飯塚市情報セキュリティ実施手順

平成23年4月1日　　策　定
平成23年12月1日　一部改定
令和2年4月1日　一部改定
令和5年4月1日　一部改定
令和7年2月7日　一部改定

目次

1　目的 2
2　定義及び適用範囲 2
3　情報資産の分類と管理 2
4　情報資産の運搬 2
5　情報資産の廃棄 2
6　情報資産の暗号化 3
7　職員の遵守事項 3
8　ID の取扱い 4
9　バックアップ 4
10　業務委託 4
11　派遣労働者、委託事業者 4
12　指定管理 5
13　情報セキュリティインシデント 6
14　監査 7
14.1　内部監査 7
14.2　外部監査 9
15　自己点検 9

1　目的

本実施手順は、「飯塚市情報セキュリティポリシー」を実施するにあたり、必要な詳細内容を定めることを目的とする。

2　定義及び適用範囲

「飯塚市情報セキュリティ基本方針」及び「飯塚市情報セキュリティ対策基準」に定めるものに準拠する。また、本実施手順の見直しについても、情報セキュリティポリシーと連携し適宜実施するものとする。

3　情報資産の分類と管理

情報資産の管理単位は、次に掲げるところによる。

①紙情報（文書）については、綴り又はファイル毎に区分け、識別し管理すること。

②電子情報（データ）を記録した機器や媒体は、次の単位毎に区分け、識別し管理すること。

ア　PC（端末機等）：1台毎

イ　情報システム：システム毎

ウ　共有フォルダ：フォルダ毎

エ　電子記録媒体：フロッピーディスク、USBメモリ、MO、CD-R（含 DVD）等の種類毎

③管理単位の中で、セキュリティレベルの異なる情報及びデータが混在する場合は、当該情報及びデータの中で、最も高いセキュリティレベルに設定すること（例:自治体機密性３Ｂ、２が混在する場合は自治体機密性３Ｂとする）。

④外部組織が作成し、本市が受け入れた情報・データについても、適切な単位に区分けのうえ、セキュリティレベルを設定すること。

4　情報資産の運搬

①情報資産の運搬とは以下のものをいう。

ア　本市と本市以外の組織（企業や自治体）

イ　本市内の異なる庁舎間（アウトソーシングセンタや出先機関を含む）

②上記アの場合、郵送等を行う場合は、紛失等の万が一に備え、セキュリティが確保できる方法により行う。

③上記イの場合、庁舎間が遠い場合は、極力上記②の方法による運搬を行う。近い場合には、書類や電子媒体の紛失を避けるため、必ずダンボール等の箱や封筒に入れることとし、職員等の同行により行うこと。

④データを運搬する場合の暗号化については、6項に従う。

5　情報資産の廃棄

①紙（文書等）を廃棄する場合は、シュレッダー等により判読できない状態としたうえで廃棄するか、職員により直接焼却施設に運搬すること。

②電子媒体を廃棄する場合は、記録される情報の機密性に応じて、物理的な破壊、又は電磁的な破壊、若しくはその両方を行う。

物理的な破壊：CD等の磁気記録媒体は破砕、メモリやHDD等の記憶媒体は3箇所以上の穴あけを行う。

電磁的な破壊：HDD等に強磁界を印可又はデータ消去ソフトウェア等を使用することでＯＳ等からアクセス可能な全てのストレージ領域のデータを消去する。

③サーバ及び端末機の廃棄又は返却については、次に掲げるところによる。
ア　リース等の契約満了等による契約相手方への返却である場合は、契約の相手方に確認をした上で、上記②の方法、又はリース先によるデータ消去契約に基づく消去を依頼する。この場合、必ず消去証明書を受領する。
イ　買い取りや譲渡による場合は、原則上記②の方法をとるが、難しい場合は、上記③アの方法により、設定データの消去を行う。
④紙文書又は電子媒体等情報資産の廃棄処分を外部業者に委託する場合は、受託業者から「廃棄証明書」を発行させ、保管すること。

6　情報資産の暗号化

暗号化は以下の方法のいずれかによるものとする。
①市販されている暗号化ソフトでぜい弱性等の問題点が発生していないもの。
②問題点等が報告されていないフリーソフト（但し、極力使用しない）。
③暗号鍵を独自に設ける場合、情報セキュリティ管理者は、ファイルの暗号化について、暗号化の鍵を決定し、適正に管理する。なお、搬送先及び電子メール送信先に対する鍵の通知は、郵送、電話、インターネットを経由しない電子メールのいずれかによるものとし、情報資産搬送時に同梱してはならない。
④通信の暗号化を行う場合、情報セキュリティ管理者は、ウェブサーバ及びウェブブラウザ間の通信の場合は、TLS を利用し、必要となるサーバ証明は、第三者認証局又は地方公共団体における組織認証基盤（LGPKI）を利用して発行されたものとする。
⑤無線 LAN を利用する場合、原則、最新の暗号化技術を適用すること。

7　職員の遵守事項

（１）安全管理措置
①外部で処理する場合、持ち出す情報は、必要最低限の範囲とする。
②情報セキュリティ対策基準５．２、５．３及び５．４に準拠した環境を整えること。
③作業者に対し、定期的な教育及び指導を行うこと。
④定期的な監査、点検等を行うこと。
但し、緊急時等により上記安全管理措置②に示す環境整備が難しい場合は、情報の閲覧等が容易に出来ないよう以下の点に注意して行う。
ア　情報が第三者に閲覧されることが無いようにパソコン等の配置に注意する。
イ　パソコンやデータ等は常に携行する。
ウ　データの存在を公表しない。
エ　外部とのネットワークの接続を行わない。
オ　情報セキュリティ管理者の許可を得る。

（２）机上の端末等の管理
①他人の ID やパスワードを使用して、PC（端末機）及び情報システムの操作をしてはならない。
②許可なく、端末等を移動させてはならない（盗難のための対応や異動等による場合を除く）。
③机上の持ち運び可能媒体（FD や USB メモリ等）は、5 分以上離席する場合には、持ち出されないように引出し等に一時保管しなければならない。
④端末は、5 分以上離席する場合には、パスワード付きスクリーンセーバー等の機能で端末操作ができないよう設定しなければならない。
⑤PC キーボード操作エリアには、茶碗、湯飲み等、蓋のない容器に入れた飲料を置いてはならない。

8　IDの取扱い

IDの取扱いを以下に従い実施すること。

①設定完了後職員等はIDの設定（登録・変更・削除等）が必要になった場合、各システムの情報システム管理者へ申請を行う。但し、定期人事異動によりIDの設定が自明の場合は、総務部からの異動リスト等を持って情報システム管理者が一括設定できる。派遣労働者、委託事業者については、所属先の情報セキュリティ管理者が行う。申請書は情報システム管理者にて保管する。

②設定完了後、情報システム管理者は、職員等、派遣労働者、委託事業者に対し、設定内容をメール若しくは紙で通知する。設定時は個人の責任が明確になるよう、原則利用者に対し個人専用のIDを設定する。やむを得ず共有IDが必要な場合には、責任の所在を明確にするために共有IDの管理者を定めなければならない。

③情報システム管理者は、定期人事（通常4月を想定）後の3ヶ月以内に、IDの設定状況を確認し、不要なID及びアクセス権を利用停止もしくは削除する。削除に当たっては、間違い防止の観点から、情報セキュリティ管理者及び人事部と相互に連絡を取り合い行う。

④システム管理者のID（root、Administrator 等の特権ID）付与は必要最小限とする。

⑤特権IDについては、情報システム管理者が厳重に管理する。

9　バックアップ

①職員等及び情報システム事業者は、セキュリティ事故によるPCやFD等のファイル消失を防ぐために、必要なファイルをファイルサーバ等に保存しなければならない。

②情報システム管理者は、災害や重大障害に備えるために、プログラムやデータのバックアップを次に掲げる事項のとおり実施しなければならない。

・サーバは、ディスク内の冗長化対策とは別に、他のディスクや媒体にバックアップを取ること

・プログラム及び自治体機密性３に相当する情報・データをバックアップした媒体は、サーバと別区画に保管すること

・情報管理担当課で管理するファイルサーバは、毎日（5世代）を標準としてバックアップを取ること

③各課で管理するシステムにおける保有するデータ等のバックアップは、毎週（2世代）を標準として定めなければならない。

10　業務委託

①システムの運用管理業務を委託事業者に委託する場合は、委託事業者の作業内容、報告義務、市資産の預託管理及び情報セキュリティ管理責任の範囲を明確にして、契約文書に明記しなければならない。

②委託事業者は、庁舎内で作業に従事する者に、本人識別のために「職員証」（社員証等でも可）を携行させなければならない。

③本市資産管理については、次に掲げるところによる。

・委託事業者は、業務の必要から市の資産を庁外に持ち出す場合は、契約文書に基づき、事前に承認願いを提出し、情報セキュリティ管理者の承認を受けなければならない。

・委託事業者は、返却時又は消去時においても、契約に基づき持ち出し時と同様の手続きを行い、情報セキュリティ管理者の返却又は消去の確認を受けなければならない。

11　派遣労働者、委託事業者

派遣労働者、委託事業者にかかる契約書等に明記すべき事項については、飯塚市長が管理する個人情報の保護に関する規則（平成 18 年飯塚市規則第 15 号）第 8 条に規定した以下のとおりとする。

①個人情報の秘密保持に関する事項
②再委託の禁止又は制限に関する事項
③個人情報の指示目的以外の利用及び第三者への提供禁止に関する事項
④個人情報の複写及び複製の禁止又は制限に関する事項
⑤事故発生時における報告義務に関する事項
⑥個人情報の管理状況についての立入調査に関する事項
⑦その他個人情報の保護に関し必要な事項
⑧前各号に掲げる事項に違反した場合における契約解除等の措置及び損害賠償に関する事項

12 指定管理

指定管理にかかる契約等の必須事項については以下のとおりとする。

①情報資産の秘密保持に関する事項
②情報資産を取り扱う者の監督に関する事項
③作業場所の制限に関する事項
④情報資産の指示目的外の利用及び第三者への提供の制限に関する事項
⑤情報資産の安全確保に関する事項
⑥情報資産の複写及び複製の制限に関する事項
⑦再委託の制限に関する事項
⑧業務終了時の情報資産の返還、廃棄等に関する事項
⑨情報資産の取り扱いの状況についての報告、監査、点検に関する事項
⑩事故並びに欠陥及び誤作動を発見したときの報告義務に関する事項
⑪事故発生時等の市による公表に関する事項
⑫前記各事項に掲げる事項に違反した場合における契約解除等の措置に関する事項
⑬その他、情報資産の保護に関し必要な事項

13 情報セキュリティインシデント

事故、欠陥等については、レベル分けを行いレベルにあった対応を実施する。

	対応	指標	内容
レベル1	対応不要	基準	・一時的にリスクとして想定した事象が発生した状態で、実害のほとんど無いもの、又は計画されたもの。 ・システムもしくはサービスのセキュリティの弱点、疑いがあるもの。
		具体例	・ビル内各種設備（ｴﾚﾍﾞｰﾀ、ｺﾋﾟｰ機等）の点検等による停止 ・収納庫等の破損等、ﾒﾝﾃﾅﾝｽ等による計画的なNW、サービス停止 ・クライアント端末への定められた管理策の未実施（ﾊﾟｽﾜｰﾄﾞ設定等） ・限られた範囲でのデータの紛失・誤った変更（復旧可能） ・長時間離席による情報放置、職員証不携帯、共有スペースでの業務に関する会話 ・上記以外に他の疑問がある時
		対応	・必要に応じ注意喚起等（課長等）、次回の監査等での確認。
レベル2	対応	基準	・復旧に特別な対応を必要としないもの。 ・情報漏えいや紛失等がシステム機能や運用ルールで未然に防げたもの。
		具体例	・ﾌﾛｱ電子キー故障、来訪者のﾌﾛｱ内での不審行為、不審物の発見。 ・NW・ﾊｰﾄﾞ障害（一部のサーバダウン等）で概ね2時間以内に回復。 ・システムにより防御された不正アクセスや、コンピュータウイルス。 ・機器（ｸﾗｲｱﾝﾄ、NW機器等）の故障（代替機等により対応可能）。 ・当組織内システムの軽微なバグ・ソフトウェアの誤動作。 ・業務用機器の紛失、職員証の盗難・紛失、外部から連絡を受けた場合
		対応	・「情報セキュリティインシデント記録表」の起票、手順に基づく対応
レベル3	対応	基準	・情報の漏洩・紛失等の事象が実際に発生した場合。 ・長期間のシステム停止等可用性に重大な影響が発生した場合。 ・外部からの攻撃により被害が発生した場合。
		具体例	・不審者の侵入、業務に支障をきたすレベルの物理的・環境的障害。 ・回復の見込のたたないNW障害、外部からの攻撃によるｻｰﾊﾞ等停止。 ・サーバ、クライアントのウィルス感染。 ・情報の大量喪失・改ざん・漏えい（故意・過失及び復旧の可否を問わず） ・法令違反
		対応	・「情報セキュリティインシデント記録表」の起票、手順に基づく対応、侵害時の対応による対応 ・緊急事態の情報セキュリティ委員会の開催

①レベル２及び３の事件・事故及びその発生の可能性を発見した者及び市民等外部からの通報を受けた者は直ちに、実態把握と応急処置を行い、情報セキュリティ管理者に報告する。報告後、事故記録表を作成する。
②連絡を受けた情報セキュリティ管理者は、直ちに実態を把握し、情報セキュリティ責任者及び統括情報セキュリティ責任者に報告する。
③統括情報セキュリティ責任者は、緊急的対応が必要と判断した場合直ちにCISOに報告し必要な処置をとる。また、協議が必要な場合、情報セキュリティ委員会を招集し必要な処置をとる。
④統括情報セキュリティ責任者は、委員会の決定を元に、必要な対応（監査・是正措置等）を情報セキュリティ管理者へ指示する。ただし、個人情報が漏えい、滅失又はき損をした場合は、本人への影響などのおそれを考慮しその影響を最小限にするために、本人への通知も検

討する。（正式な謝罪等は、⑦で実施する。ここでは、被害の拡大防止のための一報となる）
⑤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記録表」の記載項目に基づき具体的対応策を検討する。なお、個人情報が漏えい、滅失又はき損をした場合、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限にするための対応策を検討し、統括情報セキュリティ責任者へ報告する。
⑥統括情報セキュリティ責任者は、委員会の決定及び報告された情報セキュリティインシデント記録表の内容を元に二次被害の防止、類似事案の発生回避などの観点から、公開可能と判断する事実関係、発生原因及び対応策を、遅滞なく公表することを情報セキュリティ管理者に指示する。また、事実関係、発生原因及び対応策の外部関係機関への報告、マスコミ等との対応については、広報担当と協議して実施する。
⑦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の原因、本人への影響度、二次被害の有無等が明確になった時点で、情報セキュリティ管理者へ謝罪の指示を行う。謝罪は以下の流れで行う。
・謝罪は、電話、文書、訪問のいずれかの方法で行う。
・内容に、経緯、事故の原因、考えられる影響、二次被害の有無を含める。
・今後の対応について、明確にする。
・御意見を伺い、「情報セキュリティインシデント記録表」に記載する。
⑧統括情報セキュリティ責任者は、再発防止策を検討し実施する（対策の教育を含む）。

14 監査

14.1 内部監査

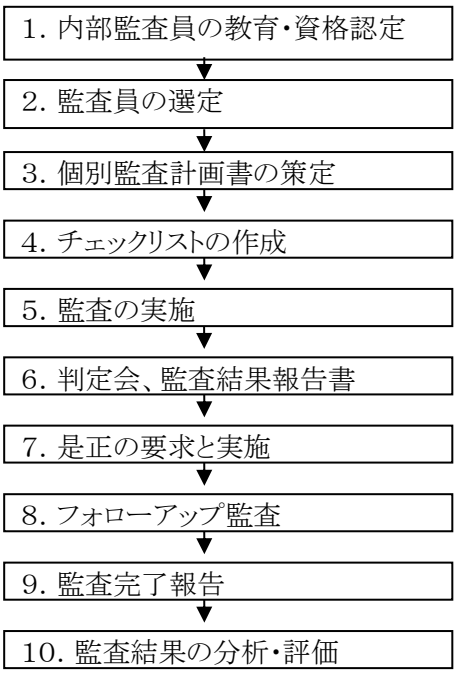
情報セキュリティの運用状況を把握するため、以下に基づき内部監査を実施する。

（1）目的
情報セキュリティ対策、プロセス及び手順について以下の事項が満たされているか否かを明確にする目的で内部監査を計画・実施する。
1)本市に関連する法令又は規制に適合していること。
2)本市の定める情報セキュリティポリシーに適合していること。
3)有効に実施され、維持されていること。

（2）指摘事項等の種別
内部監査で使用する指摘事項の区分を以下のように設定する。

分　　類	定　　義
重大な不適合	法令・規制等への違反又は、情報セキュリティの維持に重大な影響を及ぼす恐れがある場合。（ポリシーの欠落、手順からの大きな逸脱）
軽微な不適合	ポリシーの一つにおいて、部分的又は一時的に手抜かりがあった場合
観察事項	間違ってはいないが、もう少し改善をした方が良い場合又は、気になる点

（３）内部監査の実施手順図１「内部監査フロー」に示す。



※　必要時のみ実施

①内部監査員の教育・資格認定

内部監査員は、監査員として資格認定される必要がある。以下のいずれかに該当する者を監査統括責任者が監査員として認定する。認定した者は、「資格登録書」に記載する。

ア　情報セキュリティに関する基本的な知識を有し、内部監査員研修を修了した者。

イ　ISMS 及び情報セキュリティ監査に関する知識を有し、その審査員（監査員）資格を有する者。

ウ　監査統括責任者が特に認めた者。

②監査員の選定

監査統括責任者は、「資格登録書」に記載されている職員の中から、内部監査員を選出する。内部監査員にはリーダとメンバを選出し監査チームを編成する。また、監査の客観性及び公平性を確保するため、自身の業務を監査することがないよう選定する。

③個別監査計画書の作成

監査チームのリーダは、「個別監査計画書」を作成する。作成後は、監査統括責任者の承認後、監査実施予定日の１週間前までに監査対象部門へ周知する。

④チェックリストの作成

内部監査員は「チェックリスト」に基づき、監査時の質問事項等を明確にする。

⑤監査の実施

監査チームリーダは監査開始の冒頭で、開始に先立ち監査対象部署に対して、「個別監査計画書」にて、監査目的の説明、スケジュール等の確認を行う。（初回会議）

各監査員は「個別監査計画書」、「チェックリスト」に基づき監査対象部署の監査を実施する。

監査の質疑等が終了後、監査チームのみ集まり、チームリーダは監査の内容についてメンバの意見をまとめる。

これに基づき監査チームリーダは、被監査側に結果を説明する。(終了会議)

⑥監査結果報告
監査チームリーダは、「個別監査報告書」の“不適合内容”及び“監査チーム総評”を作成する。不適合がある場合は「不適合報告書」を合わせて作成する。
監査チームのリーダは「個別監査報告書」と「不適合報告書」(不適合がある場合のみ)を監査統括責任者に報告する。
監査統括責任者は、「個別監査報告書」と「不適合報告書」(不適合がある場合のみ)の内容を確認する。不適合がない場合は、承認する。

⑦是正の要求と実施
監査統括責任者は、不適合がある場合のみ「不適合報告書」にて監査対象部署の責任者に是正処置要求を通知する。
監査対象部署の責任者は、「不適合報告書」の必要な欄を記入し、是正処置を遅滞なく実施し、「不適合報告書」の“処置完了確認”欄に承認サインを記入する。その後、監査統括責任者へ提出する。

⑧フォローアップ監査
監査統括責任者は、「不適合報告書」に基づき、フォローアップ監査の必要性を判断する。
フォローアップ監査を実施する場合は、監査チームリーダにフォローアップ監査の実施を依頼する。
フォローアップ監査完了後、「不適合報告書」の“フォローアップ監査”欄を作成し監査統括責任者へ提出する。

⑨記録、様式の管理
内部監査にかかわる記録は、ポリシー事務局が保管、管理する。

14.2 外部監査

情報セキュリティにおける外部審査(監査)については、原則、審査(監査)側の指示に基づき行う。外部審査(監査)において指摘された事項への対応、及び是正の処置については、適宜実施する。

15 自己点検

情報セキュリティの実施状況について、定期的又は必要に応じて自己点検を実施する。点検項目は、情報セキュリティポリシーに基づき、「自己点検表」に従って、随時作成するものとするが、以下の内容を必ず含めるものとする。

・内部監査、外部監査の結果
・過去に発生した事件、事項等
・新聞や報道等により話題になっている内容

点検結果は、統括情報セキュリティ責任者が取りまとめを行い、情報セキュリティ委員会で報告する。

情報セキュリティインシデント記録表

発生確認	CISO	統括情報セキュリティ責任者	情報セキュリティ管理者

作成日　　年　　月　　日

該　当　担　当（室）課	
報　告　者	報告日：　　年　月　日（　）
インシデントの概要 （原因・被害状況等）	発生日：　　年　　月　　日（　）
対　応　措　置 （時　刻） （対応者） ・初期対応 ・応急措置含む対応状況 ・情報セキュリティ委員会の協議及び対応指示 ・具体的対処案 ・事後処理策 ・その他	
反　省　事　項　等	

＊必要に応じて資料等を添付願います。

終了確認	CISO	統括情報セキュリティ責任者	情報セキュリティ管理者

保管期間　３年

資格登録書

作成日	年　　月　　日

以下の者を内部監査の有資格者として登録する。資格登録を取り消す場合は、取消日を記入する。

氏名	氏名コード	所属	認定日 取消日	承認欄

事務局にて保管

個別監査計画書

承　認	作　成
（　．　．）	（　．　．）

1	監査方針	
2	監査の目的	
3	対象部署（範囲）	
4	監査年月日	
5	監査チーム	リーダ：　　メンバ：

【監査の基準】

6	適用規程	「情報セキュリティポリシー　第　　版」　　制改定日　　年　月　　日

【監査の方法、範囲】

	監査日時	部署名（対応者）	監査項目
7　監査スケジュール			

※監査実施１週間前までに、作成し承認を得ること。被監査部署へも渡すこと。
事務局にて保管

監 査 チ ェ ッ ク リ ス ト

監査日　　年　　月　　日

対象部署：	対応者：	監査員：

事前に質問内容として①、②、③に記入する。監査中は「結果」欄に「○」「×」「△」を記入する。監査中に確認した内容等はメモ欄に記入する。後に報告書へ記載する。

項番	①情報セキュリティポリシー要求項番	②セキュリティルール	③必要なアウトプット	結　果	メ　　モ

「結果」欄凡例：○適合、×不適合、△観察事項　適合不適合基準は本文１４．１（２）を参照
監査当日までに作成のこと。被監査部署へは渡さない（質問項目を事前に伝えることになります)。

個別監査報告書

【判定結果】

判定結果	下記のような判定結果になりましたので確認願います。 （通知日　　年　　月　　日）	監査リーダ （　．　．　）

1	対象部署／監査年月日		年　　月　　日実施
2	監査チーム	リーダ　　メンバ	
3	不適合等の内容	件数　　件	
		● 重大な不適合 件 詳細は不適合報告書による ● 軽微な不適合 件 詳細は不適合報告書による ● 観察事項 件 （　　） （　　） （　　） （　　） （　　）	
4	監査チーム総評		
5	是正要求	有り　／　無し	
		不適合報告書Ｎｏ．	
6	監査統括責任者確認	 （　．　．　）	

※チェックリストと一緒に提出のこと。不適合の有無に係らず監査実施後、必ず作成する。

不適合報告書

Ｎｏ.

年　月　　日実施の監査の結果、以下の不適合が発見されました。 ご対応をお願いします。	監査チームリーダ （　．　．）

部　署　名	
不適合の内容	不適合の種類（重大な不適合、軽微な不適合） 証拠「　　」 具体的内容 情報セキュリティポリシー項番

不適合の処理	（是正要求日　　年　　月　　日）
原因調査結果	
決定内容	処置内容

処置完了確認	上記処置が完了いたしましたので報告いたします。 （　　年　　月　　日）	実　施　者

フォローアップ監査 （報告兼）	フォローアップ監査の要否（　要　・　否　） フォローアップ監査内容 （実施日：　　年　　月　　日）	監査統括責任者 （．　．）	監査チームリーダ （．　．）

※不適合１つに、１枚使用する。（例:不適合が２つある場合は、２枚となる）

自己点検表

記入方法：実施できていれば「○」、できてなければ「×」を記入します。業務の状況等で、実施していない項目や該当しない項目は「－」を記入してください。

No	チェックポイント	○or×
1	5分以上、席を離れるときは、机上の電子媒体は、片付けている。	
2	スクリーンセーバーの起動開始時間は5分以内としている。	
3	ID、パスワード等の認証情報を入力する際には、周囲に配慮しているか。	
4	自治体機密性２以上の情報が保存されていたパソコン、電子媒体等を再使用する際には、保存されていた情報を消去後再使用している。	
5	自治体機密性２以上の情報が印刷された紙媒体の裏面は、使用していない。	
6	プリントアウト時は、プリンタ等に、長時間放置していない。	
7	情報が保管された媒体の廃棄を行う際は、情報が再生不可能な状態まで物理的破壊を実施している。	
8	自治体機密性２以上の紙媒体を廃棄する場合、シュレッダー等を利用している。	
9	私物のパソコンや電子媒体を持ち込んでいない。	
10	重要な情報を記録した媒体をやむを得ず外へ持ち出す場合は、情報セキュリティ管理者の許可を得ている。	
11	コンピュータウイルス感染が発生した場合、被害の拡大を防止するため、PC・サーバをネットワークから切り離し、情報セキュリティ管理者に報告している。	
12	本市の事業に関わる情報や、市民、職員のプライバシーに関わる情報などの機密情報は、電子メール本文に直接書き込んで用いて送信していない。	
13	電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信している。	
14	電子メールを個人的なメールアドレスに自動転送していない。	
15	みだりに業務目的以外に電子メールを利用していない。	

16	送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルを操作してない。	
17	一般に使われている単語や本人の趣味、プライベートなどから、他人に推測されやすいパスワードを使用していない。	
18	パスワードは口外したり、ヒントとなるような物品を身の回りに置いたり、していない。	
19	ユーザ ID を本人以外が使用していない。 （他人のアカウントの利用や、課長でログインした後の承認等の代行）	
20	個人 PC をネットワーク上でデータ共有していない。	
21	FD や CD-R などの媒体から情報を PC・サーバに取り込む場合、また、PC・サーバから書き込む場合にも、ウィルスチェックをしている。	