堺市情報セキュリティ対策基準要綱（平成１５年制定・市長決裁要綱）

目次

第１章　総則

（趣旨）

第１条　この要綱は、堺市電子計算機管理運用規程（平成１５年庁達第２号。以下「規程」という。）第７条第１項の規定に基づき、本市における情報資産に関する情報セキュリティ対策基準（以下「対策基準」という。）について必要な事項を定める。

（定義）

第２条　この要綱において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) パスワード　正当な利用者であることを認証するために使用される文字列情報をいう。

(2) アクセス　コンピュータ、ネットワーク及び情報システムを通じて、データの参照、変更等を行うことをいう。

(3) バックアップ　ソフトウェア又はデータの滅失又は毀損に備えたこれらの複製をとることをいう。

(4) 不正プログラム　コンピュータに侵入し、情報システムの正常な動作を意図的に妨げるプログラムをいう。

(5) サーバ　ネットワーク上で、データの共有、印字出力、通信制御等のサービスを端末機等に対して提供するコンピュータをいう。

(6) システム利用課　情報システムを利用している課をいう。

(7) ＩＤ　情報システムを利用する正当な利用者であることを識別するために使用される文字列情報をいう。

(8) 情報セキュリティインシデント　情報システムの停止等、サイバー攻撃及び情報の盗難、紛失、漏えい等をいう。

(9) 標的型攻撃　特定の組織内の情報を改ざんし、窃取し、又は不正に削除するという意思を持った者が、当該組織の構成員に対し不正プログラムを添付した電子メールを送るなどの方法により、当該情報の改ざん、窃取又は不正な削除を行うことをいう。

(10) 個人番号　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。以下「番号法」という。）第２条第５項に規定する個人番号をいう。

(11) 特定個人情報ファイル　番号法第２条第９項に規定する特定個人情報ファイルをいう。

(12) 個人番号利用事務　番号法第２条第１０項に規定する個人番号利用事務をいう。

(13) 個人番号関係事務　番号法第２条第１１項に規定する個人番号関係事務をいう。

２　前項に掲げるもののほか、この要綱において使用する用語の意義は、規程の定めるところによる。

第２章　管理体制

（総括電算管理者）

第３条　総括電算管理者は、電子計算機、電子計算機室等並びにデータ及びドキュメントの管理状況を把握するために必要と認める事項について、次条第１項に規定する電算管理者又は第５条第１項に規定するデータ管理者から報告させ、又は実地に調査することができる。この場合において、総括電算管理者は、報告又は調査の結果、必要と認めるときは、規程第３条第３項の事務について必要な措置を講ずるよう命ずることができる。

（電算管理者）

第４条　システム設置課における電子計算機、電子計算機室等を適正に管理するため、電算管理者を置き、システム設置課長の職にある者をもってこれに充てる。
２　電算管理者は、規程第７条第２項の実施手順（以下単に「実施手順」という。）を策定し、情報セキュリティに係る対策を行うとともに、情報システムを使用する職員等が常に実施手順を閲覧できるよう必要な措置を講ずるものとする。
３　電算管理者は、情報セキュリティポリシー及び実施手順の遵守状況を適宜点検し、これらの実効性が保たれるよう必要な措置を講ずるものとする。
（データ管理者）
第５条　業務所管課においてデータ及びドキュメント（以下これらを「データ等」という。）の保護及び管理を行うため、データ管理者を置き、業務所管課長の職にある者をもってこれに充てる。
２　データ管理者は、データ等を利用する者に情報セキュリティポリシー及び電算管理者が定める実施手順を理解させるとともに、常にこれらを遵守させ、情報セキュリティについて問題が生じないよう管理し、及び指導するものとする。
（システム利用責任者）
第６条　システム利用課において端末機及びサーバの適正な管理及び効率的な運用を行うため、システム利用責任者を置き、システム利用課の長の職にある者をもってこれに充てる。
２　システム利用責任者は、その所掌に属する課室等（これに準ずる組織等を含む。）の職員等に、第１３条に規定する職員等の責務について理解させ、及び遵守させるものとする。
３　システム利用責任者は、その所掌に属する情報資産が侵害され、又はそのおそれがあると認めるときは、電算管理者へ速やかに報告を行うとともに、その指示を受けなければならない。
（情報セキュリティ主任）
第６条の２　システム利用責任者を補佐させるため、システム利用課に情報セキュリティ主任を置き、当該システム利用課の長を補佐する職にある者（当該職を置かない組織にあっては課長補佐級の職員のうちから、課長補佐級の職員を置かない組織にあっては係長級の職員のうちから、それぞれシステム利用責任者が指定する者とする。）をもってこれに充てる。
（情報の分類）
第７条　電算管理者、データ管理者及びシステム利用責任者は、情報システムにおける情報資産の適正な運用を確保するため、重要性を踏まえて次の区分により分類し、その重要度に応じた情報セキュリティ対策を講ずるものとする。
(1) 情報セキュリティの侵害により、市民の生命、財産、プライバシー等へ重大な影響を及ぼす情報（個人情報及び業務上必要とする最小限の者のみが扱う情報（極秘の情報を含む。））
(2) 情報セキュリティの侵害により、事務の執行に重大な影響を及ぼす情報（公開することを予定していない情報）
(3) 情報セキュリティの侵害により、事務の執行に影響を及ぼす情報（外部に公開する情報のうち業務上不可欠な情報）
(4) 前３号に掲げる情報以外の情報
（情報セキュリティに関する統一的な窓口）
第７条の２　情報セキュリティに関する統一的な窓口（規程第３条の２に規定するものをいう。以下同じ。）は、最高情報セキュリティ責任者により決定された情報セキュリティに係る重要な事項を電算管理者等の関係者に通知するものとする。
２　情報セキュリティに関する統一的な窓口は、情報セキュリティに関して、関係機関及び他の地方公共団体における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組織等と情報共有を行うものとする。
３　情報セキュリティに関する統一的な窓口は、前項の規定により共有する情報のほか、情報セキュリティに関する情報を収集し、必要に応じて情報セキュリティを確保するための対応方法等について電算管理者等の関係者に通知するものとする。
４　情報セキュリティに関する統一的な窓口は、情報セキュリティインシデントが発生したときは、第１５条第４項及び第６項に定めるもののほか、その対応において中心的な役割を果たすものとする。
（兼務の禁止）

第７条の３　情報セキュリティを確保するための対策を実施するに当たり、当該対策に係る措置について、承認又は許可を必要とする行為がある場合において、当該承認又は許可の申請を行う者と当該承認又は許可を行う者とは、同じ者であってはならない。ただし、特別の事情がある場合は、この限りでない。

第３章　物理的セキュリティ

（記録媒体の管理）

第８条　情報システムに係る記録媒体の管理については、次のとおり行うものとする。

(1) 情報システムにおいて取り扱う情報については、第三者がその重要性を容易に識別することができないよう留意の上、記録媒体に記録された情報の分類がわかるように表示をするなど適切な管理を行うものとする。

(2) 第７条第１号又は第２号の規定に該当する情報（以下「重要な情報」という。）を記録した記録媒体については、その重要度に応じて、漏洩、盗難、滅失、損傷等の防止に備えるなど適切な対策を講じた場所に保管しなければならない。

(3) 記録媒体に記録した情報については、保存する必要がなくなった時点で速やかに消去しなければならない。

(4) 不要となった記録媒体を廃棄する場合は、データ管理者の許可を得なければならない。この場合において、不要となった記録媒体については、当該媒体に含まれる情報をいかなる方法によっても復元することが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。

(5) 重要な情報を記録した記録媒体の廃棄については、その重要度に応じて、日時、処理担当者及び処理内容を記録するなど適切な処理を行わなければならない。

(6) 情報を記録した記録媒体を長期間保管する場合は、書込禁止の措置を講じなければならない。この場合において、その情報に重要な情報が含まれるときは、パスワードの設定等の措置を併せて講じなければならない。

(7) 重要な情報を記録した記録媒体を執務室外に持ち出す場合は、データ管理者の許可を得るとともに、重要な情報を記録した記録媒体については、暗号化、パスワードの設定その他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。

（サーバの導入及び運用）

第９条　サーバの導入及び運用に当たっては、次に掲げる措置を講ずるものとする。

(1) サーバは、火災、水害、ほこり、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なければならない。

(2) サーバの設置は、これを容易に取り外せないよう、適切な固定を行うなど必要な措置を講じなければならない。

(3) 重要な情報を格納しているサーバについては、二重化（サーバの停止、故障等に備えて、システムを継続して運用できるような構成をとることをいう。）するなど、障害発生時に情報システムの運用に支障が生じないようにしなければならない。

(4) 操作の権限を有しない者に容易に操作されることがないよう、サーバに記録された情報の重要度に応じて設置場所への入室制限を行うなど適切な措置を講じなければならない。

(5) サーバその他の機器の電源については、サーバに記録された情報の重要度に応じて、予備電源の設置その他落雷、電圧又は周波数の変動等の障害に対する措置を講じなければならない。

(6) サーバの配線については、損傷等が発生しないよう、可能な限り必要な措置を講じ、主要な配線については、損傷等について定期的な点検を行わなければならない。

(7) 無線系のネットワークを使用する場合については、セキュリティの保護について当該ネットワークの性質に配慮した措置を講じなければならない。

（端末機及びサーバの管理）

第１０条　システム利用責任者は、執務室等に職員等がいない場合における当該執務室等の施錠等の徹底、端末機、サーバ等の固定その他情報資産の盗難防止のための措置を講じなければならない。

２　電算管理者は、許可された記録媒体又は機器以外のものについて、端末機、サーバ等への接続を制限する措置を講じなければならない。

（管理区域）

第１１条　電算管理者は、特に重要な情報システムの設置及び運用を行うための部屋（以下「情報システム室」という。）について、次の事項に配慮しなければならない。
(1) 水害対策及び確実な入退室管理を行うこと。
(2) 情報システム室内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を講ずること。
(3) 情報システム室内に設置する消火剤は、機器及び記録媒体に影響を与えるものでないこと。
(4) 情報システム室内への機器等の搬入又は搬出の際には、職員等が同行する等の必要な措置を講ずること。
(5) 情報システム室に入室する者には、身分を証明できるものを携帯させ、当該職員の求めに応じ、これを提示させること。

（ネットワーク）

第１２条　電算管理者は、情報システムに電気通信事業者の提供する通信回線を接続する場合は、当該情報システムにおいて取り扱う情報資産の重要度に応じて、情報セキュリティの水準を検討の上、適切な通信回線を選択しなければならない。
２　電算管理者は、通信回線を使用する場合は、データの破壊、盗聴、改ざん等が生じないように、十分な情報セキュリティ対策を講じなければならない。

第４章　人的セキュリティ

（職員等の責務）

第１３条　職員等は、情報セキュリティに関連する法令等を遵守の上、情報資産を使用しなければならない。
２　職員等は、業務目的以外での情報資産の執務室外への持出し、情報システムへのアクセス、電子メールの利用及びインターネットへのアクセスを行ってはならない。
３　職員等は、情報システムの管理及び運用に当たり、次の事項を遵守しなければならない。
(1) 使用する端末機及び記録媒体について、許可されたもの以外を第三者に使用されることがないよう管理すること。
(2) 許可なく、第三者に情報を閲覧されることがないよう、必要な措置を講ずること。
(3) 電算管理者の許可を得ず、情報システム又は情報システムで扱う機器を執務室外に持ち出さないこと。
(4) データ管理者の許可を得ず、データ等を執務室外に持ち出さないこと。
(5) 職員等個人が所有する電子計算機、周辺機器及び記録媒体並びにソフトウェアを業務で使用しないこと。
(6) 電算管理者の許可を得ず、ソフトウェアの導入及び機器構成の変更を行わないこと。
(7) ライセンス違反又は著作権法違反となる不正に複製等をしたソフトウェアを使用しないこと。
(8) 端末機及びサーバの操作は、電算管理者が定める運用時間内に行うこと。
(9) 操作を許可された者以外に端末機若しくはサーバの操作方法を教示し、又は端末機若しくはサーバの操作をさせないこと。
(10)磁気カード及びＩＣカードの管理に関し、セキュリティに配慮した適切な管理及び運用を行うこと。
(11)電算管理者の許可を得ず、インターネットで利用できるフリーメール、ネットワークストレージサービス等を使用しないこと。
(12)職員等は、異動、退職等により業務を離れる場合には、当該業務上知り得た情報を漏らさないこと。
(13)データ管理者の許可を得ず、端末機に内蔵された磁気記録装置に、重要な情報を保存しないこと。
(14)データ管理者の許可を得ず、及び電子署名、暗号化、パスワード設定等の措置を講ずることなく、外部に重要な情報を提供し、又は送信しないこと。
４　職員等は、ＩＤ及びパスワードの取扱いに当たり、次の事項を遵守しなければならない。
(1) 他人に自己の保有するＩＤを使用させないこと。
(2) 自己の保有するパスワードに関し、他に知られないよう適切な管理を行うこと。
(3) パスワードは、十分な長さのもので第三者が想像しにくいものとすること。

(4) パスワードは、定期的に変更すること。
(5) 端末機及びサーバにパスワードを記憶させないこと。
5　職員等は、電子メールの利用に当たり、次の事項を遵守しなければならない。
(1) 自動転送機能を用いて電子メールを転送しないこと。ただし、特別の事情がある場合は、この限りでない。
(2) 業務上必要のない送信先に、電子メールを送信しないこと。
(3) 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、他の送信先の電子メールアドレスが分からないようにすること。
(4) 差出人が不明である場合又は不自然に添付されたファイルを受信した場合は、添付ファイルや本文中のリンク先を開かず、その旨を直ちに電算管理者に連絡すること。
6　職員等は、情報システムに組み込まれていない電子計算機を使用する場合についても、前３項各号に規定する事項を遵守しなければならない。
7　電算管理者は、職員等に対し第３項から第５項までの各号に規定する事項を遵守させるために必要な措置を講じなければならない。
8　電算管理者は、災害発生時の業務継続又はシステムの障害に対する処理のため緊急かつやむを得ない場合その他市長が特に必要と認める場合については、第３項第５号、第８号及び第１１号の規定の適用を除外することができる。
9　電算管理者は、執務室外への持出し又は執務室外からの持込みを許可した情報システムで扱う端末機について、記録を作成し、及び保管しなければならない。
１０　データ管理者は、執務室外への持出し又は執務室外からの持込みを許可した情報システムで扱う記録媒体について、記録を作成し、及び保管しなければならない。
１１　データ管理者は、電子メールによる重要な情報の送信を許可しようとする場合は、当該情報の特性等を勘案し、電子メールによる送信の要否を適切に判断しなければならない。
１２　市長は、情報セキュリティポリシー又は実施手順に違反した職員について、その重大性、発生した事案の状況等に応じて懲戒処分等の対象とするものとする。
（教育及び訓練）
第１４条　総括電算管理者は、職員等に対し、その役割に応じた情報セキュリティポリシーに関する研修を実施しなければならない。
2　職員等は、定められた研修に参加し、情報セキュリティポリシーを理解し、情報セキュリティ上の問題を生じさせないようにしなければならない。
3　電算管理者は、必要に応じて緊急時の対応を想定した訓練を実施しなければならない。
（情報セキュリティインシデント等への対応）
第１５条　緊急時対応計画については、情報システムごとに実施手順において定めるものとする。
2　情報セキュリティインシデントが発生していると認めた職員等は、当該事象について速やかに電算管理者に報告しなければならない。
3　電算管理者は、前項の規定による報告を受けたときは、当該事象について速やかに情報セキュリティに関する統一的な窓口に報告しなければならない。
4　情報セキュリティに関する統一的な窓口は、情報セキュリティインシデントについて電算管理者から報告を受けた場合は、速やかに総括電算管理者へ報告するものとする。この場合において、情報セキュリティに関する統一的な窓口は、当該情報セキュリティインシデントの状況を把握し、及び分析した上で、被害の拡大の防止、情報資産の復旧、再発の防止等（以下「被害拡大防止等」という。）の必要な対策について、併せて総括電算管理者へ報告するものとする。
5　総括電算管理者は、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に関する統一的な窓口から報告を受けた場合は、当該事象について最高情報セキュリティ責任者に速やかに報告を行い、その指示その他必要に応じてその内容を確認し、被害拡大防止等に係る必要な措置を指示するものとする。
6　情報セキュリティに関する統一的な窓口は、総括電算管理者の指示に基づき、被害拡大防止等に係る必要な措置を電算管理者等の関係者に指示するものとする。
7　電算管理者は、情報セキュリティに関する統一的な窓口からの指示に基づき、情報資産の防護のために必要な被害拡大防止等の措置を講ずるものとする。
8　電算管理者は、不正なアクセスに対処するため、情報セキュリティに関する統一的な窓口と

連携し、次の措置を講ずるものとする。
(1) 外部から市のネットワークへ不正な侵入を受けることが明確な場合における、情報システムの停止その他必要な措置
(2) 前号の不正な侵入について、記録の保存に努めるとともに、警察その他の関係機関との緊密な連携に努める措置（前号の不正な侵入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）に違反しているなど犯罪の可能性がある場合に限る。）
９　職員等は、情報資産が不正プログラムに感染し、又は感染したおそれがある場合は、端末機又は記録媒体の利用を直ちに中止し、ネットワークケーブルを取り外すなど接続しているネットワークから端末機又は記録媒体を切り離さなければならない。
１０　市長は、職員による不正なアクセス又はその結果により、データの漏洩、破壊若しくは改ざん又はこれらを原因とするシステムダウン等により業務に深刻な影響をもたらした場合は、当該職員を懲戒処分等の対象とするものとする。

第５章　技術的セキュリティ

（電子計算機及びネットワークの管理）
第１６条　電算管理者は、重要な情報を扱う情報システムについて、次の措置を講じなければならない。
(1) 各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、不正なアクセス等に対処できるよう一定の期間保存し、及び記録の改ざん、窃取又は不正な削除の防止のために必要な措置を講ずること。
(2) システムの開発、変更等について、計画的に行うとともに、その記録を作成し、及びその窃取、改ざん等をされないように適切に管理すること。
(3) システムの障害に対する処理、問題等を障害記録として体系的に記録し、常に活用できるよう保存すること。
(4) サーバに記録された情報（システムを復旧するために必要な情報を含む。）について、情報の重要度に応じて期間を設定し、定期的にバックアップ用の複製をとり、必要に応じて分散管理を行うこと。
(5) 標的型攻撃による不正な侵入を防止するために、情報セキュリティに関する教育等の人的対策や出所不明の記録媒体を内部ネットワーク上の端末機等に接続させないなどの入口対策を行うこと。
(6) 不正に内部に侵入した標的型攻撃等を検知して対処するため、通信ログをチェックするなどの出口対策を行うこと。
２　データ管理者は、情報システムに組み込まれていない電子計算機（業務上のデータ等を保有するものに限る。）をインターネットに接続する場合には、十分な情報セキュリティ対策を講じなければならない。
（アクセス制御）
第１７条　電算管理者は、ネットワーク及び情報システムのアクセス制御について、次の措置を講じなければならない。
(1) 情報システムを利用する職員等について、情報システムごとに定められた方法に従い、その登録、変更、抹消等を行うこと。
(2) ＩＤ及びパスワードを厳重に管理し、利用されていないＩＤが放置されないよう点検するとともに、パスワードについては、定期変更等の対策を行うこと。
(3) 情報システムの管理に係る権限の付与は、必要最小限の者に限ることとし、厳重に管理すること。
(4) インターネット以外のネットワークについて、アクセスが可能なネットワーク及びネットワークサービスにアクセスできる者を定めること。
(5) 不必要なネットワークサービスにアクセスできないようにすること。
(6) 不正なアクセスを防止するため、適切なネットワーク経路制御を施すこと。
(7) 本市の外部の組織から本市のネットワーク及び情報システムにアクセスする場合は、直接本市の内部ネットワークに接続させないこと。
(8) 外部のネットワークとの接続に際し、当該外部のネットワークの構成、機器、セキュリティレベル等を詳細に検討し、本市の全てのネットワーク、情報システム及び情報資産に影響

が生じないことを確認した上で、情報セキュリティに留意したネットワークの構成を採ること。

(9) 外部のネットワークの瑕疵により本市のデータの漏洩、破壊、改ざん、システムダウンその他本市の業務に影響を及ぼす障害が発生した場合に対処するため、外部のネットワークについて管理責任を有する者との間で障害発生時の責任を明らかにしておくこと。

(10) 本市のネットワーク、情報システム又は情報資産に影響が生じるような問題が、接続した外部のネットワークに発生した場合は、総括電算管理者の指示に従い、直ちに当該外部のネットワークを物理的に遮断すること。

２　個人番号利用事務又は個人番号関係事務を行う場合、取り扱う特定個人情報ファイルを限定するため、必要に応じて、次の措置を講じなければならない。

(1) 個人番号によりアクセスできる情報の範囲を限定すること。

(2) 特定個人情報ファイルを取り扱う情報システムを限定すること。

(3) ＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を限定すること。

(4) 特定個人情報ファイルへのアクセス権を付与すべき者を必要最小限とすること。

(5) アクセス権を有する者に付与する権限を必要最小限とすること。

(6) 情報システムの管理に係る権限を有する者であっても、情報システムの管理において特定個人情報ファイルにアクセスする理由が明確でない場合は、特定個人情報ファイルへ直接アクセスできないようにすること。

第６章　運用

（ネットワーク及び情報システムの監視）

第１８条　電算管理者は、セキュリティに関する事案を検知するため、情報システムについて次の監視等を行わなければならない。

(1) 外部と常時接続するシステムの恒常的な監視

(2) 第７条第１号に規定する情報を扱うシステムについて、異常な運用等がなされないための監視

２　電算管理者は、前項に規定する監視により得られた情報については、消去し、又は改ざんされることがないよう、必要な措置を講ずるとともに、安全な場所に保管しなければならない。

３　電算管理者は、不正なアクセス、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機の各種アクセス記録、電子メールの送受信記録等を調査することができる。

（不正プログラム対策）

第１９条　職員等は、外部から取り入れ、又は外部へ持ち出すデータ、送受信する電子メール等については、不正プログラムチェック（当該データ等に不正プログラムが含まれているか否かを調べることをいう。次項及び第３項において同じ。）を行うなど、不正プログラムのシステムへの侵入又は外部への拡散その他不正プログラムによるシステム障害等の発生の防止に努めなければならない。

２　電算管理者は、常時不正プログラムに関する情報収集に努め、不正プログラムチェック用の定義ファイル等は常に最新のものに保たなければならない。

３　電算管理者は、不正プログラムチェックにより不正プログラムが検知された場合に備え、システムごとに適切な連絡体制を整えておかなければならない。

４　電算管理者は、端末機及びサーバに不正プログラム対策ソフトウェアを常駐させなければならない。

５　電算管理者は、業務で利用するソフトウェアにおいて、そ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。

（システムの開発、保守等）

第２０条　情報システムの開発又は保守をしようとする課の長は、事故及び不正行為の防止のため、次の事項を行わなければならない。

(1) 責任者及び管理者の配置

(2) 作業者及び作業範囲の設定

(3) 開発し、又は保守するシステムと運用システムとの分離

(4) 開発又は保守を外部に委託する場合に、それに関するソースコード（プログラム設計の元

データをいう。）の提出の要求
(5) 開発又は保守に際し、セキュリティ上問題となり得るおそれのある基本プログラム及びアプリケーションソフトの使用の禁止
(6) 開発又は保守の際のアクセスの制限
(7) 開発又は保守を外部に委託する場合に、作業に係る記録の提出の要求
(8) マニュアル等の定められた場所への保管
(9) 開発又は保守の終了後、不要となった開発又は保守を行った者のＩＤ及びパスワードの速やかな抹消
(10) 新たに導入するシステムについて、既に稼動しているシステムに接続する場合の十分な試験
(11) 廃棄又はリース会社に記録媒体の含まれる機器を返還する場合における、機器に含まれる記録媒体の内容のいかなる方法によっても復元不可能な消去
(12) 電子計算機の修理等の請負業者（その従業員を含む。）が当該修理等に伴い取得した情報について、第三者に漏洩しないことを誓約する旨の契約書への明記

（外部委託等）

第２１条　重要な情報を取り扱う情報システムの開発又は運用を委託しようとする課の長（以下この条において「委託課長」という。）は、当該委託に係る契約書に次の事項を明記し、かつ、その受託者に対して、情報セキュリティポリシー及びこれに関連する法令を遵守させるために必要な措置を講じなければならない。
(1) 委任又は下請負の禁止又は制限に関する事項
(2) 業務上知り得た事項に係る秘密保持に関する事項
(3) 個人情報、ドキュメントその他システムに係るデータの保護及び取扱いに関する事項
(4) 前３号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

２　委託課長は、重要な情報を取り扱う情報システムの開発又は運用を委託する場合であって、その受託者（次項及び第４項において単に「受託者」という。）が再委託契約を行うときは、再委託先について契約の履行能力を有するか否かについて確認しなければならない。

３　委託課長は、前項の規定による確認の結果、再委託先が契約の履行能力を有すると認めるときは、再委託について承諾するものとする。この場合において、委託課長は、受託者に対して、当該再委託先の管理及び監督に必要な措置を講じさせなければならない。

４　委託課長は、受託者及び再委託先において必要な情報セキュリティ対策が確保されていることを確認しなければならない。

５　派遣労働者に情報システムを利用した業務を行わせようとする課の長は、その労働者派遣契約に係る書面に次の事項を明記し、かつ、派遣労働者に対して、情報セキュリティポリシー及びこれに関連する法令を遵守させるために必要な措置を講じなければならない。
(1) 当該派遣労働者の情報セキュリティポリシーの遵守に関する事項
(2) 業務上知り得た事項に係る秘密保持に関する事項
(3) 前２号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

（端末機及びサーバに対する付加）

第２２条　システム利用責任者は、アプリケーションソフトを端末機又はサーバにおいて新たに使用することができるよう設定しようとする場合又は機器の増設交換その他システムに対する変更等が必要な場合は、次の事項をあらかじめ電算管理者と協議し、その承認を受けなければならない。
(1) 利用目的
(2) 接続機器及びソフトウェアの明細
(3) 設置場所
(4) 前３号に掲げるもののほか、情報システムの適正な運用を確保するために必要な事項

（その他の運用）

第２３条　次の各号に掲げる者は、情報システムの運用に当たり、当該各号に定める事項を講じなければならない。
(1) システム利用責任者　運用時間外に端末機又はサーバを操作しようとする際の電算管理者との事前協議

(2) 電算管理者　所管する電子計算機、端末機及びサーバについての情報システムの円滑な運用及び安全性確保のための定期的又は随時の保守及び点検並びに不正なアクセスに備えた情報収集
(3) 電子計算機を所管するデータ管理者　自らが所管する業務の円滑な運用及び安全性確保のための定期的又は随時のサーバ及び接続装置の保守及び点検
(4) 前条の規定により機器を接続したシステム利用責任者　当該機器の円滑な運用及び安全性確保のための定期的又は随時の機器及び接続装置の保守及び点検

第７章　見直し等

（監査）

第２４条　情報セキュリティ監査統括責任者は、十分な専門的知識を有する者をして情報セキュリティについての監査を定期的にさせなければならない。

２　前項の監査を実施する場合において、監査を受ける者と実施する者とは、同じ者であってはならない。ただし、特別の事情がある場合は、この限りでない。

３　監査を受ける課（これに準ずる組織を含む。）の長は、第１項の監査の結果に基づき、指摘事項への対処を実施しなければならない。

（情報セキュリティポリシーの見直し）

第２５条　市長は、情報セキュリティについて、新たな対策を講ずる必要が発生した場合又は技術の向上により更に安全な対策を講ずることが可能となった場合は、前条第１項の監査の結果又は点検の結果を踏まえ、情報セキュリティポリシーの見直しの内容、時期等についての決定を行うものとする。

附　則

この要綱は、平成１５年４月１日から施行する。

附　則

この要綱は、平成１７年３月１日から施行する。

附　則

この要綱は、平成１９年４月１日から施行する。

附　則

この要綱は、平成２３年４月１日から施行する。

附　則

この要綱は、平成２６年４月１日から施行する。

附　則

この要綱は、平成２７年１１月１１日から施行する。

附則

この要綱は、平成３０年９月１日から施行する。