（別紙４）

# 情報セキュリティに関する基本要綱

大阪府の情報セキュリティに関する基準（平成14年４月１日制定）の全部を改正する。

## 第１部　基本方針

（目的）

第１条　この要綱は、大阪府電子計算機、情報通信ネットワーク及び情報システム管理運用規程（平成８年大阪府訓令第38号。以下「管理運用規程」という。）第３条及び第６条並びに大阪府行政情報化推進基本要綱（以下「推進基本要綱」という。）第３条の規定に基づき、情報セキュリティを確保するために遵守すべき基本的事項を定める。

（定義）

第２条　この要綱における用語の意義は、管理運用規程及び推進基本要綱に定めるもののほか、次の各号に定めるところによる。

⑴　事業者　府との委託契約等により情報システム又は情報通信ネットワーク（以下「情報システム等」という。）の開発等を行う者をいう。

⑵　端末機　事務処理等を行うために職員や室課等に配備された電子計算機等をいう。

⑶　ＩＤ　情報システム等の利用者を識別するための文字列情報をいう。

⑷　パスワード　情報システム等の利用者がＩＤによる認証を得るため入力する文字列情報をいう。

⑸　不正アクセス　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）第２条第４項による不正アクセス行為をいう。

⑹　不正プログラム　情報システム等に対して不正かつ有害な動作を行う意図で作成されたプログラムをいう。

⑺　情報資産　情報及び情報の管理や運用を行う仕組みをいう。

⑻　情報セキュリティ　情報資産の機密性（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。）、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。）及び可用性（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。）を維持することをいう。

⑼　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）に関わる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。

⑽　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（個人番号利用事務系を除く。）。

⑾　インターネット接続系　個人番号利用事務系、ＬＧＷＡＮ接続系以外の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。

⑿　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。

⒀　無害化通信　危険因子を除去、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等、安全が確保された通信をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次の各号を想定する。

⑴　情報システム等の不正利用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

⑵　情報資産の無断持ち出し、情報システム等の設計・開発・運用・保守等の不備、情報システム等に関する内部・外部監査機能や委託管理の不備、機器故障等の非意図的な要因による情報

資産の漏えい・破壊・消去等
⑶　地震、落雷、火災等の災害による情報システム等の停止等
⑷　大規模・広範囲にわたる疾病による要員不足に伴う情報システム等の運用不全等
⑸　電力供給の途絶、通信の途絶、水道供給の途絶等による情報システム等の停止等

（適用範囲）
第４条　この要綱は、部局等に適用する。

（職員の遵守義務）
第５条　職員は、情報セキュリティ対策の重要性について共通の認識を持ち、業務の遂行に当たってはこの要綱を遵守しなければならない。

（情報セキュリティ対策）
第６条　第３条で想定する脅威から情報資産を保護するために、次の各号に掲げる対策を講じる。
⑴　組織体制　本府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。
⑵　情報資産の分類と管理　本府の保有する情報資産を重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。
⑶　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、次の対策を講じる。
イ　個人番号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等により、住民情報の流出を防ぐ。
ロ　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。
ハ　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導入等を実施する。
⑷　物理的セキュリティ対策　情報システム等が稼動する機器等の管理について、物理的な対策を講じる。
⑸　人的セキュリティ対策　情報セキュリティ対策に関し、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
⑹　技術的セキュリティ対策　不正アクセス対策等の技術的対策を講じる。
⑺　運用　情報システムの監視、この要綱の遵守状況の確認、外部委託を行う際のセキュリティ確保等、この要綱の運用面の対策を講じるものとする。
⑻　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。
イ　約款による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。
ロ　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ごとの責任者を定める。

（情報セキュリティ対策に関する監査及び自己点検の実施）
第７条　この要綱の遵守状況を検証するため、必要に応じて情報セキュリティ対策に関する監査及び自己点検を実施する。

（要綱の見直し）
第８条　情報セキュリティ対策に関する監査及び自己点検の結果、この要綱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になった場合には、この要綱を見直す。

（情報セキュリティ対策基準の策定）
第９条　前３条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策定する。

（情報セキュリティ実施手順の策定）
第 10 条　前条で策定する基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。
２　情報セキュリティ実施手順は、公にすることにより本府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。

第２部　対策基準

第１章　組織体制

（ＣＩＯ）
第 11 条　ＣＩＯは、本府における全て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　ＣＩＯは、本府の全ての情報システム等における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
３　ＣＩＯは、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティ対策に関する指導及び助言を行う権限を有する。
４　ＣＩＯは、本府の情報資産に対する侵害が発生した場合又は侵害が発生するおそれがある場合、必要かつ十分な措置を行う権限及び責任を有する。
５　ＣＩＯは、本府の共通的な情報システム等における情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
６　ＣＩＯは、緊急時等の円滑な情報共有を図るため、ＣＩＯ、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を整備しなければならない。
７　ＣＩＯは、必要に応じて情報セキュリティ対策に関する専門的な知識及び経験を有した専門家をアドバイザーとして置くことができる。
８　ＣＩＯ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。

（ＣＳＩＲＴの設置）
第 11 条の２　ＣＩＯは、ＣＳＩＲＴを整備し、役割を明確化する。
２　ＣＩＯは、情報セキュリティの統一的な窓口（以下「ＣＳＩＲＴ事務局」という。）を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない（ＣＳＩＲＴ事務局はＣＩＯの補佐を行う。）。
３　ＣＳＩＲＴ事務局は、情報セキュリティインシデントを認知した場合には、ＣＩＯ及び必要に応じ総務省へ報告しなければならない。
４　ＣＩＯは、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、外部の事業者等との情報共有を行うものとする。

（情報セキュリティ責任者）
第 12 条　行政情報化推進総括者を、情報セキュリティ責任者とする。
２　情報セキュリティ責任者は、部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。
３　情報セキュリティ責任者は、部局等の情報システム等における開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
４　情報セキュリティ責任者は、部局等の情報システム等について、緊急時等における連絡体制の整備、この要綱の遵守に関する意見の集約及び職員に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者）
第 13 条　行政情報化推進主任者を、情報セキュリティ管理者とする。
２　情報セキュリティ管理者は、室課等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　情報セキュリティ管理者は、情報システム等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事務局へ速やかに報告を行い、指示を仰がなければならない。

（情報システム管理者）
第 14 条　行政情報化推進主任者を、情報システム管理者とする。
２　情報システム管理者は、室課等の情報システム等における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
３　情報システム管理者は、室課等の情報システム等における情報セキュリティに関する権限及び責任を有する。
４　情報システム管理者は、室課等の情報システム等における情報セキュリティ実施手順の維持・管理を行う。

（情報システム担当者）
第 15 条　情報システム管理者の指示等に従い、室課等の情報システム等の開発、設定の変更、運用、更新作業、情報セキュリティ事案への対応等を行う職員を、情報システム担当者とする。

（兼務の禁止）
第 16 条　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。
２　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

## 第２章　情報資産の分類と管理方法

（情報資産の分類）
第 17 条　情報セキュリティ管理者は、情報資産を次の各号のとおり分類し、必要に応じて取扱制限を行うものとする。
⑴　重要度１　個人情報及び情報セキュリティの侵害が住民の生命、財産等へ重大な影響を及ぼす情報
⑵　重要度２　公開することを予定していない情報及び情報セキュリティの侵害が行政事務の執行等に重大な影響を及ぼす情報
⑶　重要度３　外部に公開する情報のうち、情報セキュリティの侵害が、行政事務の執行等に微妙な影響を及ぼす情報

⑷　重要度４　前３号以外の情報

（管理責任）
第 18 条　情報セキュリティ管理者は、情報資産について管理責任を有するとともに、情報資産が複製又は送付された場合、複製等された情報資産を第 17 条の分類に基づき管理しなければならない。

（情報の作成）
第 19 条　職員は、業務上必要のない情報を作成してはならない。
２　情報を作成する職員は、第 17 条の分類に基づき、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。
３　情報を作成する職員は、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、作成途上の情報が不要になった場合、当該情報を消去しなければならない。

（情報資産の入手）
第 20 条　庁内の者が作成した情報資産を入手した職員は、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　庁外の者が作成した情報資産を入手した職員は、第 17 条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
３　情報資産を入手した職員は、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。

（情報資産の利用）
第 21 条　情報資産を利用する職員は、業務以外の目的に情報資産を利用してはならない。
２　情報資産を利用する職員は、情報資産の分類に応じ、適切な取扱いをしなければならない。
３　情報資産を利用する職員は、記録媒体に情報資産の分類が異なるデータが複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

（情報資産の保管）
第 22 条　情報セキュリティ管理者及び情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。
２　情報セキュリティ管理者及び情報システム管理者は、データを記録した記録媒体を長期保管する場合、書込禁止の措置を講じるとともに、自然災害を被る可能性が低い地域に保管するよう努めなければならない。
３　情報セキュリティ管理者及び情報システム管理者は、データを記録した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するよう努めなければならない。
４　情報セキュリティ管理者は、情報資産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。

（データの送信）
第 23 条　電子メール等により重要度１又は２のデータを送信する職員は、必要に応じてデータの暗号化やパスワード設定を行わなければならない。

（データの運搬）
第 24 条　重要度１又は２のデータを車両等により運搬する職員は、情報セキュリティ管理者に運搬の許可を得るとともに、必要に応じてデータの暗号化又はパスワード設定の実施や、情報を記録した記録媒体の鍵付きのケース等への格納等、データ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。

（データの提供・公表）
第25条　重要度１又は２のデータを外部に提供する職員は、情報セキュリティ管理者に提供の許可を得るとともに、データの暗号化又はパスワード設定を行わなければならない。
２　情報セキュリティ管理者は、住民に公開するデータについて、破壊、改ざん又は消去されていない状態を確保しなければならない。

（データの廃棄）
第26条　重要度１又は２のデータを廃棄する職員は、情報セキュリティ管理者の廃棄の許可を得るとともに、データを記録している記録媒体の情報を復元できないように処置した上で廃棄しなければならない。
２　情報セキュリティ管理者は、廃棄処理について、日時、担当者及び処理内容を記録しなければならない。

第２章の２　情報システム全体の強靭性の向上

（個人番号利用事務系と他の領域との分離）
第26条の２　ＣＩＯは、個人番号利用事務系と他の領域を通信できないようにする措置を講じなければならない。
２　情報システム管理者は、個人番号利用事務系と外部との通信を行う場合、ＣＩＯの許可を得なければならない。
３　ＣＩＯは、前項の許可をする場合、次の各号を確認しなければならない。
⑴　接続が必要な合理的理由があること。
⑵　通信経路及びプロトコルを限定していること。
⑶　インターネットと直接接続していないこと（公的機関が構築・運用するシステムを除く。）。

（個人番号利用事務系の情報セキュリティ対策）
第26条の３　情報システム管理者は、個人番号利用事務系の情報システムにおいては、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）を利用しなければならない。ただし、専用端末機のログイン時に多要素認証を利用している場合はこの限りではない。
２　情報システム管理者は、個人番号利用事務系の端末機においては、外部記憶媒体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。

（ＬＧＷＡＮ接続系とインターネット接続系の分割）
第26条の４　ＣＩＯは、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、必要な通信だけを許可できるようにする措置を講じなければならない。
２　職員は、メール又はデータをＬＧＷＡＮ接続系に取り込む場合は、原則次の各号のいずれかの方式により無害化通信を図らなければならない。
⑴　危険因子をファイルから除去し、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取り込む方式
⑵　ＬＧＷＡＮ接続系の端末から、インターネット接続系の端末へ画面を転送する方式

（インターネット接続系のセキュリティ対策）
第26条の５　ＣＩＯは、インターネット接続系においては、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不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。
２　ＣＩＯは、インターネット接続系においては、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する自治体情報セキュリティクラウドに参加するとともに、関係省庁や市町村等と連携

しながら、情報セキュリティ対策を推進しなければならない。
３　ＣＩＯは、インターネット接続系に主たる端末と重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について定期的に外部監査を受けるよう努めるものとする。

## 第３章　物理的セキュリティ対策

（機器の取付け）
第 27 条　情報システム管理者は、重要情報を格納している情報システム等が稼動する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切に固定する等の措置を講じるよう努めなければならない。

（機器の冗長化）
第 28 条　情報システム管理者は、重要情報を格納している情報システム等が稼動する機器を冗長化し、単一の機器に障害が発生した際でも業務が継続できるよう努めるとともに、機器に障害が発生した場合には代替機器を起動し、機器の停止時間を最小限にするよう努めなければならない。

（機器の電源）
第 29 条　情報システム管理者は、重要情報を格納している情報システム等が稼動する機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給できる容量の予備電源を備え付けるよう努めるとともに、落雷等による過電流に対して機器を保護するための措置を講じるよう努めなければならない。

（通信ケーブル等の配線）
第 30 条　情報システム管理者は、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じるよう努めなければならない。
２　情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、施設管理部門等と連携して対応しなければならない。
３　情報システム管理者は、ネットワークの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切に管理しなければならない。
４　情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた事業者以外の者が通信ケーブル及び電源ケーブルの配線を変更、追加できないように必要な措置を施すよう努めなければならない。

（機器の保守及び修理）
第 31 条　情報システム管理者は、必要に応じて情報システム等が稼動する機器の保守を実施しなければならない。
２　情報システム管理者は、記録媒体を内蔵する機器を事業者に修理させる場合、可能な限り、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、情報システム管理者は、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。

（管理外の場所への機器の設置）
第 32 条　情報システム管理者は、本府の管理外の場所に本府の情報システム等が稼動する機器を設置する場合、定期的に情報セキュリティ対策の実施状況について確認しなければならない。

（機器の廃棄等）
第 33 条　情報システム管理者は、情報システム等が稼動する機器の廃棄等を行う場合、機器内部の

記憶装置を破壊又は記憶装置からすべての情報を消去する等、復元不可能な状態にする措置を講じなければならない。

（管理区域の設置等）

第 34 条　情報システム管理者は、全庁的な情報システム等が稼動する機器を設置する部屋、当該機器の管理運用を行うための部屋及びデータを記録した記録媒体の保管庫（以下「管理区域」という。）について、２階以上に設けるよう努めなければならない。また、管理区域の外壁については無窓とするよう努めなければならない。

２　情報システム管理者は、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者の立入りを防止しなければならない。

３　情報システム管理者は、管理区域に設置する機器に、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。

４　情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び記録媒体に影響を与えないようにしなければならない。

（管理区域の入退室管理等）

第 35 条　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ＩＣカード、指紋認証等による認証又は入退室管理簿の記載による入退室管理を行わなければならない。

２　管理区域への入退室を許可された情報システム担当者及び事業者は、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。

３　情報システム管理者は、外部からの訪問者が管理区域に入る場合、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情報システム担当者を付き添わせなければならない。

４　情報システム管理者は、管理区域に設置されている機器とは無関係の機器等を持ち込ませないよう努めなければならない。

（機器の搬入出）

第 36 条　情報システム管理者は、搬入出する機器が、既存の情報システム等に与える影響について、情報システム担当者又は既存の情報システム等の運用管理を行う事業者にあらかじめ確認を行わせなければならない。

２　情報システム管理者は、管理区域への機器の搬入出について、管理区域への入退室を許可された情報システム担当者を立ち会わせなければならない。

（ネットワークの管理）

第 37 条　情報システム管理者は、ネットワークに使用する通信回線及び機器を適切に管理しなければならない。また、これらに関連する文書を適切に保管しなければならない。

２　情報システム管理者は、外部とのネットワーク接続を必要最低限に限定し、できる限り接続点を減らさなければならない。

３　情報システム管理者は、ネットワークに使用する通信回線及び機器について、必要な情報セキュリティ対策の水準を検討の上、選択しなければならない。また、必要に応じてネットワーク上で送受信されるデータの暗号化を行わなければならない。

４　情報システム管理者は、ネットワークに使用する通信回線及び機器について、ネットワーク上で送受信されるデータの破壊、盗聴、改ざん、消去等のリスクを考慮の上、必要な情報セキュリティ対策を実施しなければならない。

５　情報システム管理者は、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するよう努めなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じるよう努めなければならない。

６　情報システム管理者は、盗難防止のため、執務室等で利用する端末機について、業務終了後は

施錠管理やワイヤー固定等の物理的措置を講じるよう努めなければならない。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。

## 第４章　人的セキュリティ対策

（職員の遵守事項）

第 38 条　職員は、情報セキュリティ対策について不明な点や遵守することが困難な点等がある場合、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

２　職員は、業務以外の目的で、情報資産の外部への持ち出し、情報システム等の利用、電子メールの使用及びインターネットの閲覧を行ってはならない。

３　職員は、本府の情報資産を府の管理外の場所に持ち出す場合や府の管理外の場所で情報処理業務を行う場合、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　職員は、原則として、私物の端末機や記録媒体を用いて業務を行ってはならない。ただし、端末機については、業務上の必要があり、ＣＩＯが定める手順に従い情報セキュリティ管理者の許可を得た場合は、この限りでない。

５　職員は、端末機のソフトウェアに関する情報セキュリティ対策機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

６　職員は、端末機や記録媒体、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や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、離席時に端末機の利用を制限するとともに、記録媒体や文書等を容易に閲覧されない場所に保管するなど、適切な措置を講じなければならない。

７　職員は、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。

（職員採用時の対応）

第 39 条　情報セキュリティ管理者は、新規に採用された職員に対し、この要綱のうち職員が守るべき内容を説明し、遵守させるよう努めなければならない。

（要綱の掲示）

第 40 条　ＣＩＯは、職員が常にこの要綱を閲覧できるように掲示しなければならない。

（事業者に対する説明）

第 41 条　情報システム管理者は、情報システム等の開発等を事業者に委託する場合、当該事業者からの再委託を受ける事業者も含めて、この要綱のうち事業者が守るべき内容を説明し、遵守させるよう努めなければならない。

（情報セキュリティに関する研修・訓練）

第 42 条　ＣＩＯは、必要に応じて情報セキュリティ対策に関する研修・訓練を実施しなければならない。

２　ＣＩＯは、必要に応じて職員が情報セキュリティ対策に関する研修・訓練を受講できるよう研修計画を立案しなければならない。

３　ＣＩＯは、新規に採用された職員に対し、情報セキュリティ対策に関する研修を実施するよう努めなければならない。

（事故、欠陥等の報告）

第 43 条　職員は、情報セキュリティに関する事故、情報システム等の欠陥及び誤動作を発見した場合、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。

２　前項による報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
３　情報セキュリティ管理者は、報告のあった事故等について、ＣＩＯに報告しなければならない。

（住民等外部からの事故等の報告）
第 44 条　職員は、本府が管理する情報資産に関する事故、欠陥について、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。
２　報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
３　情報セキュリティ管理者は、当該事故等について、必要に応じてＣＩＯに報告しなければならない。
４　ＣＩＯは、情報システム等の情報資産に関する事故、欠陥について、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

（事故等の分析・記録等）
第 45 条　ＣＳＩＲＴ事務局は、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。
２　ＣＳＩＲＴ事務局は、情報セキュリティインシデントであると評価した場合、ＣＩＯに速やかに報告しなければならない。
３　ＣＩＯ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。
４　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は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、ＣＩＯに報告しなければならない。
５　ＣＩＯは、前項により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。

（ＩＤ及びパスワード等の管理）
第 46 条　職員は、自己の管理するＩＤに関し、次の各号を遵守しなければならない。
⑴　自己に専属するＩＤは、他者に利用させないこと。
⑵　共用のＩＤを利用する場合、当該ＩＤの利用者以外に利用させないこと。
２　職員は、自己の管理するパスワードに関し、次の各号を遵守しなければならない。
⑴　パスワードは、他者に知られないように管理すること。
⑵　パスワードは秘密にし、パスワードの照会等には一切応じないこと。
⑶　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にすること。
⑷　パスワードが流出したおそれがある場合、情報セキュリティ管理者に速やかに報告のうえ、パスワードを速やかに変更すること。
⑸　複数の情報システムを扱う職員は、同一のパスワードを情報システム間で用いないこと。
⑹　仮に発行されたパスワードは、最初の認証時点で変更すること。
⑺　端末機等にパスワードを記憶させないこと。
⑻　共用のＩＤを除き、職員間でパスワードを共有しないこと。

## 第５章　技術的セキュリティ対策

（データ共有用機器の設定等）
第 47 条　情報システム管理者は、職員が使用できるデータ共有用機器について、当該機器に保存できるデータの容量を設定し、職員に周知しなければならない。

２　情報システム管理者は、担当業務に関係のない室課等のデータを職員が閲覧及び使用できないよう機器を設定しなければならない。
３　情報システム管理者は、住民の個人情報、人事記録等、特定の職員しか取扱うべきでないデータに関しては、特定の職員のみが取扱うことができるよう機器を設定しなければならない。
４　情報システム管理者は、機器に保存されたデータについて、必要に応じて定期的に複製を作成するよう努めなければならない。

（バックアップの実施）
第47条の２　情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

（他団体との情報システム等に関する情報等の交換）
第48条　情報システム管理者は、他の団体と情報システム等に関する情報や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、ＣＩＯ及び情報セキュリティ責任者の許可を得なければならない。

（作業記録の作成や作業の確認等）
第49条　情報システム管理者は、情報システム等の運用により実施した作業に関する記録を作成しなければならない。
２　情報システム管理者は、情報システム等において、変更等の作業を行った場合、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。
３　情報システム管理者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事業者が、障害発生の危険性を伴うシステム変更等の作業を行う場合、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。

（情報システム等の仕様書等の管理）
第50条　情報システム管理者は、情報システム等の仕様書や構成図等について、記録媒体に関わらず、業務上必要とする者以外の者による閲覧、又は紛失等がないよう、適切に管理しなければならない。

（情報システム等の動作記録等の取得等）
第51条　情報システム管理者は、情報システム等の各種の動作記録及び情報セキュリティ対策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　情報システム管理者は、前項で取得及び保存した記録について、重要度に応じて期間を定めて保管するとともに、詐取、改ざん、誤消去等が行われないよう必要な措置を講じなければならない。
３　情報システム管理者は、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。

（障害記録の管理）
第52条　情報システム管理者は、情報システム等に関する障害の報告、障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（ネットワークの通信経路の制御等）
第53条　情報システム管理者は、ネットワークで円滑な通信が行われるよう、ネットワークに使用する通信回線及び機器について、通信経路の制御等が適切に設定されていることを確認しなければならない。

（外部ネットワークとの常時接続時の制限等）
第54条　ＣＩＯは、外部ネットワークとの常時接続に際しては、当該ネットワークの機器構成等を詳細に検討し、情報システム等に影響が生じないことを確認した上で、接続させることができる。
２　ＣＩＯは、外部ネットワークの管理責任者との協議により、責任分界点を明確にしなければならない。
３　ＣＩＯは、外部ネットワークに問題が認められ、情報システム等に支障が生じることが想定される場合、速やかに外部ネットワークとの接続を遮断しなければならない。
４　ＣＩＯは、外部ネットワークとの常時接続に際しては、外部ネットワークとの通信を制御し、情報システム等の安全維持を図る機器を外部ネットワークとの境界に設置したうえで接続しなければならない。
５　情報セキュリティ管理者は、ＩｏＴ機器を含む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、必要に応じて、当該機器の特性に応じた対策を講じなければならない。

（ネットワークの盗聴対策）
第55条　情報システム管理者は、ＣＩＯの許可なく、無線機器によるネットワークを整備してはならない。
２　ＣＩＯは、無線機器によるネットワークの整備を認める場合、解読が困難な暗号化及び認証技術を有する無線機器の使用を義務づけなければならない。
３　情報システム管理者は、重要度の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）
第56条　ＣＩＯは、原則として、外部から外部への電子メールの中継処理が行われることを不可能にしなければならない。
２　ＣＩＯは、業務に関係のない大量の広告メール等の受信又は送信を検知した場合、電子メールの運用を停止することができる。
３　ＣＩＯ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するとともに、その旨を職員に周知しなければならない。
４　ＣＩＯは、情報システム等の開発等のため庁舎内に常駐している事業者による電子メールの利用について、事業者との間で利用方法を取り決めなければならない。

（電子メールの利用制限）
第57条　職員は、原則として、自動転送機能を用いて、電子メールを転送してはならない。
２　職員は、業務上必要のない送信先に電子メールを送信してはならない。
３　職員は、複数人に電子メールを送信する際、必要に応じて他の送信先が分からないようにしなければならない。
４　職員は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。
５　職員は、インターネットで不特定多数が利用できる電子メールやデータ共有サービス等を使用して自ら情報を共有又は送信してはならない。

（無許可ソフトウェアの導入等の禁止）
第58条　職員は、端末機等に無断でソフトウェアを導入してはならない。ただし、業務上の必要があり、情報セキュリティ管理者及び情報システム管理者の許可を得て、適正な利用権限がある場合は、この限りでない。
２　情報セキュリティ管理者は、前項ただし書きの導入を許可する際には、ソフトウェアの利用権限を管理しなければならない。

（機器構成の変更の制限）
第 59 条　職員は、端末機の改造及び増設・交換を行ってはならない。
２　職員は、業務上、端末機の改造及び増設・交換を行う必要がある場合、情報システム管理者の許可を得なければならない。

（無許可でのネットワーク接続の禁止）
第 60 条　職員は、ＣＩＯの許可なく、端末機をネットワークに接続してはならない。

（業務以外の目的でのインターネット閲覧の禁止）
第 61 条　職員は、業務以外の目的でインターネットを閲覧してはならない。

（利用制御）
第 62 条　情報システム管理者は、情報システム等の機能により、職員の情報システム等の利用を制限しなければならない。
２　情報システム管理者は、不特定多数に公開する情報システム等を除き、職員に応じた利用制御ができるよう、認証機能を確保しなければならない。
３　情報システム管理者は、情報システム等を利用する職員のＩＤ及びパスワードに関する登録、変更、抹消等の取扱方法を定めなければならない。
４　職員は、情報システム等を利用する必要がなくなった場合、登録されているＩＤ及びパスワードを抹消するよう、情報システム管理者に通知しなければならない。
５　情報システム管理者は、利用されていないＩＤ及びパスワードが放置されないよう、点検しなければならない。
６　情報システム管理者は、管理者権限等の特権を付与されたＩＤ及びパスワードを利用する職員を必要最小限にし、当該ＩＤ及びパスワードの漏えい等が発生しないよう厳重に管理しなければならない。
７　情報システム管理者は、管理者権限等の特権を付与されたＩＤ及びパスワードについて、通常のＩＤ及びパスワードよりも有効となる期間を短くするなど、情報セキュリティ対策を強化しなければならない。

（職員による外部ネットワークからのアクセス等の制限）
第 63 条　職員及び事業者が、外部からインターネットや公衆回線を経由して情報システム等に接続する場合、ＣＩＯの許可を得なければならない。
２　ＣＩＯは、前項の接続を許可する場合、次の各号を遵守しなければならない。
⑴　接続が必要な合理的理由を有する必要最小限の職員に接続を限定すること。
⑵　情報システム等の機能により職員の本人確認を行うこと。
⑶　接続に伴う盗聴を防御するために暗号化等の措置を講じること。
３　ＣＩＯは、第１項の接続のために必要となる端末機を職員に貸与する場合、情報セキュリティ対策のために必要な措置を講じなければならない。
４　職員は、貸与された端末機を情報システム等に接続する際、前項の措置が講じされているか確認しなければならない。
５　ＣＩＯは、インターネットや公衆回線を経由したリモートアクセス環境を構築する場合は、利用者の認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。
６　職員等は、リモートアクセス環境を利用する際、前項の措置が講じされているか確認しなければならない。
７　情報システム管理者は、必要に応じてログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等により、正当なアクセス

権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（認証情報に関する情報の管理）

第 64 条　情報システム管理者は、職員の認証情報を厳重に管理しなければならない。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、これを有効に活用するよう努めなければならない。

２　情報システム管理者は、職員に対して情報システム等を利用するためのパスワードを発行する場合、仮のパスワードを発行するとともに、認証後直ちに当該パスワードを変更させなければならない。

３　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るよう努めなければならない。

（管理者権限等の特権による接続時間の制限）

第 65 条　情報システム管理者は、原則として、管理者権限等の特権による情報システム等への接続時間を必要最小限に制限しなければならない。

（情報システム等の調達）

第 66 条　情報システム管理者は、情報システム等の開発、導入、保守等の調達に当たっては、情報セキュリティを確保するために必要とする技術的な機能を調達仕様書に明記しなければならない。

２　情報システム管理者は、情報システム等に関する機器及びソフトウェアの調達に当たっては、当該製品における情報セキュリティを確保するための機能を調査し、情報セキュリティ対策上問題のないことを確認しなければならない。

（情報システム等の開発）

第 67 条　情報システム管理者は、情報システム等の開発に関する責任者及び作業者（以下「責任者等」という。）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定を確立しなければならない。

２　情報システム管理者は、情報システム等の開発に関し、次の各号を遵守しなければならない。

⑴　責任者等が使用するＩＤ及びパスワードを管理し、開発完了後、当該ＩＤ及びパスワードを削除すること。

⑵　責任者等が利用する情報システム等の利用権限を設定すること。

⑶　責任者等が使用する機器及びソフトウェアを特定すること。

（情報システム等の導入）

第 68 条　情報システム管理者は、情報システム等の運用環境を事業者が許可なく操作しないよう、適切に管理しなければならない。

２　情報システム管理者は、必要に応じてシステム開発、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。

３　情報システム管理者は、情報システム等の開発・保守及び試用環境から稼働環境への移行について、情報システム等の開発・保守計画の策定時に手順を明確にしなければならない。

４　情報システム管理者は、前項による移行の際、情報システム等に記録されているデータの保存を確実に行い、移行に伴う情報システム等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。

５　情報システム管理者は、新たに情報システム等を導入する場合、十分な試験を行わなければならない。

６　情報システム管理者は、運用試験を行う場合、あらかじめ試用環境による操作確認を行わなければならない。

7　情報システム管理者は、個人情報を含むデータを、運用試験に使用してはいけない。

（情報システム等の開発・保守に関連する資料等の保管）

第 69 条　情報システム管理者は、情報システム等の開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

2　情報システム管理者は、情報システム等に関する試験結果を一定期間保管しなければならない。

3　情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

（情報システム等における入出力データの正確性の確保）

第 70 条　情報システム管理者は、情報システム等に入力されるデータについて、範囲、妥当性の確認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等を設計しなければならない。

2　情報システム管理者は、故意又は過失によりデータが改ざんされる又は漏えいするおそれがある場合、これを検出する確認機能を組み込むように情報システム等を設計しなければならない。

3　情報システム管理者は、情報システム等から出力されるデータについて、処理が正しく反映され、出力されるように情報システム等を設計しなければならない。

（情報システム等の変更管理）

第 71 条　情報システム管理者は、情報システム等を変更した場合、仕様書等の変更履歴を作成するとともに、変更後の資料や文書を適切な方法で保管しなければならない。

（情報システム等の開発・保守用のソフトウェアの更新等）

第 72 条　情報システム管理者は、情報システム等の開発・保守用のソフトウェアの更新等を行う場合、他の情報システム等との整合性を確認しなければならない。

（情報システム等の更新や統合時の検証等）

第 73 条　情報システム管理者は、情報システム等の更新・統合を行うにあたり、更新・統合の基準を明確化するとともに、更新・統合後の業務運営体制の検証等を行わなければならない。

（不正プログラム対策）

第 74 条　情報システム管理者は、不正プログラム対策として、次の各号を措置しなければならない。

⑴　インターネットとの通信について、インターネットとの接続点に、不正プログラムによる不審な通信を検知し、通信を遮断する機器を設置する等の措置を講じること。

⑵　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、必要に応じ職員に対して注意喚起しなければならない。

⑶　情報システム等が稼動する機器に、コンピュータウイルス等の不正プログラム対策用のソフトウェアを常駐させるとともに、当該ソフトウェアを常に最新の状態に保つこと。また、当該ソフトウェアによる不正プログラムの探索が定期的に実施されるよう設定すること。

⑷　情報システム等が稼動する機器に導入されたソフトウェアについては、既知の脆弱性が無い状態に常時保つこと。

⑸　情報システム等が稼動する機器が不正プログラムに感染した場合、ネットワークから当該機器を切り離すこと。

2　職員は、不正プログラム対策に関し、次の各号を遵守しなければならない。

⑴　端末機に不正プログラム対策用のソフトウェアが導入され、必要な設定が行われている場合、当該ソフトウェアの設定を変更しないこと。

⑵　端末機に外部からデータ又はソフトウェアを取り入れる場合、必ず不正プログラム対策用のソフトウェアによるチェックを行うこと。

⑶　端末機で差出人が不明なデータ等を受信した場合、速やかに削除すること。
⑷　端末機が不正プログラムに感染した場合、ネットワークから即時に切り離すこと。
⑸　ＣＩＯが提供する情報セキュリティ対策に関する情報を、常に確認すること。

（不正アクセス対策）
第 75 条　情報システム管理者は、不正アクセス対策として、情報システム等に次の各号を措置しなければならない。
⑴　業務に不必要な通信を遮断するよう設定すること。
⑵　機器の OS 等における不要なサービスについて、機能を削除し、又は停止すること。
⑶　侵入やデータの改ざん等を監視及び防止するよう設定すること。
２　ＣＩＯは、情報システム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、情報システム等の停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。
３　ＣＩＯは、情報システム等に攻撃を受け、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、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。
４　ＣＩＯ及び情報システム管理者は、職員による不正アクセスを発見した場合は、当該職員が所属する室課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。
５　情報システム管理者は、必要に応じて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、情報システムが提供するサービスを利用者が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。

（情報セキュリティ対策に関する情報収集）
第 76 条　ＣＩＯは、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者は、情報セキュリティ対策に関する情報を収集のうえ、必要に応じて関係者間での共有や職員への周知を行わなければならない。
２　ＣＩＯは、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者は、当該情報の緊急度に応じて、情報セキュリティの侵害等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。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も、同様の対策を速やかに講じなければならない。

（情報システム等の監視）
第 77 条　情報システム管理者は、情報システム等の情報セキュリティに関する事案を常時検知できるよう措置を講じなければならない。
２　情報システム管理者は、情報システム等が稼動する機器に正確な時刻を設定し、機器間の時刻同期ができる措置を講じなければならない。
３　情報システム管理者は、インターネットに公開される情報システム等を常時監視できるよう措置を講じなければならない。

（違反時の対応等）
第 78 条　ＣＩＯは、職員の違反行動に関する報告を受けた場合、報告内容の確認のために、端末機や情報システム等の利用記録、電子メールの送受信記録、インターネットの閲覧記録等を調査することができる。
２　ＣＩＯは、前項の調査により職員の違反行動を確認した場合、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通知し、適切な措置を求めなければならない。
３　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指導によっても職員の違反行動が改善されない場合、ＣＩＯは、当該職員が端末機などを使用する権利を停止あるいは剥奪することができる。その場合、ＣＩＯは、権利を停止あるいは剥奪した旨を情報セキュリティ責任者、情報

セキュリティ管理者及び情報システム管理者に速やかに通知しなければならない。

（外部委託等）

第 79 条　情報セキュリティ管理者は、外部委託等を行う事業者の選定する際、委託等の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。

２　情報セキュリティ管理者は、外部委託等を行う事業者の選定する際、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、選定するよう努めなければならない。

３　情報セキュリティ管理者は、外部委託を行う事業者と次の各号の要件を明記した契約を必要に応じて締結しなければならない。

⑴　この要綱の遵守
⑵　責任者、委託内容、作業者及び作業場所の特定
⑶　提供される品質や成果等に関する水準保証
⑷　従業員に対する教育の実施
⑸　提供された情報の目的外利用及び契約者以外の者への提供の禁止
⑹　業務上知り得た情報の守秘義務
⑺　再委託等に関する制限事項の遵守
⑻　業務終了時の情報資産の返還、廃棄等
⑼　業務の定期報告及び緊急時報告の義務
⑽　府による監査及び検査
⑾　府による事故時等の公表
⑿　この要綱が遵守されなかった場合の損害賠償等の規定
⒀　外部委託事業者にアクセスを許可する情報の種類、範囲及びアクセス方法

４　情報セキュリティ管理者は、外部委託等を行う事業者において必要な情報セキュリティ対策が実施されていることを定期的に確認し、必要に応じて前項の契約内容に基づく措置を行わなければならない。

（約款による外部サービスの利用）

第 79 条の２　情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要度１又は２（個人情報に関して、個人情報保護審議会の許可を得たものは除く。）の情報が取り扱われないように規定しなければならない。

⑴　約款によるサービスを利用して良い範囲
⑵　業務により利用する約款による外部サービス
⑶　利用手続及び運用手順

２　職員は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

３　重要度１又は２の情報を取り扱わず高いレベルの情報管理を要求しない事業で利用するソーシャルメディアサービスについては、第 79 条の４を適用する。

（クラウドサービスの利用）

第 79 条の３　情報セキュリティ管理者は、クラウドサービス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　情報セキュリティ管理者は、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委託先を選定し、必要に応じて委託事業の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　情報セキュリティ管理者は、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、必要に応じ委託先を選定する際の要件としなければならない。
４　情報セキュリティ管理者は、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。

（ソーシャルメディアサービスの利用）
第79条の４　情報セキュリティ管理者は、本府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各号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。
⑴　本府のアカウントによる情報発信が、実際の本府のものであることを明らかにするために、本府の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。
⑵　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等の方法で、不正アクセス対策を実施すること。
２　職員は、重要度１又は２の情報を、ソーシャルメディアサービスで発信してはならない。
３　情報セキュリティ管理者は、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。
４　情報セキュリティ管理者は、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。

（例外措置の許可）
第80条　情報セキュリティ管理者及び情報システム管理者は、情報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し、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、ＣＩＯの許可を得て、例外措置を取ることができる。
２　情報セキュリティ管理者及び情報システム管理者は、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ＣＩＯに報告しなければならない。
３　ＣＩＯは、例外措置の申請書及び審査結果を適切に保管しなければならない。

（法令遵守）
第81条　職員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。
⑴　地方公務員法(昭和 25 年法律第 261 号)
⑵　著作権法（昭和 45 年法律第 48 号）
⑶　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）
⑷　個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑸　大阪府個人情報保護条例（平成８年大阪府条例第２号）
⑹　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）
⑺　サイバーセキュリティ基本法（平成 26 年法律第 104 号）

## 第６章　評価・見直し

（監査）
第82条　ＣＩＯは、原則、情報セキュリティ監査統括責任者を指名し、情報資産に対する情報セキュリティの対策状況について、必要に応じて監査を行わせなければならない。

２　情報セキュリティ監査統括責任者は、監査を実施する場合、被監査部門から独立するとともに、監査及び情報セキュリティ対策に関する専門知識を有する者に対して、監査の実施を依頼しなければならない。
３　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案しなければならない。
４　外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、この要綱の遵守についての監査を必要に応じて行わなければならない。
５　情報セキュリティ監査統括責任者は、監査結果を取りまとめ、ＣＩＯに報告しなければならない。
６　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切に保管しなければならない。
７　ＣＩＯは、監査結果を踏まえ、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に対し、監査結果への対処を指示しなければならない。
８　ＣＩＯは、この要綱の見直しに、監査結果を活用するよう努めなければならない。

（自己点検）
第 83 条　ＣＩＯ、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者は、この要綱の遵守状況について、必要に応じて自己点検を実施するとともに、自己点検の結果を踏まえて、自己の権限の範囲内で改善を図るよう努めなければならない。

（要綱の見直し）
第 84 条　ＣＩＯは、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、必要に応じてこの要綱の見直しを行わなければならない。

附　則
１　この要綱は、平成 26 年４月１日から施行する。
２　大阪府情報セキュリティ委員会設置要綱については、平成 26 年３月 31 日をもって廃止する。

附　則
この要綱は、令和２年４月１日から施行する。

附　則
この要綱は、令和３年３月 29 日から施行する。

附　則
この要綱は、令和３年 11 月 22 日から施行する。