資料１－２

石巻市情報セキュリティポリシー　新旧対応表

改　　正	現　　行
石巻市情報セキュリティポリシー	石巻市情報セキュリティポリシー
目次	目次
第１章　情報セキュリティ基本方針	第１章　情報セキュリティ基本方針
１～10　（略）	１～10　（略）
11　監査及び自己点検の実施	11　監査
12　（略）	12　（略）
第２章　情報セキュリティ対策基準	第２章　情報セキュリティ対策基準
１～７　（略）	１～７　（略）
８　業務委託と外部サービスの利用	８　法令等の遵守
９　法令等の遵守	９　評価・見直し等
10　評価・見直し等	
第１章　情報セキュリティ基本方針	第１章　情報セキュリティ基本方針
１　（略）	１　（略）
２　用語の定義	２　用語の定義
情報セキュリティポリシーにおける用語の意義は、次に定めるところによる。	情報セキュリティポリシーにおける用語の意義は、次に定めるところによる。
（１）　ネットワーク	（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、その構成機器をいう。	データの受渡しを行うため、電子計算機（附属機器含む。以下この号において同じ。）と電子計算機を通信回線により相互に結合した処理を行う仕組みをいう。
（２）～（３）　（略）	（２）～（３）　（略）
（４）　情報システム	（４）　情報システム
情報を処理するためのハードウェア、ソフトウェア、ネットワーク、電磁的記録媒体及びその関連機器で構成され、処理を行なう仕組みをいう。	情報を処理するためのハードウェア、ソフトウェア、その関連機器及びネットワーク等で構成され、処理を行なう仕組みをいう。
（５）　（略）	（５）　（略）
（６）　電磁的記録媒体	（６）　記録媒体
情報システムでデータ等を記録するための磁気ディスク、磁気テープ、フロッピーディスク、保存用メモリ等をいう。	情報システムでデータ等を記録するための磁気ディスク、磁気テープ、フロッピーディスク等をいう。

（７）（略） （８）　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。 （９）　完全性 情報が破壊、改ざん又は消去されない状態を確保することをいう。 (10)　可用性 情報にアクセスすることを認められた者だけが、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。 (11)　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。 (12)　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。） (13)　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。 (14)　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。 (15)　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	（７）（略）

等、安全が確保された通信をいう。	
３～５　（略）	３～５　（略）
６　情報資産への脅威 情報資産に対して想定される脅威は、その発生頻度や発生した場合の影響を考慮するものとし、特に認識すべき脅威については次のとおりとする。	６　情報資産への脅威 情報資産に対して想定される脅威は、その発生頻度や発生した場合の影響を考慮するものとし、特に認識すべき脅威については次のとおりとする。
（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	（１）　部外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等
（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・設定のミス、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	（２）　職員及び外部委託業者による意図しない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持出･盗聴･改ざん・消去、機器及び記録媒体の盗難、規定外の情報システム接続や操作によるデータ漏洩等
（３）　職員及び外部委託業者による意図しない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持出･盗聴･改ざん・消去、機器及び電磁的記録媒体の盗難、規定外の情報システム接続や操作によるデータ漏洩等	（３）　地震、落雷、火災、水害等の災害並びに事故、故障等によるの施錠可能な場所への保管業務の停止
（４）　地震、落雷、火災、水害等の災害並びに事故、故障等によるサービス及び業務の停止	
（５）　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	
（６）　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	
７　情報セキュリティ対策 情報資産を脅威から保護するため、次に定める情報セキュリティ対策を講ずるものと	７　情報セキュリティ対策 情報資産を脅威から保護するため、次に定める情報セキュリティ対策を講ずるものと

する。 （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） 物理的セキュリティ対策 情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講ずる。また、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により、情報資産の流出を防ぐ。 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、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの	する。 （１） 物理的セキュリティ対策 情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講ずる。 （２） 人的セキュリティ対策 情報セキュリティに関する権限や責任を定めるとともに、情報資産に関する業務に携わる全ての職員に情報セキュリティポリシーを周知徹底するための教育を実施する等の必要な対策を講じる。 （３） 技術的セキュリティ対策 情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウィルス対策ソフトの導入等の技術面における対策を講じる。

導入等を実施する。 （４） 人的セキュリティ対策 情報セキュリティに関する権限や責任を定めるとともに、情報資産に関する業務に携わる全ての職員に情報セキュリティポリシーを周知徹底するための教育を実施する等の必要な対策を講じる。 （５） 技術的セキュリティ対策 情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウィルス対策ソフトの導入等の技術面における対策を講じる。 （６） 運用におけるセキュリティ対策 システム開発の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面における対策を講じるとともに緊急事態の発生に備えた危機管理対策を講じる。 （７） 業務委託と外部サービスの利用 業務委託などにより外部サービスを利用する場合は､以下の対策を講ずるものとする。 ア 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書を締結し、委託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。 イ 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。 ウ 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の責任者を定める。 （８） 評価及び見直し	（４） 運用におけるセキュリティ対策 システム開発の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面における対策を講じるとともに緊急事態の発生に備えた危機管理対策を講じる。

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、適時情報セキュリティポリシーの見直しを行う。	
８　（略）	８　（略）
９　情報セキュリティ実施手順の策定 情報セキュリティ対策基準を遵守した情報セキュリティ対策を実施するため、各部局等が管理する個々の情報資産については、それぞれ情報セキュリティ実施手順を定めるものとする。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。	９　情報セキュリティ実施手順の策定 情報セキュリティ対策基準を遵守した情報セキュリティ対策を実施するため、各部局等が管理する個々の情報資産については、それぞれ情報セキュリティ実施手順を定めるものとする。
10　（略）	10　（略）
11　監査及び自己点検の実施 情報セキュリティポリシーが遵守されていることを検証するため、定期的又は必要に応じて監査及び自己点検を実施する。	11　監査 情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施する。
12　（略）	12　（略）
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とは、情報セキュリティ基本方針を実行に移すための本市の情報資産に関する情報セキュリティ対策の基準である。	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とは、情報セキュリティ基本方針を実行に移すための本市の情報資産に関する情報セキュリティ対策の基準である。
１　（略）	１　（略）
２　管理体制 石巻市の情報セキュリティ管理については、以下の組織・体制とする。	２　管理体制 石巻市の情報セキュリティ管理については、以下の組織・体制とする。
（１）　最高情報セキュリティ責任者 ア　最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）は、最高情報責任者（以下「ＣＩＯ」という。）が兼務する。	（１）　最高情報統括責任者 石巻市における全ての情報資産を統括する最高責任者として、市長をもって充てる。

イ　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。 ウ　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くことができる。 エ　ＣＩＳＯは、本対策基準に定められた自らの業務を、本対策基準に定める責任者に担わせることができる。 オ　ＣＩＳＯは、情報セキュリティインシデントに対処するための体制(以下「ＣＳＩＲＴ」という。)を整備し、役割を明確化する。	
（２）　情報セキュリティ責任者 ア　次の職にある者を情報セキュリティ責任者とする。 (ア)～(カ)　(略) イ　情報セキュリティ責任者は、所掌に属する部局等における情報セキュリティに関する総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、所掌に属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、助言及び指示を行う。	（２）　統括情報セキュリティ担当者 ア　次の職にある者を統括情報セキュリティ担当者とする。 (ア)～(カ)　(略) イ　統括情報セキュリティ担当者は、所掌に属する部局等における情報セキュリティに関する総括的な権限及び責任を有する
（３）　情報セキュリティ管理者 ア　情報資産を利用する課等におけるセキュリティ対策を実施するため、情報セキュリティ管理者を置き、情報資産を利用する課等の所属長をもって充てる。 イ　情報セキュリティ管理者は、所掌に属する課等における情報セキュリティに関する総括的な権限及び責任を有する。	（３）　情報セキュリティ担当者 ア　情報資産を利用する課等におけるセキュリティ対策を実施するため、情報セキュリティ担当者を置き、情報資産を利用する課等の所属長をもって充てる。 イ　情報セキュリティ担当者は、情報セキュリティポリシーに定められている事項について職員に実施及び遵守させなければならない。

ウ　情報セキュリティ管理者は、情報セキュリティポリシーに定められている事項について職員に実施及び遵守させなければならない。	ウ　情報セキュリティ担当者は、非常勤職員及び臨時的任用職員の任用時に必ず情報セキュリティポリシーのうち、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。
エ　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及びＣＳＩＲＴへ速やかに報告を行い、指示を仰がなければならない。	
（４）　ネットワーク管理者 ア～イ　（略）	（４）　ネットワーク管理者 ア～イ　（略） ウ　ネットワーク管理者は、ネットワークの適正かつ効率的な運用を図るため、ネットワーク接続基準を定めるものとする。
ウ　（略）	エ　（略）
（５）～（７）　（略）	（５）～（７）　（略）
（８）　石巻市デジタル・トランスフォーメーション推進本部 情報資産の適正かつ効率的な管理運営を行うため、石巻市デジタル・トランスフォーメーション推進本部(以下「推進本部」という。)において、情報セキュリティ対策基準等セキュリティに関する重要な事項を審議する。	（８）　石巻市情報化推進本部 情報資産の適正かつ効率的な管理運営を行うため、石巻市情報化推進本部(以下「推進本部」という。)において、情報セキュリティ対策基準等セキュリティに関する重要な事項を審議する。
（９）　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。	

(10)　ＣＳＩＲＴの設置・役割 ア　ＣＳＩＲＴを復興企画部ＩＣＴ総合推進課に設置し、ＣＳＩＲＴ責任者に復興企画部ＩＣＴ総合推進課長を充てる。 イ　ＣＳＩＲＴに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情報セキュリティ管理者より報告を受けた場合には、その状況を確認し、ＣＩＳＯへ報告しなければならない。 ウ　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。 エ　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。 オ　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。 カ　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。	
３　情報の管理 （１）　情報の定義 本ポリシーで定義する重要な情報とは、以下のものをいう。 (ア)　個人情報の保護に関する法律(平成17年法律第57号)第60条第１項に規定する保有個人情報 (イ)　法令又は条例(以下「法令等」という。)の定めにより守秘義務を課されている情報((ア)の保有個人情報を除く。) (ウ)～(キ)　(略) （２）　情報の分類と管理	３　情報の管理 （１）　情報の定義 本ポリシーで定義する重要な情報とは、以下のものをいう。 (ア)　石巻市個人情報保護条例(平成17年石巻市条例第15号)第２条第１号に規定する個人情報 (イ)　法令又は条例(以下「法令等」という。)の定めにより守秘義務を課されている情報((ア)の個人情報を除く。) (ウ)～(キ)　(略)

ア　情報資産の分類 本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類する。 (ア)　機密性による情報資産の分類 本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類する。 a　行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産を機密性３とする b　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を機密性２とする c　機密性２又は機密性３に該当する情報資産以外の情報資産 (イ)　完全性による情報資産の分類 a　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を完全性２とする b　完全性２の情報資産以外の情報資産を完全性１とする。 (ウ)　可用性による情報資産の分類 a　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を可用性２とする b　可用性２の情報資産以外の情報資産を可用性１とする。 イ　情報資産の取扱制限 本市における情報資産は、必要に応じ、次のとおり取扱制限を行うものとする。 (ア)　分類が機密性２又は機密性３に該当		

する情報資産 a　支給以外の端末での作業の原則禁止 b　必要以上の複製及び配布の禁止 c　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 d　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 e　復元不可能な処理を施しての廃棄 f　信頼のできるネットワーク回線の選択 g　外部で情報処理を行う際の安全管理措置の規定 h　電磁的記録媒体の施錠可能な場所への保管 （イ）　分類が完全性２に該当する情報資産 a　バックアップ及び電子署名の付与 b　外部で情報処理を行う際の安全管理措置の規定 c　電磁的記録媒体の施錠可能な場所への保管 （ウ）　分類が可用性２に該当する情報資産 a　バックアップ、指定する時間以内の復旧 b　電磁的記録媒体の施錠可能な場所への保管	
（３）　情報の管理責任 ア　情報は、当該情報を作成した各部局等が管理責任を有する。 イ　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分類に基づき管理しなければならない。	（２）　情報の管理責任 情報は、当該情報を作成した各部局等が管理責任を有する。
（４）　情報資産の分類の表示 職員等は、情報資産について、ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産	

の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。	
（５） 情報の管理方法 ア　情報の管理及び取扱 (ア)～(イ) （略） （ウ） 職員等は、業務上必要のない情報を作成してはならない。 （エ） 情報を作成する者は、情報の作成時に当該情報の分類と取扱制限を定めなければならない。 （オ） 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。 （カ） 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。 （キ） 庁外の者が作成した情報資産を入手した者は、当該情報の分類と取扱制限を定めなければならない。 （ク） 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。 （ケ） 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。 （コ） 情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。 （サ） 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。 （シ） 電子メール等により機密性２以上の情報を送信する者は、必要に応じ、パスワ	（３） 情報の管理方法 ア　情報の管理及び取扱 (ア)～(イ) （略）

ード等による暗号化を行わなければならない。 （ス） 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。 （セ） 機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。 （ソ） 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。 （タ） 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。	
イ 電磁的記録媒体の管理 （ア） 取り出しが可能な電磁的記録媒体は、適切な管理を行わなければならない。 （イ） 重要な情報を記録した取り外し可能な電磁的記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない。 （ウ） 重要な情報を記録した電磁的記録媒体を外部に持出しする場合は、職員又は守秘義務を明記した契約等を締結した外部業者に行わせるとともに、電磁的記録媒体の物理的な保護措置を講じなければならない。 （エ） 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。 （オ） 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。	イ 記録媒体の管理 （ア） 取り出しが可能な記録媒体は、適切な管理を行わなければならない。 （イ） 重要な情報を記録した取り外し可能な記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない。 （ウ） 重要な情報を記録した記録媒体を外部に持出しする場合は、職員又は守秘義務を明記した契約等を締結した外部業者に行わせるとともに、記録媒体の物理的な保護措置を講じなければならない。

（カ） 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。 （キ） 情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、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。 （ク） 車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、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。	
ウ 電磁的記録媒体の処分 （ア） 電磁的記録媒体が磨耗等により不要となった場合は、当該媒体に記録されている重要な情報をいかなる方法によっても復元できないように消去等を行った上で廃棄しなければならない。 （イ） 重要な情報を記録した電磁的記録媒体の廃棄は、情報セキュリティ担当者の許可を得ることとし、廃棄を行った日時、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、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。 （エ） 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	ウ 記録媒体の処分 （ア） 記録媒体が磨耗等により不要となった場合は、当該媒体に記録されている重要な情報をいかなる方法によっても復元できないように消去等を行った上で廃棄しなければならない。 （イ） 重要な情報を記録した記録媒体の廃棄は、情報セキュリティ担当者の許可を得ることとし、廃棄を行った日時、担当者及び処理内容を記録しなければならない。

い。 （オ）　情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。	
４　物理的セキュリティ （１）　サーバの設置等 ア～イ　（略） ウ　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。 エ　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、同一データを保持するのが望ましい。 オ　メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にすることが望ましい。 カ　機器を廃棄や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講じなければならない。 キ　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、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、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。	４　物理的セキュリティ （１）　サーバの設置等 ア～イ　（略）
（２）　電源 ア　停電及び電圧異常等の電源障害により業務処理に支障を来す恐れのある情報システムの機器については、当該機器を適切に停止するまでの間に必要な電力を供給する	（２）　電源 停電及び電圧異常等の電源障害により業務処理に支障を来す恐れのある情報システムの機器については、当該機器を適切に停止するまでの間に必要な電力を供給する容量

容量の予備電源を備え付ける等の措置を講じなければならない。 イ　落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。	の予備電源を備え付ける等の措置を講じなければならない。
（３）　配線 ア～イ　（略） ウ　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。 エ　主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理者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。 オ　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。 カ　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講じなければならない。	（３）　配線 ア～イ　（略）
（４）　外部に設置する装置 ア　外部に設置する装置は、ＣＩＳＯの承認を受けたものでなければならない。 イ　ネットワーク管理者又はシステム担当者は、定期的に外部に設置した装置の情報セキュリティの水準について確認をしなければならない。	（４）　外部に設置する装置 ア　外部に設置する装置は、最高情報統括責任者の承認を受けたものでなければならない。 イ　最高情報統括責任者は、定期的に外部に設置した装置の情報セキュリティの水準について確認をしなければならない。 ウ　石巻市以外に持ち出される端末、記録媒体等については、石巻市以外での使用方法を定め、管理簿等を設ける等適切に管理しなければならない。
（５）　機器室の管理等 ア　機器室 (ア)～(イ)　（略）	（５）　機器室の管理等 ア　機器室 (ア)～(イ)　（略）

（ウ） 防火対策を施すとともに、サーバや電磁的記録媒体に影響を与えない消火剤を用いた消火器を設置しなければならない。	（ウ） 防火対策を施すとともに、サーバや記録媒体に影響を与えない消火剤を用いた消火器を設置しなければならない。
（エ）（略） （オ） 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「情報システム室」という。）や電磁的記録媒体の保管庫をいう。 （カ） 外部からの侵入が容易にできないように無窓の外壁にしなければならない。 （キ） 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。 （ク） 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。 （ケ） 管理区域を囲む外壁等の床下開口部を全て塞がなければならない。 （コ） 管理区域に配置する消火薬剤や消防用設備等が、機器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。	（エ）（略）
イ 入退室の管理等 （ア） 機器室の入退室は許可された者のみとし、入退室管理簿の記載等、適切な管理をしなければならない。 （イ） 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。 （ウ） 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。	イ 入退室の管理等 機器室の入退室は許可された者のみとし、入退室管理簿の記載等、適切な管理をしなければならない。

(エ)　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。 (オ)　機密性２以上の情報資産を扱う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、また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。	
ウ　機器等の搬入・搬出 (ア)～(イ)　(略) (ウ)　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。 (エ)　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。	ウ　機器等の搬入・搬出 (ア)～(イ)　(略)
(６)　ネットワーク 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、施設管理者と連携し、適正に管理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、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の回線を選択し、必要に応じて送受信される情報の暗号化を行わなければならない。 エ　ネットワーク管理者は、ネットワーク	(６)　ネットワーク 外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

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。 オ　ネットワーク管理者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。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。 カ　ネットワーク管理者は、マイナンバー利用事務系、ＬＧＷＡＮ接続系、インターネット接続系にネットワークを分類し、相互の通信ができないようにしなければならない。 キ　ネットワーク管理者は、マイナンバー利用事務系とＬＧＷＡＮ接続系との通信を行う必要がある場合は、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番号による通信制限を行わなければならない。 ク　ネットワーク管理者は、ＬＧＷＡＮ接続系とインターネット接続系との通信を行う必要がある場合は、必要な通信だけを許可する通信制限を行わなければならない。 ケ　ネットワーク管理者は、インターネット接続系において、自治体情報セキュリティクラウドに参加するとともに、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。 コ　ネットワーク管理者は、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、インターネット接続系に関するセキュリティ対策について、定期的に外部監査を実施しなければならない。 サ　ネットワーク管理者は、マイナンバー利用事務系と外部接続先は相互の通信ができないようにしなければならない。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い。 シ　ネットワーク管理者は、マイナンバー利用事務系の端末において、情報システムが正規の利用者かどうかを判断するため、原則として多要素認証を利用しなければならない。 ス　ネットワーク管理者は、マイナンバー利用事務系の端末において、電磁的記録媒体による端末からの情報持ち出しが、原則としてできないように設定しなければならない。 セ　ネットワーク管理者は、ＬＧＷＡＮ接続系とインターネット接続系の通信のうち、インターネット接続系からＬＧＷＡＮ接続系に取り込む場合は、原則として次の方法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ＬＧＷＡＮ接続系に転送する方式		

（7） 執務室の管理等 ア　情報セキュリティ管理者は、重要な情報が記録されている電磁的記録媒体の保管場所及びそれを取り扱う情報機器の設置場所(機器室を除く。)への入退室の管理について必要な措置を講じなければならない。 イ　情報セキュリティ管理者は、執務室に職員等が不在となる場合には、施錠等の盗難及び部外者の侵入を防ぐ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は、執務室における機器の配置について、のぞき見等を防ぐための必要な措置を講じなければならない。 エ　情報セキュリティ管理者は、盗難防止のため、執務室等で利用する端末の固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。 オ　情報セキュリティ管理者は、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。 カ　情報セキュリティ管理者は、執務室内のネットワーク配線やネットワーク機器をネットワーク管理者以外が変更・追加できないように必要な措置を講じなければならない。 キ　情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。 ク　情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。	（7） 執務室の管理等 ア　情報セキュリティ担当者は、重要な情報の記録されている媒体保管場所及びそれを取り扱う情報機器の設置場所(機器室を除く。)への入退室の管理について必要な措置を講じなければならない。 イ　執務室に職員等が不在となる場合には、施錠等の盗難及び部外者の侵入を防ぐ措置を講じなければならない。

ケ　情報システム管理者は、端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。	
５　人的セキュリティ	５　人的セキュリティ
（１）　職員等	（１）　職員等
ア　情報セキュリティ対策の遵守義務	ア　情報セキュリティ対策の遵守義務
(ア)～(イ)　(略)	(ア)～(イ)　(略)
(ウ)　職員等は、業務以外の使用目的で、情報資産を使用してはならない。	
(エ)　職員等は、業務以外の使用目的で、情報システムやネットワークを使用してはならない。	
(オ)　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、その後も業務上知り得た情報を漏らしてはならない。	
イ　その他	イ　その他
(ア)　職員等は、業務で使用する場合であっても、電子的記録媒体やネットワークを介して機密性２以上の情報資産を外部に複製・移動・転送・持ち出し等を行う場合は、あらかじめ情報セキュリティ管理者の許可を得なければならない。	(ア)　職員等は、情報システム管理者の許可を得ずに、情報システムの機器、記録媒体等を執務室外に持ち出してはならない。
(イ)　職員等は、業務で使用する場合であっても、端末、電磁的記録媒体、その他ハードウェア及びソフトウェアを外部に持ち出す場合には、あらかじめ情報セキュリティ管理者の許可を得なければならない。	(イ)　職員等は、異動等により業務を離れる場合には、知り得た情報を他に漏らしてはならない。
(ウ)　職員等は、外部で情報処理業務を行う場合には、あらかじめ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、支給以外の端末や機器を使用してはならない。ただし、正規の職員として認証する要素として、個人が所有する端末等を用いる必要がある場合はこの限りではない。	

（オ） 職員等は、支給以外の電磁的記録媒体等を用いる場合には、機密性２又は機密性３に該当する情報資産以外の情報資産のみとし、あらかじめ情報セキュリティ管理者の許可を得なければならない。 （カ） 職員等は、端末や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、適正な措置を講じなければならない。 （キ） 職員等は、端末等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システム管理者の許可なく変更してはならない。 （ク） 職員等は、業務以外の目的でホームページの閲覧等をしてはならない。 （ケ） 情報セキュリティ管理者は、電子的記録媒体やネットワークを介して情報資産を外部に複製・移動・転送・持ち出し等を行う場合は、安全対策など必要な措置を指示したうえで、必要最低限の許可を行うものとする。 （コ） 情報セキュリティ管理者は、端末、電磁的記録媒体、その他ハードウェア及びソフトウェアを外部に持ち出す場合は、安全対策など必要な措置を指示したうえで、必要最低限の許可を行うものとする。 （サ） 情報セキュリティ管理者は、外部で情報処理業務を行う場合には、安全対策など必要な措置を指示したうえで、必要最低限の許可を行うものとする。 （シ） 情報セキュリティ管理者は、情報資産の持ち出し及び持ち込み、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。 (ス)　情報セキュリティ管理者は、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等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。 (セ)　情報セキュリティ管理者は、非常勤及び臨時職員等の採用の際、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。 (ソ)　情報セキュリティ管理者は、職員等のホームページの閲覧等について、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、適正な使用について指導しなければならない。 (タ)　情報セキュリティ責任者は、職員等のホームページの閲覧等について、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指示し適正な措置を求めなければならない。 (チ)　ネットワーク管理者及び情報システム管理者は、職員等のホームページの閲覧等について、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指示し適正な措置を求めなければならない。	
（２）　教育・訓練 ア　ＣＩＳＯは、職員に対し情報セキュリティポリシーについて啓発に努めるとともに、職員を対象とした情報セキュリティポリシーに関する研修の機会を設けるものとする。 イ～オ　（略） （３）　事故、欠陥に対する報告	（２）　教育・訓練 ア　最高情報統括責任者は、職員に対し情報セキュリティポリシーについて啓発に努めるとともに、職員を対象とした情報セキュリティポリシーに関する研修の機会を設けるものとする。 イ～オ　（略） （３）　事故、欠陥に対する報告

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、速やかに情報セキュリティ管理者に報告しなければならない。 イ　職員等は、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。 ウ　情報セキュリティ管理者は、情報セキュリティインシデントの報告を受けた場合は、速やかに情報セキュリティ責任者・ＣＳＩＲＴ・関係するネットワーク管理者及び情報システム管理者へ報告しなければならない。 エ　情報セキュリティインシデントの報告を受けた情報セキュリティ責任者は、ＣＩＳＯに報告しなければならない。 オ　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。 カ　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。 キ　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管理者・ネットワーク管理者・情報システム管理者に対し、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。 ク　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の上、記録を	ア　職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤作動を発見した場合には、速やかに情報セキュリティ担当者に報告しなければならない。 イ　情報セキュリティ担当者は、職員等から情報セキュリティに関する事故、システム上の欠陥及び誤作動の報告を受けた時は、速やかにネットワーク管理者又は情報システム管理者に報告し、その指示に従い必要な措置を講じなければならない。 ウ　ネットワーク管理者及び情報システム管理者は、情報セキュリティ担当者から情報セキュリティに関する事故、システム上の欠陥及び誤作動の報告を受けた時は、直ちに必要な措置を指示するとともに、状況に応じ統括情報セキュリティ担当者、最高情報統括責任者に報告しなければならない。

保存し、ＣＩＳＯ・県及び国等に報告しなければならない。 ケ　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及びパスワードの取扱い ア～イ　（略） ウ　職員等は、パスワードを、他の者に知られないように管理しなければならない。 エ　職員等は、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。 オ　職員等は、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、数字や記号を織り交ぜる等)にしなければならない。 カ　職員等は、複数の情報システムを扱う場合は、同一のパスワードをシステム間で用いてはならない。 キ　職員等は、仮のパスワードや初期パスワードについて、最初のログイン時点で変更しなければならない。 ク　職員等は、パスワードが流出したおそれがある場合には、情報セキュリティインシデントとして取り扱い、速やかに対応しなければならない。 ケ　職員等は、自己が利用しているＩＤは、他人に利用させてはならない。 コ　職員等は、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。	（４）　パスワードの管理 ア～イ　（略）
（５）　ＩＣカード等の管理	（５）　ＩＣカード等の管理

ア　職員等は、ＩＣカード等の認証を用いた情報システムを利用する場合、当該ＩＣカード等を適切に管理しなければならない。	ア　ＩＣカード等の認証技術を用いた情報システムを利用する職員は、当該ＩＣカード等を適切に管理しなければならない。
イ　職員等は、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　職員は、ＩＣカード等を紛失した場合には、速やかに当該情報システムを管理する情報システム管理者に通報し指示を仰がなければならない。
ウ　職員等は、業務上必要がない場合、ＩＣカード等をカードリーダ等から取り外し、適切に保管しなければならない。	ウ　情報システム管理者は、ＩＣカード等の紛失にかかる通報を受けた場合は、当該ＩＣカード等によるアクセスを停止するよう措置しなければならない。
エ　職員等は、ＩＣカード等を紛失した場合には、情報セキュリティインシデントとして取り扱い、速やかに対応しなければならない。	
オ　ネットワーク管理者又は情報システム管理者は、ＩＣカード等の紛失にかかる報告を受けた場合は、当該ＩＣカード等によるアクセスを停止するよう措置しなければならない。	
カ　ネットワーク管理者又は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。	
６　技術的セキュリティ	６　技術的セキュリティ
（１）（略）	（１）（略）
ア　（略）	ア　（略）
(ア)～(ウ)　（略）	(ア)～(ウ)　（略）
イ～ウ　（略）	イ～ウ　（略）
エ　（略）	エ　（略）
(ア)～(イ)　（略）	(ア)～(イ)　（略）
オ　バックアップの取得	オ　バックアップの取得
(ア)　職員等は、情報資産の重要度に応じて定期的にバックアップを取り、安全な場	ネットワーク管理者及び情報システム管理者は、情報の重要度に応じて定期的にバッ

所へ保管しなければならない。 (イ)　ネットワーク管理者及び情報システム管理者は、管理権限により職員等が取得することができない情報資産について、定期的にバックアップを取り、安全な場所へ保管しなければならない。	クアップを取り、安全な場所へ保管しなければならない。
カ　電子メールの送受信等 (ア)　職員等は、電子メールの自動転送機能を用いて、業務上不必要な者へ職場の電子メールを転送してはならない。 (イ)　職員等は、チェーンメールや不審な電子メールを他者に転送してはならない。 (ウ)　職員等は、重要な情報に該当する添付ファイルのある電子メールを送信する必要がある場合には、事前に情報を所管する所属長の承認を受けなければならない。 (エ)　ネットワーク管理者及び情報システム管理者は、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。 (オ)　ネットワーク管理者及び情報システム管理者は、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しなければならない。 (カ)　ネットワーク管理者及び情報システム管理者は、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不可能にしなければならない。 (キ)　ネットワーク管理者及び情報システム管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監	カ　電子メールの送受信等 (ア)　職員は、電子メールの自動転送機能を用いて、業務上不必要な者へ職場の電子メールを転送してはならない。 (イ)　職員は、チェーンメールや不審な電子メールを他者に転送してはならない。 ウ)　職員は、重要な情報に該当する添付ファイルのある電子メールを送信する必要がある場合には、事前に情報を所管する所属長の承認を受けなければならない。

視等によりシステム上措置を講じなければならない。	
キ　(略)	キ　(略)
ク　(略)	ク　(略)
(ア)～(イ)　(略)	(ア)～(イ)　(略)
ケ　(略)	ケ　(略)
コ　(略)	コ　(略)
(ア)～(エ)　(略)	(ア)～(エ)　(略)
サ　(略)	サ　(略)
シ　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、情報セキュリティ責任者の許可を得なければならない。	
ス　ログの取得等 (ア)　ネットワーク管理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。 (イ)　ネットワーク管理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。 (ウ)　ネットワーク管理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。	
セ　ネットワークの接続制御、経路制御等 (ア)　ネットワーク管理者及び情報システム管理者は、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)　ネットワーク管理者及び情報システム管理者は、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。 ソ　外部の者が利用できるシステムの分離等 ネットワーク管理者及び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。 タ　外部ネットワークとの接続制限等 (ア)　ネットワーク管理者及び情報システム管理者は、外部のネットワークと接続しようとする場合には、情報セキュリティ責任者及び情報セキュリティ管理者の許可を得なければならない。 (イ)　ネットワーク管理者及び情報システム管理者は、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)　ネットワーク管理者及び情報システム管理者は、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。 (エ)　ネットワーク管理者及び情報システム管理者は、ウェブサーバ等をインターネ		

ットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

(オ)　ネットワーク管理者及び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、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。

チ　複合機のセキュリティ管理

(ア)　情報セキュリティ管理者は、複合機を調達する場合、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。

(イ)　情報セキュリティ管理者は、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。

(ウ)　情報セキュリティ管理者は、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)　ネットワーク管理者及び情報システム管理者は、複合機をネットワークに接続する場合、当該機器の情報セキュリティ管理者が策定したセキュリティ要件を確認し、不備がある場合は、その対応を求めることができる。

ツ　ＩｏＴ機器を含む特定用途機器のセキュリティ管理

(ア)　情報セキュリティ管理者は、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講じなければならない。 (イ)　ネットワーク管理者及び情報システム管理者は、複合機をネットワークに接続する場合、当該機器の情報セキュリティ管理者が策定したセキュリティ要件を確認し、不備がある場合は、その対応を求めることができる。 テ　無線ＬＡＮ及びネットワークの盗聴対策 (ア)　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の使用を義務付けなければならない。 (イ)　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。 ト　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、ＣＩＳＯが定めた電子署名、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)　ＣＩＳＯは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。 ナ　無許可ソフトウェアの導入等の禁止 (ア)　職員等は、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、ネットワーク管理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。なお、導入する際は、ネットワーク管理者又は情報システム管理者は、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。
ニ 機器構成の変更の制限
（ア） 職員等は、端末等に対し機器の改造及び増設・交換を行ってはならない。
（イ） 職員等は、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、情報セキュリティ責任者・情報システム管理者・ネットワーク管理者及び情報システム監理者の許可を得なければならない。
ヌ 業務外ネットワークへの接続の禁止
（ア） 職員等は、ネットワーク管理者及び情報システム管理者によって設定されたネットワークと異なるネットワークに端末等を接続してはならない
（イ） 職員等は、ネットワーク管理者及び情報システム管理者によって設定された接続方法と異なる方式で端末等を接続してはならない
（ウ） ネットワーク管理者又は情報システム管理者は、端末に搭載された機能等により、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。
ネ ネットワーク及び情報システムにおける機器の修理及び廃棄
（ア） 電磁的記録媒体の含まれる機器を、外部の業者に修理させる場合又は貸借期限

終了等により廃棄する場合は、電磁的記録媒体内の全ての情報を消去しなければならない。 （イ） 情報を消去しての機器の修理が難しい場合は、修理を委託する業者と守秘義務を明記した契約又は覚書を締結しなければならない。	
（２） 情報システムアクセス制御 ア 利用者登録 （ア） 情報システムの利用者の登録、変更、抹消等については、情報システムごとに定められた方法に従って行わなければならない。 （イ） 利用者登録、変更等は、ネットワーク管理者又は情報システム管理者に対する申請により行わなければならない。 イ 管理者権限 （ア） （略） （イ） 管理者権限は、必要最小限のネットワーク管理者又は情報システム管理者に付与し、厳重に管理しなければならない。 ウ～オ （略） カ （略） （ア）～（エ） （略） キ ＩＤ及びパスワード等の管理 （ア） ネットワーク管理者又は情報システム管理者は、情報セキュリティ管理者が指名し、情報セキュリティ責任者が認めた者でなければならない。 （イ） ネットワーク管理者又は情報システム管理者は、特権が付与された管理者としてのＩＤと、一般的な権限が付与された職員としてのＩＤを区別し、特権が付与された管理者ＩＤは必要最低限の使用にとどめなければならない。 （ウ） ネットワーク管理者又は情報システ	（２） 情報システムアクセス制御 ア 利用者登録 （ア） 情報システムの利用者の登録、変更、抹消等については、各情報システムごとに定められた方法に従って行わなければならない。 （イ） 利用者登録、変更等は、情報システム管理者に対する申請により行わなければならない。 イ 管理者権限 （ア） （略） （イ） 管理者権限は、必要最小限の者に与え、厳重に管理しなければならない。 ウ～オ （略） カ （略） （ア）～（エ） （略） キ パスワード等の管理 （ア） 情報システム管理者は、情報システムで使用するＩＤ、パスワードを厳重に管理しなければならない。 （イ） ネットワーク管理者は、ネットワーク並びにネットワーク上で利用する各種サービスのＩＤ、パスワードを厳重に管理しなければならない。

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、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。 (エ)　ネットワーク管理者又は情報システム管理者は、使用するＩＤ、パスワード等を厳重に管理しなければならない。 (オ)　ネットワーク管理者又は情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。 (カ)　ネットワーク管理者又は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、点検しなければならない。 (キ)　職員等は、業務上必要がなくなった場合は、ネットワーク管理者又は情報システム管理者に通知しなければならない。 (ク)　ネットワーク管理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。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。 (ケ)　ネットワーク管理者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。 (コ)　ネットワーク管理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。 ク　自動識別の設定 ネットワーク管理者又は情報システム管理		

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。	
（3） 情報システムの開発・導入・保守 ア　ネットワーク及び情報システムの調達	（3） 情報システムの開発・導入・保守 ア　ネットワーク及び情報システムの開発・導入 ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムを新規に開発・導入する場合及び大規模な変更等を行う場合は、事前に推進本部で審議したうえで実施しなければならない。 この場合、ネットワーク管理者及び情報システム管理者は、ネットワーク構成図、情報システムの仕様書等を整備しなければならない。
（ア） ネットワーク管理者又は情報システム管理者は、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） ネットワーク管理者又は情報システム管理者は、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　ネットワーク及び情報システムの開発	イ　ネットワーク及び情報システムの変更管理 ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムを追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。
（ア） ネットワーク管理者又は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。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)　ネットワーク管理者又は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。 (ウ)　ネットワーク管理者又は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らない。 (エ)　ネットワーク管理者又は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なければならない。 (オ)　ネットワーク管理者又は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。	
ウ　ネットワーク及び情報システムの導入 (ア)　ネットワーク管理者又は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)　ネットワーク管理者又は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)　ネットワーク管理者又は情報システム管理者は、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。	ウ　ソフトウェアの保守及び更新 (ア)　情報システム管理者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切な保守が行われるようにし、その不具合については、速やかに修正等の対応を行わなければならない。 (イ)　情報を消去しての機器の修理が難しい場合は、修理を委託する業者と守秘義務を明記した契約又は覚書を締結しなければならない。

（エ） ネットワーク管理者又は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。 （オ） ネットワーク管理者又は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。 （カ） ネットワーク管理者又は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。 （キ） ネットワーク管理者又は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を、テストデータに使用してはならない。 （ク） ネットワーク管理者又は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。	
エ ネットワーク及び情報システムの開発・保守に関連する資料等の整備・保管 （ア） ネットワーク管理者又は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正に整備・保管しなければならない。 （イ） ネットワーク管理者又は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。 （ウ） ネットワーク管理者又は情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならな	エ 機器の修理及び廃棄 （ア） 記録媒体の含まれる機器を、外部の業者に修理させる場合又は貸借期限終了等により廃棄する場合は、可能な範囲でバックアップを取り、記録媒体内の全ての情報を消去しなければならない。 （イ） 情報を消去しての機器の修理が難しい場合は、修理を委託する業者と守秘義務を明記した契約又は覚書を締結しなければならない。

い。
オ　ネットワーク及び情報システムにおける入出力データの正確性の確保
（ア）　ネットワーク管理者又は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。
（イ）　ネットワーク管理者又は情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。
（ウ）　ネットワーク管理者又は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。
カ　ネットワーク及び情報システムの変更管理
（ア）　ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムを追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。
（イ）　ネットワーク管理者又は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。
キ　ネットワーク及び情報システムのソフトウェアの保守及び更新
（ア）　ネットワーク管理者又は情報システム管理者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切

な保守が行われるようにし、その不具合については、速やかに修正等の対応を行わなければならない。 (イ)　ネットワーク管理者又は情報システム管理者は、情報システムの更新等については、計画的に実施しなければならない。	
(4)　コンピュータウイルス対策 ア　ネットワーク管理者及び情報システム管理者は、コンピュータウィルス対策として、次の事項を実施しなければならない。 (ア)～(オ)　(略) イ　職員等は、コンピュータウィルス対策として、次の事項を遵守しなければならない。 (ア)～(オ)　(略)	(4)　コンピュータウイルス対策 ア　ネットワーク管理者及び情報システム管理者は、次の事項を実施しなければならない。 (ア)～(オ)　(略) イ　職員等は、次の事項を遵守しなければならない。 (ア)～(オ)　(略)
(5)　不正プログラム対策 ア　ネットワーク管理者及び情報システム管理者は、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。 (ア)　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。 (イ)　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。 (ウ)　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。	(5)　不正アクセス対策 ア　ネットワーク管理者及び情報システム管理者は、セキュリティホール等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録・保存しなければならない。

（エ） 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。 （オ） 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。 （カ） 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。 （キ） 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。 （ク） 情報システム管理者は、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。 （ケ） 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。 （コ） 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。 （サ） 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。 (シ)　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。	
イ　職員等は、不正プログラム対策として、次の事項を遵守しなければならない。	イ　情報システム管理者は、情報システムに攻撃を受けていることが明らかな場合には、システムの停止を含め必要な措置を講じなければならない。
(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。 (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)　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。 (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、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてＬＡＮケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。	
	ウ　外部ネットワークより不正アクセスがあった場合には記録の保全に努めるとともに、適切な措置を講じなければならない。 エ　職員により本市ネットワーク、外部ネットワーク及び情報システムに対して不正なアクセスがあった場合は、当該職員が所属する課等の情報セキュリティ担当者に通知し、適切な処置を求めなければならない。 オ　ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムに不正な侵入や利用があった場合に探知等できるよう、適切な対策に努めなければならない。
（６）　不正アクセス対策 ア　ネットワーク管理者及び情報システム管理者は、セキュリティホール等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録・保存しなければならない。 イ　ネットワーク管理者及び情報システム管理者は、情報システムに攻撃を受けていることが明らかな場合には、システムの停止を含め必要な措置を講じなければならない。 ウ　ネットワーク管理者及び情報システム管理者は、外部ネットワークより不正アクセスがあった場合には、記録の保全に努め	

るとともに、適切な措置を講じなければならない。 エ　ネットワーク管理者及び情報システム管理者は、職員等により本市ネットワーク、外部ネットワーク及び情報システムに対して不正なアクセスがあった場合は、当該職員が所属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。 オ　ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムに不正な侵入や利用があった場合に探知等できるよう、適切な対策に努めなければならない。 カ　ネットワーク管理者及び情報システム管理者は、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。 (ア)　使用されていないポートを閉鎖しなければならない。 (イ)　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。 (ウ)　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、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。 (エ)　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。 (オ)　情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。 キ　ＣＩＳＯ及び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、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。 ク　ＣＩＳＯ及び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。 ケ　ネットワーク管理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。 コ　ネットワーク管理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、適正な処置を求めなければならない。 サ　ネットワーク管理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。 シ　ネットワーク管理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） セキュリティ情報の収集 ア 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、石巻市の全てのネットワーク及び情報システムについてソフトウェアにパッチを当てる等、情報システム管理者に命じ、情報セキュリティ対策上必要な措置を講じなければならない。 イ 情報セキュリティ責任者及び情報システム管理者は、これらの情報を定期的に取りまとめ、情報セキュリティポリシーの改定につながる情報については推進本部に報告しなければならない。 ウ 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情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。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。 エ 不正プログラム等のセキュリティ情報の収集・周知 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。 オ 情報セキュリティに関する情報の収集及び共有 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、セキュリティ侵害を未然に防止するための対策	（6） セキュリティ情報の収集 ア 最高情報統括責任者は、情報セキュリティに関する情報を収集し、石巻市の全てのネットワーク及び情報システムについてソフトウェアにパッチを当てる等、情報システム管理者に命じ、情報セキュリティ対策上必要な措置を講じなければならない。 イ 最高情報統括責任者は、これらの情報を定期的に取りまとめ、情報セキュリティポリシーの改定につながる情報については推進本部に報告しなければならない。

を速やかに講じなければならない。 (8)情報システムの調達 ア　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　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。	
7　運用 (1)　ネットワーク及び情報システムの監視 ア　ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムの運用にあたっては、常にネットワーク及び情報システムを監視するとともに情報セキュリティ障害に対して細心の注意を払わなければならない。 イ　ネットワーク管理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。 ウ　ネットワーク管理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。 エ　ネットワーク管理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。 オ　暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化す	7　運用 (1)　ネットワーク及び情報システムの監視 ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムの運用にあたっては、常にネットワーク及び情報システムを監視するとともに情報セキュリティ障害に対して細心の注意を払わなければならない。

る機能を導入しなければならない。	
（２） 情報セキュリティポリシーの遵守状況の確認	（２） 情報セキュリティポリシーの遵守状況の確認
ア 情報セキュリティ責任者及び情報セキュリティ担当者は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じていないかについて確認を行い、問題が発生していた場合には、速やかにネットワーク管理者又は情報システム管理者に報告しなければならない。	ア 統括情報セキュリティ担当者及び情報セキュリティ担当者は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じていないかについて確認を行わなければならない。 問題が発生していた場合には、速やかに最高情報統括責任者、ネットワーク管理者あるいは情報システム管理者に報告しなければならない。
イ （略）	イ （略）
ウ ネットワーク管理者及び情報システム管理者は、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端末及び電磁的記録媒体等のデータやログ、電子メール等の送受信記録等の利用状況を調査することができる。	ウ 最高情報統括責任者は速やかに発生した問題に適切に対処しなければならない。
エ 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。	
オ 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ＣＩＳＯ又は情報セキュリティ責任者が判断した場合において、職員等は適正に対処しなければならない。	
（３） セキュリティ障害時の対応等	（３） 運用管理における留意点
ア セキュリティ障害が発生した場合は、緊急時対応計画に従い速やかに対応しなければならない。	ア ネットワーク管理者又はシステム管理者は、管理者権限を有する職員等を情報セキュリティ実施手順に定めなければならない。 ただし、法令で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法

イ　緊急時対応計画には、以下のものを明記しなければならない。 （ア）　連絡体制 （イ）　障害等に対する対応 （ウ）　再発防止に関する措置 ウ　ネットワーク管理者及び情報システム管理者は、故意の不正アクセス又は不正操作によりネットワーク及び情報システムに障害を及ぼすことが明らかな場合には、ネットワーク及び情報システムの停止を含む必要な措置を講じなければならない。 エ　ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。 オ　ネットワーク管理者及び情報システム管理者は、セキュリティ障害が発生した場合、次の項目について調査をしなければならない。 カ　ネットワーク管理者及び情報システム管理者は、調査した内容は速やかに情報セキュリティ担当者へ報告しなければならない。ただし、障害の程度が軽微なものについては報告を要しないものとする。 キ　情報セキュリティ担当者は、セキュリティ障害により重大な被害が想定されるときは、ネットワーク管理者又は情報システム管理者に事案の詳細な報告を求めるとともに、情報セキュリティ責任者に報告しなければならない。この場合、障害が外部に対し重大な影響を及ぼす恐れがあると認め	令に定められた手続に従う。 イ　情報セキュリティ担当者は、職員等が常に情報セキュリティポリシーおよび実施手順を参照できるよう配慮しなければならない。

られる場合には、速やかにＣＩＳＯに必要な指示を仰がなければならない。 ク　ネットワーク管理者及び情報システム管理者は、速やかに、再発防止の措置を講じるとともに、その結果をＣＩＳＯに報告しなければならない。 ケ　情報セキュリティ責任者及び情報セキュリティ担当者は、セキュリティ障害の原因が人的セキュリティによる場合は、職員に対して再発を防止するため必要な措置を講じなければならない コ　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）　セキュリティ侵害時の対応等 ア　情報漏洩など情報資産に対するセキュリティ侵害が発生した場合は、緊急時対応計画に従い速やかに対応しなければならない。 イ　緊急時対応計画には、以下のものを明記しなければならない。 (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　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）　セキュリティ障害時の対応 ア　セキュリティ障害が発生した場合は、情報セキュリティ実施手順において定める緊急時対応計画に従い速やかに対応しなければならない。 イ　緊急時対応計画には、以下のものを明記しなければならない。 （ア）　連絡体制 （イ）　障害等に対する対応 （ウ）　再発防止に関する措置 ウ　障害拡大の防止措置 （ア）　ネットワーク管理者及び情報システム管理者は、故意の不正アクセス又は不正操作によりネットワーク及び情報システムに障害を及ぼすことが明らかな場合には、ネットワーク及び情報システムの停止を含む必要な措置を講じなければならない。

	（イ） ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。 エ　障害の調査 （ア） ネットワーク管理者及び情報システム管理者は、セキュリティ障害が発生した場合、次の項目について調査をしなければならない。 ａ　障害の内容 ｂ　障害が発生した原因 オ　調査した内容は速やかに統括情報セキュリティ担当者へ報告しなければならない。ただし、障害の程度が軽微なものについては報告を要しないものとする カ　障害への対応 統括情報セキュリティ担当者は、セキュリティ障害により重大な被害が想定されるときは、ネットワーク管理者又は情報システム管理者に事案の詳細な報告を求めるとともに、最高情報統括責任者に報告しなければならない。 この場合、障害が外部に対し重大な影響を及ぼす恐れがあると認められる場合には、速やかに最高情報統括責任者に必要な指示を仰がなければならない。 キ　再発防止の措置 （ア） ネットワーク管理者及び情報システム管理者は速やかに、再発防止の措置を講じなければならない。 （イ） 統括情報セキュリティ担当者は、必要な再発防止の措置を講じるとともに、その結果を最高情報統括責任者に報告しなければならない。

	（ウ） 統括情報セキュリティ担当者及び情報セキュリティ担当者は、セキュリティ障害の原因が人的セキュリティによる場合は、職員に対して再発を防止するため必要な措置を講じなければならない
（５） 例外措置 ア 情報セキュリティ管理者・ネットワーク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。	（５） 外部委託による運用契約 ア 運用を外部委託する場合は、委託に関する責任を有する部署を明確にするとともに、委託事業者に対し必要なセキュリティ要件を記載した契約書による契約を締結しなければならない。
イ 情報セキュリティ管理者・ネットワーク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。 ウ 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。	イ 委託に関する責任を有する部署は、委託先において必要なセキュリティ対策が確保されていることを確認し、その内容をネットワーク管理者に報告するとともに、その重要度に応じて最高情報統括責任者に報告しなければならない。
８ 業務委託と外部サービスの利用	８ 法令等の遵守 職員等は、使用する情報資産について、次の法令等を遵守しなければならない。 また、マナーと倫理をもって情報システムを利用しなければならない。
（１） 業務委託 ア 委託事業者の選定基準 (ア) 情報セキュリティ担当者は、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。	（１） 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)

（イ） 情報セキュリティ担当者は、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。 イ 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情報セキュリティ実施手順の遵守 （イ） 委託事業者の責任者、委託内容、作業者の所属、作業場所の特定 （ウ） 提供されるサービスレベルの保証 （エ） 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 （オ） 委託事業者の従業員に対する教育の実施 （カ） 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 （キ） 業務上知り得た情報の守秘義務 （ク） 再委託に関する制限事項の遵守 （ケ） 委託業務終了時の情報資産の返還、廃棄等 （コ） 委託業務の定期報告及び緊急時報告義務 （サ） 市による監査、検査 （シ） 市による情報セキュリティインシデント発生時の公表 （ス） 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 ウ 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、契約に基づく措置を実施しなければならない。 （２） 機密性２以上の情報を取り扱う外部サービスの利用 ア　情報セキュリティ管理者は、機密性２以上の情報を取り扱う場合、以下を含む外部サービスの利用に関する規定を整備すること。 (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申請の許可権限者と利用手続 (エ)　外部サービス管理者の指名と外部サービスの利用状況の管理 イ　外部サービスの選定 (ア)　情報セキュリティ管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、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すること。 (イ)　情報セキュリティ管理者は、次の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こと。 a 外部サービス提供者が外部サービスの利用により知りえた情報の目的外利用の禁止 b 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及び資格や研修実績などの専門性・実績及び国籍に関する情報開示 c 外部サービス提供者による外部サービスの施設の所在地やリージョンの指定 d 外部サービス提供者の情報セキュリティ対策の実施内容及び管理体制の情報開示	（２） 著作権法(昭和45年法律第48号)

e 外部サービス提供者や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の情報開示 f 外部サービス提供者の情報セキュリティ監査の受入れ g 外部サービス提供者によるサービスレベルの保証 h 外部サービス提供者の情報セキュリティインシデントへの対処方法に関する情報開示 i 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手法に関する情報開示 j 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 k 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 （ウ） 情報セキュリティ管理者は、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ること。 （エ） 情報セキュリティ管理者は、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、外部サービス提供者に対し必要な情報を開示させ、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、再委託の承認の可否を判断すること。 （オ） 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、外部サービスを選定すること。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こと。 (カ)　情報セキュリティ管理者は、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ること。 (キ)　情報セキュリティ管理者は、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すること。 ウ　外部サービスの利用に係る調達・契約 (ア)　情報セキュリティ管理者は、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ること。 (イ)　情報セキュリティ管理者は、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確認し、調達仕様の内容を契約に含めること。 エ　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)　情報セキュリティ管理者は、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すること。		

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 (イ) 情報セキュリティ管理者は、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・記録すること。 オ 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) 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、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すること。 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 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すること。 j 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・記録すること。 カ 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)　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、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すること。 a 外部サービスの利用終了時における対策	
（３）　ソーシャルメディアサービスの利用	（３）　行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律(昭和63年法律第95号)
ア　情報セキュリティ管理者は、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。 イ　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、本市のホームページ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。 ウ　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電子的記録媒体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。 エ　機密性２以上の情報はソーシャルメディアサービスで発信してはならない。 オ　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。 カ　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。	
	（４）　石巻市個人情報保護条例
９　法令等の遵守 （１）　職員等は、使用する情報資産につい	

て、次の法令等を遵守しなければならない。また、マナーと倫理をもって情報システムを利用しなければならない。

ア　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）

イ　著作権法（昭和45年法律第48号）

ウ　地方公務員法（昭和25年法律第261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）

キ　石巻市個人情報の保護に関する法律施行条例（令和４年12月16日条例第48号）

（２）　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。

（３）　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　情報セキュリティ責任者が違反を確認した場合は、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、適正な措置を求めなければならない。

イ　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、適正な措置を求めなければならない。

ウ　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、情報セキュリティ

責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨をＣＩＳＯ及び当該職員等が所属する課室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。 10　評価・見直し等 （1）　自己点検 ア　情報セキュリティ責任者及び情報セキュリティ担当者は、当該部署の情報セキュリティが確保されていることを確認するため自己点検を行い、必要に応じて改善措置を講じなければならない。 イ　ネットワーク管理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自己点検を行い、必要に応じて改善措置を講じなければならない。 （2）　監査 ア　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、必要に応じ監査を実施しなければならない。 イ　情報セキュリティ監査統括責任者は、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。 ウ　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。 エ　情報セキュリティ監査統括責任者は、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対して、必要に応じて監査を実施しなければならない。 オ　情報セキュリティ監査統括責任者は、ネットワーク管理者及び情報システム管理		

者に対して、必要に応じて監査を実施しなければならない。 カ　情報セキュリティ監査統括責任者は、委託事業者に対して、必要に応じ監査を行わなければならない。 キ　情報セキュリティ監査統括責任者は、監査の結果をＣＩＳＯに報告しなければならない。 ク　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正に保管しなければならない。 ケ　ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ責任者及び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。 コ　ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管していない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対して、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。 サ　ＣＩＳＯは、監査結果を踏まえ、庁内で横断的に改善が必要な事項については、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対し、当該事項への対処を指示しなければならない。 シ　ＣＩＳＯは、監査結果を踏まえ、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の更新 ＣＩＳＯは、情報セキュリティポリシーの評価及び見直しが必要となる事象が発生した場合には、推進本部に諮り必要な見直し	（３）　情報セキュリティポリシーの更新 最高情報統括責任者は、評価及び見直しが必要となる事象が発生した場合には、推進本部に諮り必要な見直しを行い、適切な情

を行い、適切な維持及び運用に努めなければならない。	報セキュリティポリシーの維持及び運用に努めなければならない。