情報の機密性保護のための暗号化
(3)　開発時におけるセキュリティ対策
(4)　設計・設定時の誤りの防止
2　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告しなければならない。
3　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。
(1)　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
(2)　クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順
(3)　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順
4　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・記録しなければならない。

（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）

第136条　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。
(1)　クラウドサービス利用方針の規定
(2)　クラウドサービス利用に必要な教育
(3)　取り扱う資産の管理

(4)　不正アクセスを防止するためのアクセス制御
(5)　取り扱う情報の機密性保護のための暗号化
(6)　クラウドサービス内の通信の制御
(7)　設計・設定時の誤りの防止
(8)　クラウドサービスを利用した情報システムの事業継続

2　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告しなければならない。

3　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

4　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、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。

5　クラウドサービス管理者は、前各号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。

（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）

第137条　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。

(1)　クラウドサービスの利用終了時における対策
(2)　クラウドサービスで取り扱った情報の廃棄
(3)　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・記録しなければならない。

第10章　評価・見直し

（自己点検）

第138条　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情報セキュリティ対策に係る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。

（報告）

第139条　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、前条の規定による自己点検を行った場合は、当該自己点検の結果と当該結果に基づく情報セキュリティ対策の改善策を決定し、石垣市情報セキュリティ委員会に報告しなければならない。

（自己点検結果の活用）

第140条　職員は、第138条の規定による自己点検の結果に基づき自己の権限の範囲内で情報セキュ

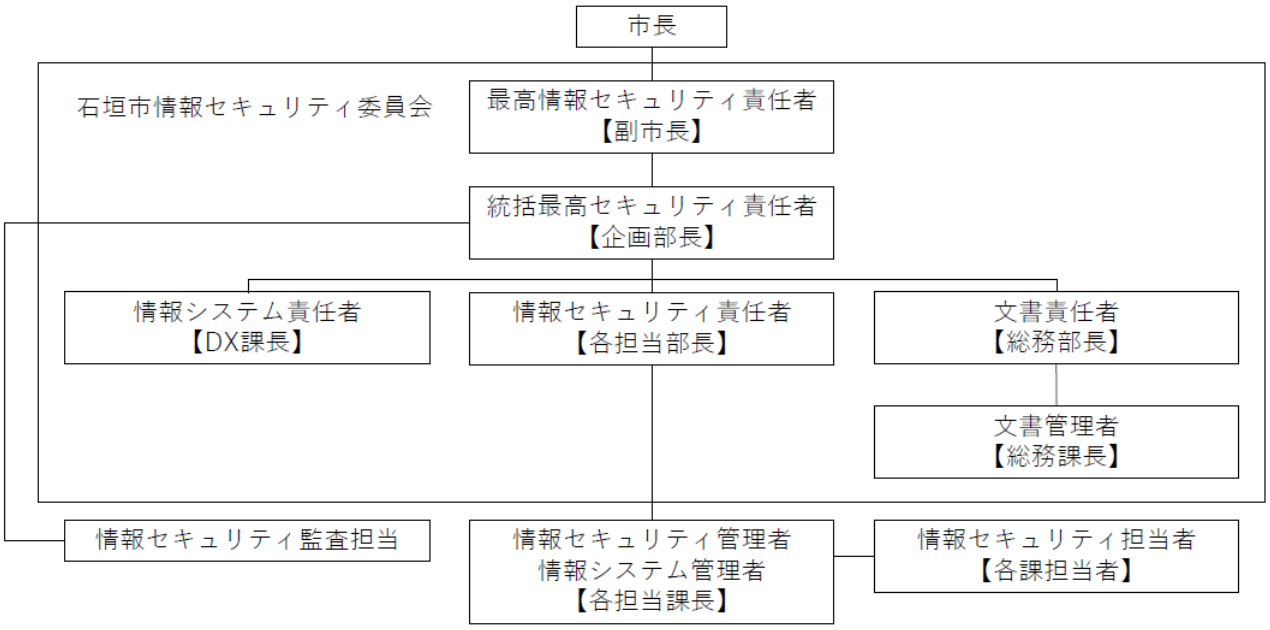
リティ対策の改善を図らなければならない。

2　石垣市情報セキュリティ委員会は、前条の規定により報告を受けた自己点検の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を行う場合において活用しなければならない。

（情報セキュリティポリシー及び関係規程等の見直し）

第141条　石垣市情報セキュリティ委員会は、第139条の規定により報告を受けた自己点検の結果及び情報セキュリティに関する状況の変化等を踏まえ、毎年度及び当該状況の重大な変化が発生した場合において情報セキュリティポリシー及び関係規程等の評価を行い、必要があると認めるときは、情報セキュリティポリシー又は関係規程等の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。

別表第1(第10条関係)



別表第2(第13条関係)

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 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）に定める秘密文書に相当する文書	・支給された端末以外での作業禁止（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、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
機密性 3B	行政事務で取り扱う情報資産のうち、漏えい等が発生した際に、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	
機密性 3C	行政事務で取り扱う情報資産のうち、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	
機密性2	行政事務で取り扱う情報資産のうち、機密性3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	機密性2又は機密性3の情報資産以外の情報資産	―

別表第3(第13条関係)

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、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	完全性2の情報資産以外の情報資産	―

別表第4(第13条関係)

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、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	可用性2の情報資産以外の情報資産	―