公益財団法人神戸市産業振興財団 情報セキュリティポリシー

第１章 情報セキュリティ基本方針

１．目的

財団が取り扱う情報には，企業・市民情報や財団運営上重要な情報が含まれており，情報資産を人的脅威や災害，事故等様々な脅威から防御することは，企業・市民の財産，プライバシー等を守るためにも，また，継続的かつ安全・安定的なサービスの実施を確保するためにも必要不可欠である。

このため，財団が保有する情報資産の機密性，完全性及び可用性を維持することを目的として神戸市産業振興財団情報セキュリティポリシー（以下「情報セキュリティポリシー」という）を定める。

２．定義

（１）ネットワーク

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

（２）情報システム

コンピュータ及びネットワークで構成され，情報処理を行う仕組みをいう。

（３）データ

処理に係る入出力帳票，記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（４）情報セキュリティ

情報資産の機密性，完全性及び可用性を維持することをいう。

（５）情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

（６）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。

（７）完全性

情報が破壊，改ざん又は消去されていない状態を確保することをいう。

（８）可用性

情報にアクセスすることを認められた者が，必要な時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。

（９）マイナンバー利用事務系

個人番号を取扱う業務に関わる情報システム及びデータをいう。

３．情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは，財団が保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり，情報セキュリティ基本方針及び情報セキュリティ対策基準により構成される。

情報セキュリティ対策基準は、情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために最低限必要な水準として、市派遣職員，固有職員，嘱託職員，短期雇用職員，派遣労働者，出向職員，業務委嘱等により本財団業務に従事する者（以下「職員等情報取扱者」という）が遵守すべき事項及び判断基準をまとめたものである。本財団では、組織等の状況に合わせた情報セキュリティ対策基準を策定する。

４．情報資産への脅威

情報セキュリティ対策を講じるうえでは，情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に次の脅威については，十分な措置を講じるものとする。

(ア)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、部外者の侵入等による情報資産の漏洩・破壊・改ざん・消去、重要情報の搾取、内部不正等。

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

(ウ)地震，落雷，火災等の災害，事故，故障等によるサービス及び業務の停止。

(エ)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。

(オ)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。

５．情報セキュリティポリシーの適用範囲

（１）組織の範囲

本財団の全ての部門・部署に適用する。

（２）情報資産の範囲

情報セキュリティ基本方針が対象とする情報資産は次のとおりとする。

(ア)物理資産

コンピュータ・ネットワーク・電磁的記録媒体等物理的な形状を有する資産でありかつ，情報を利用するのに必要な資産。

(イ)データ資産

ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む）

情報システムの仕様書及びネットワーク図等のシステム関連文書

(ウ)ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム。

(エ)サービス資産

電源，メールサービス等契約により提供される情報システムに関連する業務。

６．職員等の遵守義務

職員等情報取扱者は，情報セキュリティの重要性について共通の認識を持つとともに，業務の遂行にあたっては情報セキュリティポリシーを遵守するものとする。

７．情報セキュリティ対策

（１）情報セキュリティ管理体制

財団の情報資産について，適切に情報セキュリティ対策を推進・管理するため、常務理事を情報セキュリティ責任者とする組織体制を確立する。必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

（２）情報資産の分類と管理

本財団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講じる。

（3）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、情報資産の分類に応じた情報セキュリティ対策を講じる。

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うえで、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、個人情報の流出を防ぐ。

（4）物理的セキュリティ

通信回線及び端末等への物理的な対策を講じる。

（5）人的セキュリティ

情報セキュリティに関し，職員等情報取扱者が遵守すべき事項を定めるとともに，研修実施するなど人的な対策を講じる。

（6）技術的セキュリティ

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

（7）運用面のセキュリティ

情報システムの監視，情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等，情報セキュリティポリシーの運用面の対策を講じる。また，情報資産への侵害が発生した場合等に，迅速かつ適切に対応する。

（8）外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

8．情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため，必要に応じて情報セキュリティ監査及び自己点検を実施する。

9．情報セキュリティポリシーの見直し

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

１０．情報セキュリティ対策基準の策定

上記７、８及び９に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を第二章に定める。

１１．情報セキュリティ個別基準の策定

情報セキュリティ対策基準を補完するために必要な内容に関して、具体的な内容を定める情報セキュリティ個別基準を第三章に定める。なお、情報セキュリティ個別基準は、公にすることにより本財団の業務に重大な支障を及ぼすおそれがあることから非公開とする。

第２章 情報セキュリティ対策基準

１．目的

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に基づき情報セキュリティ対策等を実施するために共通の基準として具体的な遵守事項及び判断基準を定めたものである。

２．適用範囲

本財団の全ての部門・部署に適用する。

３．組織体制

（１）体制

適切に情報セキュリティ対策を推進・管理するため、次の者を置く。

(ア)情報セキュリティ責任者

常務理事を情報セキュリティ責任者とする。

(イ)情報セキュリティ管理者

総務部長を情報セキュリティ管理者とする。

(ウ)情報管理者

各部の長（所属長）及びグループリーダーを情報管理者とする。

(エ)情報基盤管理者

総務部総務グループリーダーを情報基盤管理者とする。

(オ)情報セキュリティ監査責任者

情報セキュリティ責任者が指名する。

（２）権限と責任

(ア)情報セキュリティ責任者

① 情報セキュリティ責任者は，財団における情報システム，データ等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

② 情報セキュリティ責任者は，財団の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害の恐れがある場合に，必要かつ十分な措置を行う権限及

び責任を有する。

③　情報セキュリティ責任者は、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専門家をアドバイザーとして置くものとする。

(イ)情報セキュリティ管理者

①　情報セキュリティ管理者は，情報セキュリティ責任者を補佐しその実務を担当する。

②　情報セキュリティ管理者は、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専門家をアドバイザーとして置くものとする。

(ウ)情報管理者

①　情報管理者は，所管部内におけるデータ等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

②　情報管理者は，所管部内におけるデータ等の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害の恐れがある場合には，情報セキュリティ管理者へ速やかに報告を行い，指示を仰がなければならない。

③　情報管理者は、情報システム運用管理者の指示に従い所管部内におけるネットワーク、情報システム、情報等の情報資産のうち所轄組織内のパーソナルコンピュータ等についての物理的セキュリティに関する管理を行う。

(エ)情報基盤管理者

①　情報基盤管理者は、ネットワーク、情報システム、情報等の情報資産における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

②　情報基盤管理者は、ネットワーク、情報システム、情報等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

③　情報基盤管理者は、ネットワーク、情報システム、情報等の情報資産に係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

④　情報基盤管理者は、ネットワーク、情報システム、情報等の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者、情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

⑤　情報基盤管理者は、ネットワーク、情報システム、情報等の情報資産における開発、設定の変更、運用等についての作業を情報セキュリティ管理者が指名する者に行わせることができる。

⑥　情報基盤管理者は、ネットワーク、情報システム、情報等の情報資産のうちパーソナルコンピュータ等についての物理的セキュリティに関する管理を情報管理者に行わせることができる。

(オ)情報セキュリティ監査責任者

情報セキュリティ監査責任者は、情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

(カ)兼務の禁止

① 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認または許可の申請を行うものとその承認者又は許可者は、同じ者が兼務してはならない。

② 情報セキュリティ監査の実施において、監査を受けるもの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。

(キ)情報セキュリティ委員会

① 本財団の情報セキュリティ対策を統一的に実施するため、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の重要な変更等情報セキュリティに関する重要な事項を決定する。

② 情報セキュリティ委員会は、必要に応じて、本財団における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

４．情報資産の分類と管理

（１）情報資産の分類と管理方法

(ア)対象となる情報資産は，各々の情報資産の機密性，完全性及び可用性を踏まえ，次の重要性分類に従って分類する。(表参照)

機密性	
2	財団業務で取り扱う情報資産のうち，特に機密性を要するもの 次のデータだけでなくそれらが含まれる電磁的記録媒体，パーソナルコンピュータ，システム等も同様) ● 市民情報に関するデータ（個人の携帯電話番号が含まれるデータ等） ● 法令の規定により秘密を守る義務を課されているデータ（秘密保持契約によって保護されるデータ等） ● 部外に知られることが適当でない法人その他団体に関するデータ（事業承継に関するデータ等） ● 部外に漏れた場合に財団の信頼を著しく害するおそれのあるデータ（認定・審査に関するデータ等）

	● 公開することでセキュリティ侵害が生じるおそれのあるデータ（無線 LAN の接続パスワードや情報システムの仕様書データ等）
1	機密性２の情報資産以外のもの
完全性	
2	財団業務で取り扱う情報資産のうち，特に完全性を要するもの 改ざんあるいは誤りがあると個人の権利が侵害される，又は事業の適確な遂行に支障を及ぼす可能性があるもの 次のデータだけでなくそれらが含まれる電磁的記録媒体、パーソナルコンピュータ，システム等も同様 ● 市民情報に関するデータ ● 法令の規定により秘密を守る義務を課されているデータ ● 部外に知られることが適当でない法人その他団体に関するデータ ● 部外に漏れた場合に財団の信頼を著しく害するおそれのあるデータ
1	完全性２の情報資産以外のもの
可用性	
2	財団業務で取り扱う情報資産のうち，特に可用性を要するもの 利用できないと市民の権利が侵害される，又は事業の安定的な遂行に支障を及ぼす可能性があるもの 次のデータだけでなくそれらが含まれる電磁的記録媒体，パーソナルコンピュータ，システム等も同様 ● 滅失し又は損傷した場合その復元が著しく困難であるため事業の円滑な運営が妨げられるおそれのあるデータ
1	可用性２の情報資産以外のもの

(イ)情報資産の機密性，完全性，可用性のいずれかの重要性分類２に分類される情報資産は，この対策基準の対象とする。

(ウ)重要性分類がいずれも１の情報資産も，必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

（２）情報資産の管理

(ア)管理責任

① 情報資産は，情報管理者がそれぞれ所管する情報資産についての管理責任を有する。また，情報管理者は、当該情報資産の利用範囲を定め、リスクを分析し、リスクに応じた対策を講じなければならない。

② 職員等情報取扱者は，情報資産の作成・入手・利用等に際しては，十分にその責任を自覚したうえで行わなければならない。

③ データが複製又は伝送された場合には，当該複製等も原本と同様に管理しなければならない。

(イ)情報資産の分類の表示

① 重要な情報資産に対しては、必要に応じて、目録を作成して管理しなければならない。

② 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。

(ウ)情報の作成

① 職員等情報取扱者は、業務上必要のないデータを作成してはならない。

② 情報を作成する者は、情報の作成時に重要性分類に基づき、当該情報の分類を定めなければならない。

③ 作成途上のデータについても，紛失や流失等を防止しなければならない。また，データ作成上で不要になった場合は，当該データを消去しなければならない。

(エ)情報資産の入手

① 財団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。

② 財団外の者が作成した情報資産を入手した者は，重要性分類に基づき，当該情報の分類を定めなければならない。

③ 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，情報管理者に判断を仰がなければならない。

(オ)情報資産の利用

① 情報資産を利用する者は，情報資産を業務上の目的以外に利用してはならない。

② 情報資産の利用においては、情報資産の分類に応じ、利用者並びにアクセス権限を定めなければならない。

③ 機密性 2 の情報は、情報管理者の許可を得た場合、複製・送付・送信・電子メー

ル送信を行うことができる。また、権限のある者だけがアクセスできる環境で、保存・利用をしなければならない。複数の権限ある者で情報を共有したり、所属外に情報を送付・送信・電子メール送信したりするときは、暗号化又はパスワード等による情報漏えい対策を施さなければならない。

④ 電磁的記録媒体又は紙媒体に情報資産の重要性分類 1 と 2 の両方が記録されている場合、重要性分類 2 に従って、当該媒体を取り扱わなければならない。

(カ)情報資産の保管

① 情報管理者は，情報資産の重要性分類に従って，情報資産の保管を適切に行わなければならない。

② 最終的に確定したデータを記録した電磁的記録媒体は，書込禁止措置を行ったうえで保管しなければならない。

③ 情報管理者は、持ち運び可能な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。

④ 情報基盤管理者は、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情報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への保管を考慮しなければならない。

(キ)情報資産の運搬

① 機密性 2 の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

② 機密性 2 の情報資産を運搬する者は，情報管理者に必要に応じて許可を受けなければならない。

(ク)情報資産の提供・公表

① 機密性 2 の情報資産を外部に提供する者は，必要に応じ暗号化又はパスワードの設定を行わなければならない。

② 機密性 2 の情報資産を外部に提供する者は，情報管理者に事前に許可を得たうえで、日時・担当者及び提供概要が記録に残るように注意しなければならない。

③ 情報管理者は，市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。

(ケ)情報資産の廃棄

① 情報資産の廃棄を行うものは、情報を記録している電磁的記録媒体が不要となった場合，当該媒体に含まれるデータの消去を行ったうえで焼却，裁断又は溶解

等により復元不可能な状態にして廃棄しなければならない。紙媒体が不要となった場合は、焼却、裁断、溶解等により廃棄しなければならない。

② 情報資産の廃棄を行う者は、行った処理について日時、担当者及び処理内容を記録しなければならない。

③ 情報資産の廃棄を行う者は、情報管理者の許可を得なければならない。

（３）文書の管理

(ア)情報セキュリティ対策基準を実施していくうえで必要とされる文書は、文書取扱規程に従い管理しなければならない。

(イ)情報セキュリティに係る文書（以下「文書」という。）を作成又は更新する場合は、あらかじめ定められた者による承認を受けなければならない。

(ウ)文書は、定期的に見直しを行い、必要に応じて更新しなければならない。

(エ)文書を廃棄する場合は、廃棄文書が誤って使用されないようにしなければならない。ただし、廃棄文書を保持する必要がある場合には、廃棄文書と分かるように適切な識別を施さなければならない。

（４）記録の管理

情報セキュリティ対策基準の効果的運用の証拠を示すために、記録を作成し、適切な管理をしなければならない。

５．情報システム全体の強靭性の向上

（１）マイナンバー利用事務系

(ア)マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。

(イ)情報のアクセス及び持ち出しにおける対策

① 情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用することが望ましい。また、業務毎に専用端末を設置することが望ましい。

② 原則として、USB メモリ等の電磁的記録媒体やモバイル端末等による情報持ち出しができないように設定しなければならない。

６．物理的セキュリティ

（１）情報機器の管理

(ア)機器の取付け

情報基盤管理者は、ネットワーク機器及び情報システム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な固定を行う等必要な措置を講じなければならない。

(イ)機器の定期保守及び修理

情報基盤管理者及び情報管理者は，記憶装置を内蔵する機器を外部の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、修理を委託する事業者との間で，守秘義務契約を締結する他、秘密保持体制の確認などを行わなければならない。

（２）ネットワークの管理

(ア)通信回線及び通信回線装置の管理

情報基盤管理者、財団内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

(イ)外部ネットワークへの接続

情報基盤管理者は、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)機密を要する情報システムで使用する回線

情報基盤管理者は、所管する情報システムにおいて機密性 2 の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討のうえ、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化や送信する情報を必要最小限にする等、情報保護のために適正な措置を講じなければならない。

(エ)ネットワークで使用する回線

① 情報基盤管理者、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。

② 情報基盤管理者は、ネットワークで使用する回線を選択するにあたって、必要な可用性を考慮しなければならない。

(オ)執務区域外からのマイナンバー利用事務系への接続制限

情報基盤管理者は、執務区域外で業務を行うモバイル端末からマイナンバー利用事務系にアクセスできるようにしてはならない。

（３）端末や電磁的記録媒体等の管理

(ア)端末等の盗難防止策

情報管理者は、執務区域等の端末等について盗難防止のための措置を講じなければならない。また、情報管理者は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措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

(イ)ログイン認証

① 情報基盤管理者及び情報管理者は，職員等情報取扱者が情報システムへログインする際に、パスワード、スマートカード、或いは生体認証等の認証情報の入力を求めるように設定しなければならない。また、執務区域外に持ち出す可能性のある端末には、電源起動時のパスワード入力(BIOS パスワード、ハードディスクパスワード等）を求めるように設定するものとする。

② 情報基盤管理者は、マイナンバー利用事務系では認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定することが望ましい。

(ウ)暗号化機能の利用

情報基盤管理者及び情報管理者は、端末等におけるデータの暗号化等の機能を利用するように設定しなければならない。端末等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。また、電磁的記録媒体についても、取り扱う情報の重要度に応じてデータ暗号化機能を備える媒体を使用しなければならない。

(エ)モバイル端末のセキュリティ

① 情報基盤管理者は、モバイル端末を執務区域外で業務利用する場合は、上記対策に加え、端末の紛失・盗難対策として、情報システムへログインする際に、パスワードとは別に、スマートカード、或いは生体認証等の複数の認証情報の入力を求めるように設定しなければならない。

② 情報基盤管理者は、モバイル端末を執務区域外で業務利用する場合に、紛失・盗難に遭った際の対応として、遠隔消去（リモートワイプ）や自己消去機能などを活用できるときは、それらの機能を活用し、モバイル端末内のデータを消去しな

ければならない。

③　モバイル端末には覗き見防止の措置を講じなければならない。

(オ)記録管理

情報基盤管理者は，情報資産にアクセスできる全ての端末を管理台帳に記載しなければならない。

７．人的セキュリティ

（１）職員等情報取扱者の責務

(ア)情報セキュリティポリシー等の遵守義務

職員等情報取扱者は，情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守しなければならない。また、情報セキュリティ対策について不明な点，遵守することが困難な点がある場合には，情報セキュリティ責任者等権限のある者に相談し，指示を仰がなければならない。

(イ)業務以外の目的での使用禁止

職員等情報取扱者は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセス等を行ってはならない。

(ウ)指示に基づいた情報資産の利用等

職員等情報取扱者は，情報セキュリティ責任者等権限のある者の指示等に従い，情報資産を利用するとともに，開発，設定の変更，運用，更新等の作業を行う。

(エ)情報資産の持ち出し禁止

職員等情報取扱者は、情報管理者の許可を得た場合に限り、記録を作成したうえで、執務区域外へ情報資産を持ち出すことができる。

(オ)執務区域外における情報処理作業の制限

①　職員等情報取扱者は、執務区域外で情報処理作業を行う場合には、情報管理者の許可を得なければならない。

②　職員等は，執務区域外で端末を使用して情報処理作業を行う場合には，大量または機微な個人情報を取り扱ってはならない。また，公共の場又は公共の乗り物内においては個人情報を取り扱ってはならない。

③　職員等情報取扱者は紛失・盗難を防止するため、移動の際は細心の注意をもってモバイル端末を携行しなければならない。

④　職員等情報取扱者は覗き見を防止するため、執務区域外において職員等以外の目に触れないように取り扱わなければならない。

⑤　職員等情報取扱者は不正使用を防止するため、モバイル端末を使用しないときは、他者に端末が使用されないように必要な対策を取らなければならない。

⑥　職員等情報取扱者はモバイル端末でデータを保存する場合、指定された領域にデータを保存することとし、原則として端末内にデータを保存してはならない。

⑦　職員等情報取扱者は、使用しているモバイル端末について、定期的に情報管理者の確認を受けなければならない。

⑧　職員等情報取扱者は、執務区域外でモバイル端末を使用する場合、原則としてモバイル端末をプリンタに接続して、情報資産の出力等を行ってはならない。

(カ)支給以外の端末及びモバイル端末及び電磁的記録媒体等の業務利用

職員等情報取扱者は，支給以外の端末，モバイル端末及び電磁的記録媒体等（データ保存機能のないマウスやキーボード等の PC 周辺機器を除く）を原則として業務に利用してはならない。ただし，支給以外の端末の業務利用については，情報セキュリティ管理者が利用手順を定め，職員等情報取扱者は利用手順に従い情報管理者の許可を得て利用することができる。

(キ)持ち出しの記録

情報管理者は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

(ク)端末やモバイル端末におけるセキュリティ設定変更の禁止

職員等情報取扱者は、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又は情報管理者の許可なく変更してはならない。

(ケ)机上の端末等の管理

職員等情報取扱者は、端末や電磁的記録媒体、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。

(コ)異動，退職時等の遵守事項

職員等情報取扱者は，異動，退職等により業務を離れる場合には，利用していた情報資産を，返却しなければならない。また，その後も業務上知り得た情報を漏らしてはならない。

(サ)情報セキュリティポリシー等の掲示

情報管理者は，職員等情報取扱者が常に情報セキュリティポリシー及びこれに基づく文書を参照できるよう配慮しなければならない。

（２）職員等情報取扱者に対する研修・訓練の実施

(ア)情報セキュリティに関する研修・訓練

情報セキュリティ責任者は，定期的に職員等情報取扱者に対する情報セキュリティに関する研修を実施させなければならない。情報管理者は，所属の研修の実施状況を記録し，情報セキュリティ責任者に対して，報告しなければならない。

(イ)研修の実施

研修は、情報セキュリティ管理者、情報管理者及び職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

(ウ)緊急時対応訓練

① 情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練は、ネットワーク及び各情報システムの規模等を考慮し、実施体制、範囲等を定め、また、効果的に実施できるようにしなければならない。なお、情報セキュリティ責任者は、緊急時対応訓練の実施結果を受けて、必要に応じて緊急時の体制や対応手順の改善を行わなければならない。

② 情報セキュリティ責任者は、緊急時対応訓練の実施結果を受けて、緊急時の体制や対応手順の改善を行わなければならない。

(エ)研修・訓練への参加

すべての職員等情報取扱者は，情報セキュリティに関する意識を深め，情報セキュリティ上の問題が生じないようにするため，定められた研修に参加しなければならない。

（３）事故等の報告・分析等

(ア)事故等の報告

① 職員等情報取扱者は，情報セキュリティに関する事件・事故等を発見した場合，市民等外部から報告を受けた場合，速やかに情報管理者又は情報セキュリティ管理者等権限のある者に報告しなければならない。

② 報告を受けた情報管理者又は情報セキュリティ管理者等権限のある者は，必要に応じて情報セキュリティ責任者に報告しなければならない。また、当該事故等がネットワークに関連する場合は、情報基盤管理者に対しても報告しなければ

ならない。

③　情報セキュリティ管理者は、報告のあった事故等について、市の業務上の関係機関に必要な連絡を行わなければならない。

(イ)事故等の報告内容

情報セキュリティに関する事件・事故等の報告には、以下の内容を含むものとする。

①　件名

②　判明した日時

③　発生した日時

④　通報者

⑤　事件・事故等の内容

⑥　漏えいした情報

⑦　想定される原因

⑧　事件・事故等の対応方針

⑨　事件・事故等の復旧方針

(ウ)事故等の分析・記録・再発防止等

情報セキュリティ管理者及び事故等を引き起こした部門の情報管理者は，これらの事故等を分析し，記録を保存し、再発防止策を講じなければならない。

①　情報セキュリティ管理者は、事件・事故等に関係する情報管理者に対し、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。

②　情報セキュリティ管理者及び情報管理者は、事件・事故の原因を究明し、記録を保存しなければならない。また、事件・事故の原因究明の結果から、再発防止策を検討し、情報セキュリティ責任者に報告しなければならない。

③　情報セキュリティ責任者は、事件・事故について報告を受けた際に、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）アクセスのための認証情報及びパスワードの管理

(ア)ID の取り扱い

職員等情報取扱者は，自己の ID に関し，次の事項を遵守しなければならない。

①　自己が利用している ID は、他人に利用させてはならない

②　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

(イ)パスワードの取り扱い

職員等情報取扱者は，自己のパスワードに関し，次の事項を遵守しなければならない。

① パスワードは、他者に知られないように管理しなければならない。
② パスワードは秘密とする。パスワードの照会等には一切応じてはならない。
③ パスワードは十分な長さとし，文字列は想像しにくいものとする。
④ 原則として，パスワードを記載したメモを作成しない。やむを得ずメモを作成する場合は，特定の場所に施錠して保存する等により、他人が容易に見ることができない措置をとる。
⑤ パスワードに対する危険のおそれがある場合には，情報管理者に報告し，パスワードを速やかに変更する。
⑥ 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑦ 仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
⑧ 職員等情報取扱者の間でパスワードを共有しない。ただし、共用 ID に対するパスワードを除く。
⑨ パスワードは定期的に変更しなければならない。

８．技術的セキュリティ

（１）コンピュータ及びネットワーク管理

情報基盤管理者及び情報管理者は，情報資産に関する脅威から情報資産を守るために，コンピュータやネットワークを適切に設定し，管理しなければならない。

(ア)情報の保存

情報の保存については、情報基盤管理者等権限のある者の定める方法により保存を行わなければならない。

(イ)情報共有システムの設定等

情報基盤管理者がファイルサーバ等の情報共有システムを設置する場合には、次の事項を遵守しなければならない。

① 職員等が他所属等の情報を閲覧及び使用できないように、所属等の単位でアクセス制限を設定しなければならない。
② 特定の職員等のみが取扱う権限を持つ情報については、同一所属であっても、権限のない職員等が閲覧及び使用できないよう、アクセス制限を設定しなければならない。

(ウ)バックアップの実施

情報基盤管理者は、必要に応じて、定期的に情報資産のバックアップのための対応を

実施しなければならない。

(エ)他団体との情報システムに関する情報等の交換

情報基盤管理者は、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。

(オ)システム管理記録及び作業の確認

① 情報基盤管理者は、情報システムの運用において実施した作業について、作業記録を作成しなければならない。

② 情報基盤管理者は、情報システムのシステム変更等の作業を行った場合は、作業内容を記録し、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 情報基盤管理者又は職員等及び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名以上で作業し、互いにその作業を確認しなければならない。

(カ)情報システム仕様書等の管理

情報基盤管理者は、ネットワーク構成図及び情報システム仕様書については、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすること等がないよう、適正に管理しなければならない。

(キ)ログの取得等

① 情報基盤管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 情報基盤管理者は、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 情報基盤管理者は、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。

④ 情報基盤管理者は、システムから自動出力したログ等について、必要に応じ、外部記録媒体にバックアップしなければならない。

(ク)障害記録

情報基盤管理者は、所管するシステムにおいて、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を障害記録として体系的に記録し、適正に保存しなければならない。

(ケ)ネットワークの接続制御等

① 情報基盤管理者は、ネットワーク上のサービス毎に、アクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない者が当該サービスを利用できるようにしてはならない。

② 情報基盤管理者は、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。

③ 情報基盤管理者及び業務システム管理者は、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。

(コ)外部の者が利用できるシステムの分離等

① 情報基盤管理者は、電子申請の汎用受付システム等、外部の者（職員等情報取扱者及び委託業務従事者等以外の者）が利用できるシステムにおいては、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、情報セキュリティ対策について特に強固に対策を講じなければならない。

② 外部の者が利用できるシステムにおいて、機密性 2 の情報を照会又は更新するために外部の者がインターネット経由でシステムにアクセスしようとする場合は、多段階認証又は多要素認証を利用しなければならない。ただし、定型的な回答又は届出を送信するためにアクセスしようとする場合はこの限りではない。

(サ)外部ネットワークとの接続制限等

① 情報基盤管理者は、外部ネットワークとの接続にあたり、当該外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、適用範囲における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。

② 情報基盤管理者は、接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。情報基盤管理者は、当該外部ネットワークの瑕疵により本財団のデータの漏えい、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応するため、必要に応じて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するよう努めなければならない。

③ 外部からの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。

④ 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、適用範囲における情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークとの接続を物理的に遮断しなければならない。

(シ) Web サイトでの情報公開時の注意事項

① 情報基盤管理者は、Web サイトにより情報を公開・提供する場合に、所管するサイトに係るシステムにおいて情報の漏えい・改ざん・消去、踏み台、DoS 攻撃等を防止しなければならない。

② メールシステムを含め各業務システムにおいても、他のシステムに対する攻撃の踏み台とならないようにコンピュータウィルス対策等適正な管理をしなければならない。

③ 新たに Web サイトを公開する場合、全てのページで TLS 通信を利用すること。なお、現状未対応の公開 Web サイトは、全てのページで TLS 通信を利用するために必要な作業を実施しなければならない。

(ス) 複合機のセキュリティ管理

① 情報基盤管理者は、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機能を持つ機材を調達しなければならなない。

② 情報基盤管理者は、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リスクへの対策を講じなければならない。

③ 情報基盤管理者は、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。

(セ) IoT 機器を含む特定用途機器のセキュリティ管理

情報基盤管理者は、所管する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。

(ソ) 電子メールのセキュリティ管理

① 電子メールの利用を希望する場合は、情報基盤管理者が利用者を特定し、メールアドレスの取得を申請するものとする。

② 情報基盤管理者は、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。

③ 情報基盤管理者は、電子メールに添付されるファイルについて、セキュリティ上問題があると思われるファイルについては、送受信を制限できるようにしなければならない。

④ 情報基盤管理者は、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。

⑤ 情報基盤管理者は、システム開発や運用、保守等のため財団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利用について、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。

(タ)電子メールの利用制限

① メールアドレス保有者は，自動転送機能を用いて，電子メールを転送してならない。

② メールアドレス保有者は，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 メールアドレス保有者は，複数の宛先に電子メールを送信する場合，必要がある場合を除き他の送信先の電子メールアドレスがわからないように（ＢＢＣに入力）しなければならない。

④ メールアドレス保有者は，重要な電子メールを誤送信した場合，情報管理者に報告しなければならない。

⑤ 職員等情報取扱者は、インターネット上で利用できる電子メールやファイルストレージ等において、個人アカウント等を用いて利用してはならない。

(チ)電子署名・暗号化

① 職員等情報取扱者は、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、情報セキュリティ管理者が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

② 職員等情報取扱者は、暗号化を行う場合に情報セキュリティ管理者が定める以外の方法を用いてはならない。また、情報セキュリティ管理者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。

③ 情報セキュリティ管理者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(ツ)無許可ソフトウェアの導入等の禁止

① 職員等情報取扱者は，各自に提供された端末に対して情報基盤管理者が定めるもの以外のソフトウェアの導入を行ってはならない。

② 業務を円滑に遂行するために必要なソフトウェアについては，情報基盤管理者の許可を得た場合に限り，利用することができる。

③ 職員等情報取扱者は，不正にコピーしたソフトウェア及び個人所有のソフトウ

ェアを導入又は使用してはならない。

(テ)機器構成の変更の制限

職員等情報取扱者は、ネットワーク及び各自に供与された端末等に対して、端末及びその他機器の接続、増設又は改造を行ってはならない。軽微な機器の増設の場合は、情報基盤管理者及び情報管理者等権限のある者の許可を必要とする。

(ト)無許可でのネットワーク接続の禁止

職員等情報取扱者は、情報基盤管理者及び情報管理者等権限のある者の許可なく端末等をネットワークに接続してはならない。

(ナ)利用可能なネットワークプロトコル

職員等情報取扱者が利用できるネットワークプロトコルは、業務上必要最低限のものとする。

(ニ)業務以外の目的での Web サイト閲覧の禁止

① 職員等情報取扱者は、業務以外の目的で Web サイトを閲覧してはならない。

② 情報基盤管理者は、職員等情報取扱者のウェブ利用について、明らかに業務に関係のない Web サイトを閲覧していることを発見した場合は、情報管理者に通知し、適正な措置を求めなければならない。

（2）アクセス制御

(ア)アクセス制御等

情報基盤管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

(イ)利用者 ID の取扱い

① 情報基盤管理者は、ネットワーク又はシステムに権限がない職員等がアクセスすることが不可能となるように、利用者の識別及び認証等適正な対応を行わなければならない。

② 情報基盤管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者 ID の取扱い等については適切な方法を定めなければならない。

③ 情報基盤管理者は、利用されていない ID が放置されないよう、定期的に点検しなければならない。

④ 情報基盤管理者は、ID に割り当てているアクセス権の正当性を確保するよう、

定期的に点検しなければならない。

(ウ)管理者権限の取扱い

情報基盤管理者は、所管する情報システムの管理者権限を持つ ID（以下「特権 ID」という）の扱いについて、以下に掲げる事項を遵守しなければならない。

① 情報基盤管理者は、特権 ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

② 情報基盤管理者は、特権 ID 及びパスワードの変更について、原則として外部委託事業者に行わせてはならない。

③ 情報基盤管理者は、特権 ID 及びパスワードについて、職員等情報取扱者の端末等のパスワードと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

④ 情報基盤管理者は、特権 ID の利用者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

⑤ 情報基盤管理者は、特権 ID は初期設定以外のものに変更しなければならない。

(エ)外部からのアクセス

① 情報基盤管理者は、外部からのアクセスを許可する場合、合理的理由を有する必要最低限のものに限定しなければならない。

② 情報基盤管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

③ 情報基盤管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

④ 情報基盤管理者は、外部からのアクセスに利用するモバイル端末を職員等情報取扱者に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑤ 情報基盤管理者は、執務区域外のネットワークから執務区域内のネットワークへのアクセスに公衆通信回線（公衆無線 LAN 等）を利用することを原則禁止しなければならない。

(オ)内部ネットワーク間の接続

情報基盤管理者は、他の内部ネットワークとの接続については、あらかじめ接続先の内部ネットワークの管理者と協議し、以下の内容を確認したうえで、接続しなければならない。

① 接続によりそれぞれの情報資産に影響が生じないこと

② 接続した場合のそれぞれの情報システムの責任範囲
③ 障害発生時の対応体制

(カ)自動識別の設定

情報基盤管理者及び業務システム管理者は、内部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必要に応じてシステムを設定するものとする。

(キ)ログイン試行回数の制限等

情報基盤管理者は、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持たない職員等が利用できないようにシステムを設定しなければならない。

(ク)認証情報の管理

① 情報基盤管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報を不正利用から保護するため、認証情報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。
② 職員等情報取扱者のパスワードを発行する場合において、仮のパスワードを発行する場合、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。
③ 情報基盤管理者は、仮のパスワードも含めパスワードを発行する場合、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としなければならない。
④ 情報基盤管理者は、特権 ID のパスワードを定期的（おおむね 6 か月以内）又はアクセス回数に基づいて変更し、古いパスワードを再利用しないものとする。
⑤ 情報基盤管理者は、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）システム開発・導入・保守等

(ア)情報システムの調達

情報基盤管理者は、機器及びソフトウェアの調達にあたり、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(イ)情報システムの開発・導入・保守等

情報基盤管理者は、情報システムの開発・導入・テスト・保守等を行うにあたり、次に掲げる事項を遵守しなければならない。

① 責任者及び監督者を定めなければならない。
② 開発・保守に関する仕様書等の成果物を適切に管理しなければならない。

③　適切なアクセス制限が設定できることを確認しなければならない。
④　導入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

上記以外に、市の情報セキュリティ対策基準に記載されているシステム開発・導入・保守等に関する規定を可能な限り考慮すること。

（４）不正プログラム対策

(ア)情報基盤管理者等の措置事項

情報基盤管理者及び情報管理者は、必要に応じて、次の事項を措置しなければならない。

①　所管するサーバ及び端末に，コンピュータウィルス等対策ソフトウェアを常駐させなければならない。
②　情報システムにおいてＵＳＢメモリ等の電磁的記録媒体を使用する場合，財団が管理しているものを職員等情報取扱者に使用させるとともに，当該媒体の使用にあたり，ウィルスチェックを行わせなければならない。
③　コンピュータウィルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たなければならない。インターネットに接続していないシステムにおいても、定期的に当該ソフトウェア及び定義ファイルの更新を実施しなければならない。
④　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原則として利用してはならない。
⑤　コンピュータウィルス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)職員等情報取扱者の遵守事項

職員等情報取扱者は，次の事項を遵守しなければならない。

①　端末において，コンピュータウィルス等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ない。
②　端末において，コンピュータウィルス等対策ソフトウェアが導入されている場合は，当該ソフトウェア及びウィルス定義情報を常に最新バージョンに保つ。
③　外部ネットワーク及びＵＳＢメモリ等の電磁的記録媒体からデータ又はソフトウェアを取り入れる際には，必ずコンピュータウィルス等対策ソフトウェアによるチェックを行う。
④　外部ネットワーク及びＵＳＢメモリ等の電磁的記録媒体へデータ又はソフトウ

ェアを送信・書き込みする際には，必ずコンピュータウィルス等対策ソフトウェアによるチェックを行う。

⑤ 差出人が不明な電子メール又は不自然なファイルが添付された電子メールを受信した場合は速やかに削除する。

⑥ 端末に対して，コンピュータウィルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

⑦ 情報セキュリティ管理者が提供するコンピュータウィルス等の情報を常に確認する。

⑧ 添付ファイルのあるメールを送受信する場合は，コンピュータウィルス等対策ソフトウェアでチェックを行う。

⑨ コンピュータウィルス等に感染した場合は，速やかに情報管理者に報告するとともに、その指示に従い、ＬＡＮケーブルの即時取り外し又は機器の電源遮断を行う等、他への感染を防止する措置を講じる。

⑩ 端末には、業務に必要なソフトウェアのみをインストールするとともに、端末に導入されているソフトウェアについて、情報管理者等から最新版へのアップデートの指示等があったときは、速やかにその指示に従う。

(ウ)専門家の支援体制

情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、コンピュータウィルス等対策ソフトのサポート契約を締結する等、外部の専門家の支援を受けられるようにしておかなければならない。

（５）不正アクセス対策

(ア)使用されていないポートの閉鎖等

情報基盤管理者は、所管するシステムにおいて、不正なアクセスによる影響を防止するため、以下の事項を措置しなければならない。

① 使用されていないポートを閉鎖しなければならない。

② 不要なサービスについて、機能を削除又は停止しなければならない。

③ 不正アクセスによるデータの書換えを検出する等、Web サイトの改ざんを防止しなければならない。

④ ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用しなければならない。

⑤ 不正アクセスの監視、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。

(イ)攻撃への対処

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、市と連絡を密にして情報の収集に努めなければならない。

(ウ)記録の保存

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。

(エ)内部からの攻撃

情報基盤管理者は、職員等情報取扱者及び外部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。

(オ)職員等情報取扱者による不正アクセス

情報基盤管理者は、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部署の情報管理者に通知し、適正な処置を求めなければならない。

(カ)サービス不能攻撃

情報基盤管理者は、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。

(キ)標的型攻撃

情報基盤管理者は、標的型攻撃情報システムにおいて、標的型攻撃による内部への侵入を防止するために、研修・啓発や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（6）セキュリティ情報の収集

(ア)セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

情報セキュリティ管理者は、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。

(イ)不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

(ウ)情報セキュリティに関する情報の収集及び共有

情報セキュリティ管理者は、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を速やかに講じなければならない。

９．運用面のセキュリティ

（１）情報システムの監視

① 情報基盤管理者は、セキュリティに関する事案を検知するため、情報システムを適時監視しなければならない。

② 情報基盤管理者は、重要なログ等を取得するサーバの正確な時刻設定又は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。

③ 情報基盤管理者は、外部と常時接続するシステムを適時監視しなければならない。

（２）情報セキュリティポリシー等の遵守状況の確認

(ア)遵守状況の確認及び対処

① 情報管理者は，所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い，問題を認めた場合に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。

② 情報セキュリティ管理者は，発生した問題について、適切かつ速やかに対処しなければならない。

③ 情報基盤管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシー及びこれに基づく文書の遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

(イ)端末、モバイル端末及び電磁的記録媒体等の利用状況調査

情報基盤管理者は、不正アクセス、不正プログラム等の調査のために、職員等情報取扱者が使用している端末、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(ウ)職員等情報取扱者の報告義務

① 職員等情報取扱者は、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、直ちに情報管理者に報告を行わなければならない。

② 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情報セキュリティ責任者が判断した場合は、職員等情報取扱者は、緊急時対応手順書に従って適切に対処しなければならない。

（３）管理者権限の代行

情報基盤管理者，情報管理者の権限を代行する者は，それぞれが指名する。

（４）侵害時の対応等

(ア)情報セキュリティ事件・事故等発生時の対応手順書の策定

情報セキュリティ責任者は、情報セキュリティ事件・事故、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、情報セキュリティ事件・事故等発生時の対応手順書を定めておき、セキュリティ侵害時には当該手順書に従って適正に対処しなければならない。

(イ)情報セキュリティ事件・事故等発生時の対応手順書に盛り込むべき内容

情報セキュリティ事件・事故等発生時の対応手順書には、以下の内容を定めなければならない。

① 緊急時連絡網

② 意思決定の所在

③ 発生した事案に係る報告すべき事項

④ 発生した事案への対応措置

⑤ 再発防止策の策定

(ウ)緊急連絡網に盛り込むべき内容

緊急時の連絡先（所属、役職、電話番号、電子メールアドレス等）及び連絡順序がわかるように記載する。財団内部や委託先だけでなく、警察・関係機関も記載されていることが望ましい。

(エ)情報セキュリティ事件・事故等発生時の対応手順書の見直し

情報セキュリティ責任者は、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、必要に応じて情報セキュリティ事件・事故等発生時の対応手順書の規定を見直さなければならない。

（５）例外措置

(ア)例外措置の許可

情報基盤管理者及び情報管理者は、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、業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、情報セキュリティ責任者の許可を得て、例外措置を講じることができる。なお、情報セキュリティ管理者が、軽微な例外措置と判断したものについては、当該管理者の許可により、例外措置を講じることができる。

(イ)緊急時の例外措置

情報基盤管理者は、前項に該当する場合であって、業務の遂行に緊急を要し、前項に定める許可を得る時間的な猶予のないときは、例外措置を実施し、実施後速やかに情報セキュリティ責任者に報告しなければならない。

(ウ)例外措置の記録管理

情報セキュリティ責任者は、許可した例外措置の内容及び方法について、適切に記録及び管理しなければならない。

（６）法令遵守

職員等情報取扱者は，職務の遂行において使用する情報資産を保護するために，次の法令等を遵守しこれに従わなければならない。

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）
② 著作権法（昭和４５年法律第４８号）
③ 個人情報の保護に関する法律（平成１５年法律第５７号）
④ サイバーセキュリティ基本法（平成２６年法律第１０４号）
⑤ 財団法人神戸市産業振興財団就業規則
⑥ 財団法人神戸市産業振興財団嘱託の就業に関する要綱
⑦ 財団法人神戸市産業振興財団短期雇用職員の就業に関する要綱
⑧ 財団法人神戸市産業振興財団個人情報保護規程
⑨ 財団法人神戸市産業振興財団文書取扱規程

（７）懲戒処分

(ア)懲戒処分

職員等情報取扱者が，情報セキュリティポリシー及びこれに基づく文書に違反した場合は，その重大性，発生した事案の状況に応じて別に定める懲戒処分等の対象とす

る。

なお，派遣労働者及び出向職員並びに業務委嘱者が，情報セキュリティポリシー及びこれに基づく文書に違反した場合の対応については，予め契約等に定めておかなければならない。

(イ)再発防止の指導等

職員等情報取扱者に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には，情報管理者は速やかに次の措置を講じなければならない。

① 再発防止の指導その他適切な措置

当該職員等情報取扱者に対して違反する行為の事実を通知し，再発防止の指導その他適切な措置を行う。

② 使用権の停止・剥奪

指導等によっても改善されない場合、当該職員等の情報資産の使用権を停止あるいは剥奪する。

③ 報告

違反する行為が生じた場合，違反する行為の内容，指導内容その他措置の状況について情報セキュリティ管理者に報告する。

１０．外部サービスの利用

（１）外部委託

(ア)外部委託業者の選定基準

特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、委託先の選定にあたり、委託内容に応じた情報セキュリティ対策の実施が確保されることを確認しなければならない。

(イ)契約書の記載事項

特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、当該委託先事業者との間で、下記事項を明記した契約を締結しなければならない。

① データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項

② 第三者への委託（以下、「再委託」という）の禁止又は制限に関する事項

③ データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項

④ データ等の複写及び複製の禁止に関する事項

⑤　データ等の取り扱いに関する事故の発生時における報告義務に関する事項
⑥　データ等の取り扱いに関する財団による検査の実施に関する事項
⑦　契約に違反した場合における契約の解除及び損害賠償に関する事項
⑧　委託業務終了時の情報資産の返還、廃棄等に関する事項
⑨　情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項
⑩　事故時等の公表に関する事項
⑪　委託先の責任者、委託内容、従事者 の所属 、作業場所の特定に関する事項
⑫　委託先の責任者及び従事者に対する研修の実施に関する事項
⑬　情報セキュリティ確保への取り組みの実施状況に係る報告義務に関する事項

また、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。
⑭　提供されるサービスレベルの保証に関する事項
⑮　委託業務の定期報告及び緊急時報告義務に関する事項
⑯　外部施設等への情報資産の搬送時における紛失、盗難、不正コピー等の防止に関する事項

(ウ)確認・措置等
情報基盤管理者は、契約締結後においても、当該委託先事業者の情報セキュリティ確保への取組みの実施状況等について、定期的若しくは随時、調査を行い、安全を確保しなければならない。情報セキュリティ責任者から内容の報告を求められた場合には、報告を行わなければならない。

(エ)再委託等
再委託（再々委託を含む）を受ける事業者がある場合、本項（イ）及び本項（ウ）に定める事項は再委託（再々委託を含む）を受ける事業者にも適用する。

（２）約款による外部サービスの利用
利用規約等に同意して利用する外部サービス（民間事業者等が規定した約款に基づき、インターネット上で提供される情報処理サービスの内、１０．（４）に規定するクラウドサービスを除く）では、機密性２の情報を扱ってはならない。

（３）ソーシャルメディアサービス又はソーシャルネットワーキングサービスの利用
ソーシャルメディアサービス又はソーシャルネットワーキングサービスの利用にあたっては、次に掲げる事項を遵守しなければならない。
①　本財団のアカウントによる情報発信が、実際の本財団のものであることを明らかにするために、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(IC カード等）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 機密性 2 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。

④ アカウントの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）クラウドサービスの利用

① 情報基盤管理者は、クラウドサービス（民間事業者が提供するものに限らず、市が提供するもの等を含む。以下同じ。）を利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。

② 情報基盤管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して事業者を選定し、必要に応じて実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

③ 情報基盤管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し事業者を選定する際の要件としなければならない。

④ 情報基盤管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス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セキュリティ要件を定めなければならない。

⑤ 情報基盤管理者は、クラウドサービスに対する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、クラウドサービス及び当該サービス提供事業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。

１１．評価・改善・見直し

（1）監査

(ア)実施方法

情報セキュリティ責任者は、情報セキュリティ監査責任者に命じ、情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

(イ)監査を行う者の条件

① 情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

② 監査を行う者は、必要に応じ、監査及び情報セキュリティに関する専門知識を有

する専門家から助言を受けることができる。

(ウ)監査実施計画の立案及び実施への協力

① 情報セキュリティ監査責任者は、監査を行うに当たって、監査実施計画を策定し、情報セキュリティ責任者に報告しなければならない。

② 被監査部門は、監査の実施に協力しなければならない。

(エ)外部委託事業者に対する監査

情報セキュリティ監査統括責任者は、委託先事業者に対して、委託先事業者からの再委託（再々委託を含む）の事業者も含めて、情報セキュリティポリシーの遵守について、必要に応じて、監査を行わなければならない。

(オ)報告

情報セキュリティ監査責任者は、監査結果を取りまとめ、情報セキュリティ責任者に報告しなければならない。

(カ)保管

情報セキュリティ監査責任者は、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。

(キ)監査結果への対応

情報セキュリティ責任者は、監査結果を踏まえ、指摘事項に関係する情報管理者等に対し、当該事項への対処を指示しなければならない。また、指摘事項に関係しない情報管理者等に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、財団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。

(ク)情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ責任者は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

（2）自己点検

(ア)実施方法

情報管理者は，所管する所属の情報セキュリティ対策状況について，定期的及び必要

に応じて自己点検を行わなければならない。

(イ)自己点検結果等の報告

① 情報管理者は，自己点検結果と自己点検結果に基づく改善策を取りまとめ，情報セキュリティ管理者に報告しなければならない。

② 情報セキュリティ管理者は、報告を受けた点検結果及び改善策を情報セキュリティ責任者に報告しなければならない。

(ウ)自己点検結果の活用

① 職員等情報取扱者は，自己点検の結果に基づき，自己の権限の範囲内で改善を図らなければならない。

② 情報セキュリティ責任者は，情報セキュリティポリシー等情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

(エ)改善

① 是正措置

情報管理者は，業務上発見された問題，企業・個人からの指摘による問題，自己点検において指摘された問題等に対する再発防止のため，その原因を除去するための措置を施さなければならない。

② 予防措置

情報管理者，情報セキュリティ管理者は，業務上予見される問題，他の組織で発生したものと同種の情報セキュリティ事件・事故及び自己点検において指摘されうる問題等の発生を未然に防止するため，その原因を除去するための措置を施さなければならない。

（3）情報セキュリティポリシーの見直し

情報セキュリティ責任者は，自己点検の結果，改善の状況，情報セキュリティに関する状況の変化等を踏まえ，情報セキュリティポリシーに対して必要があると認めた場合その見直しを行う。

（4）情報セキュリティ個別基準の策定

情報セキュリティ責任者は，情報セキュリティポリシーを補完するために必要な本財団共通の事項に関して、具体的な内容を定めた情報セキュリティ個別基準を策定する。

附則

　この情報セキュリティポリシーは，平成２１年１２月１日から施行する。

附則

　この情報セキュリティポリシーは，平成２３年４月１日から施行する。

附則

　この情報セキュリティポリシーは，令和３年５月１日から施行する。