福岡県情報セキュリティ対策基準

目次

第１章　総則

（趣旨）

第１条　この基準は、福岡県情報処理規程（平成２４年２月福岡県訓令第１号。以下「規程」という。）第５条第２項第１号の規定に基づき、県が保有する情報資産を災害、不正アクセス、紛失等の脅威から保護し、機密情報の滅失及び漏えい、業務の停止その他の事故を防止するため、県が実施する情報セキュリティ対策に関し、具体的な遵守事項を定めるものとする。

（用語の定義）

第２条　この基準において、次の各号に掲げる用語の意義は、当該各号に定めるもののほか、規程の定めるところによる。

（１）不正アクセス

情報資産を利用する権限のない者が、正当な利用者を偽って、不正に情報資産にアクセスし、情報資産の窃取、改ざん又は破壊等を行うことをいう。

（２）脅威

情報資産の滅失及び漏えい、業務の停止その他の事故に伴う損害の原因となる次の事象をいう。

ア　地震、風水害その他の災害
イ　プログラムの不具合、機器の故障その他の障害
ウ　不正アクセス、不正プログラムその他の不正行為
エ　紛失、誤送信、操作ミスその他の過失

（３）所属

規程第２条第２号において課等として定める本庁の課及び室並びに出先機関をいう。

（４）所属長

所属の長をいう。

（５）情報システム管理者

福岡県情報システム開発・運用基準第７条に定める情報システム管理者をいう。

（６）電子情報

規程第２条第７号に定める情報資産のうち、電子的に記録された情報をいう。

（７）行政汎用パソコン

福岡県共用パソコン管理運用要領第２条第３号に定める行政汎用パソコンをいう。

（８）業務用パソコン等

前項に定める行政汎用パソコン及び業務で利用するために所属で導入したパソコン等をいう。

（９）パスワード

利用者本人であることを確認するために入力させる文字列をいう。

（１０）不正プログラム

利用者が意図しないうちに電子計算機に侵入し、情報資産の窃取、改ざん又は破壊等の被害を与えるコンピュータウイルス及びスパイウェア等をいう。

（１１）ＩＤ

情報資産の正当な利用者であることを識別するために用いる符号をいう。

（１２）真正性

情報資産の利用者及び機器等がなりすまし、偽装等のない本物であることをいう。

（１３）フィルタリング

一定の条件に基づいて、インターネットの閲覧内容又は悪質な電子メールの受信を制限する機能をいう。

（１４）約款による外部サービス

有料、無料にかかわらず、約款への同意及び簡易なアカウントの登録により利用可能であるサービスをいう。

（１５）クラウドサービス

事業者等が提供するコンピュータ、記憶装置及びソフトウェア等を、ネットワーク経由で利用するサービスをいう。

（１６）ソーシャルメディア

事業者等が運営するインターネット上のサービスを利用して、利用者自らが不特定多数に対して情報を発信、あるいは相互に情報のやり取りや共有を行うことができる情報伝達媒体をいう。

（適用範囲）

第３条　この基準の適用範囲は、次の各号に掲げるとおりとする。

（１）組織

規程第２条第２号に定める課等

（２）情報資産

規程第２条第７号に定める情報資産

（３）職員

課等に属する職員（非常勤職員及び臨時職員を含む。）

第２章　組織・体制

（最高情報責任者）

第４条　規程第４条に定める最高情報責任者は、県の情報セキュリティ対策を統括するものとし、次の業務を行う。

（１）情報セキュリティに関する重要事項の決定

（２）重大な情報資産の滅失及び漏えい、業務の停止その他の事故（以下この章、第７章及び第８章において「事故」という。）が発生したときの指示

（３）その他前２号を実施するために必要な事項

（企画・地域振興部長）

第５条　企画・地域振興部長は、最高情報責任者を補佐し、総合的な情報セキュリティ対策を講じるものとし、次の業務を行う。

（１）実施すべき情報セキュリティ対策の決定

（２）規程に基づく情報セキュリティ監査の実施

（３）事故が発生したときの指示

（４）その他前３号を実施するために必要な事項

（情報政策課長）

第６条　企画・地域振興部情報政策課長（以下「情報政策課長」という。）は、企画・地域振興部長を補佐し、全所属における情報セキュリティ対策の徹底を図るものとし、次の業務を行う。

（１）情報セキュリティに関する指導

（２）情報セキュリティに関する研修の実施

（３）情報セキュリティに関する情報の収集及び最新技術の評価

（４）その他前３号を実施するために必要な事項

（情報セキュリティ管理者）

第７条　所属における情報セキュリティ対策を確実に実施するため、情報セキュリティ管理者を置く。

２　情報セキュリティ管理者は所属長とし、その所属における情報資産に関して次の業務を行う。

（１）所掌事務の遂行に必要な情報資産（情報システムに関わるものを除く。）の管理

（２）情報セキュリティ対策の実施

（３）事故発生時の報告及び必要な措置の実施

（４）その他前３号を実施するために必要な事項

３　規程第６条第２項に定める情報化推進リーダーは、前項に掲げる情報セキュリティ管理者の業務を補佐するものとする。

第８条　削除

（職員）

第９条　職員は、この基準に定められている事項を遵守し、事故の発生を未然に防止するよう努めるとともに、事故が発生した場合は、速やかに情報セキュリティ管理者又は情報システム管理者に報告した上で、必要な措置を講じなければならない。

第３章　情報資産の管理

（情報資産の管理責任）

第１０条　情報セキュリティ管理者及び情報システム管理者は、所属又は所管する情報システムにおいて取り扱う情報資産に関し、次の措置を講じなければならない。

（１）情報資産（規程第２条第７号イに該当するものを除く。以下第１４条までにおいて同じ。）の分類

（２）情報資産の利用目的の明確化及び利用権限の設定

（３）情報セキュリティ対策の実施

（４）その他前３号を実施するために必要な事項

（情報資産の分類）

第１１条　情報セキュリティ管理者及び情報システム管理者は、別表第１の分類基準に従って、所管する情報資産の分類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システム管理者は、前項の分類について適時見直しを行うとともに、その変更内容を職員その他関係者に周知徹底しなければならない。

（情報資産の利用目的の明確化及び利用権限の設定）

第１２条　情報セキュリティ管理者及び情報システム管理者は、所管する情報資産の利用目的を明らかにするとともに、当該情報資産を利用する職員、県民等に対して、その利用目的に沿った利用権限を設定しなければならない。

（情報セキュリティ対策の実施）

第１３条　情報セキュリティ管理者及び情報システム管理者は、所管する情報資産に対する脅威の内容を把握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、第１１条第１項の規定に基づく情報資産の分類及び前項の規定により把握した脅威の内容に応じて、この基準に基づく情報セキュリティ対策を適切に実施しなければならない。

３　情報セキュリティ管理者及び情報システム管理者は、この基準に基づく情報セキュリティ対策を実施することが困難な場合、その対応策について情報政策課長と協議しなければならない。

（電子情報の保存）

第１４条　情報セキュリティ管理者は、所属に備える外部記憶媒体は必要最小限とし、紛失及び盗難を防止するため、管理責任者を指名し、外部記憶媒体に番号を付して一括管理させなければならない。

２　前項に定める管理責任者は、外部記憶媒体を施錠可能な場所に保管するとともに、外部記憶媒体ごとの使用状況を様式第１号により、常時把握しなければならない。
３　職員は、行政汎用パソコンで取り扱う電子情報（情報システムで処理するものを除く。以下この条において同じ。）のうち、別表第１に掲げる機密性１及び機密性２、完全性１並びに可用性１のいずれかに分類されるものについては、当該電子情報を安全に保護するため、ファイル共有システムに保存しなければならない。なお、機密性１に該当するものについては、情報漏えいの防止策として、秘匿性等その内容に応じて、当該電子情報へのパスワードの設定による暗号化を行うなどの必要な措置を講じなければならない。
４　職員は、前項の規定によりファイル共有システムに保存した電子情報を外部記憶媒体に書き出してはならない。業務上やむを得ない理由により書き出す必要がある場合は、データ持ち出し管理システムにより、情報セキュリティ管理者にその理由を申し出て、許可を得なければならない。
５　職員は、長期保存のために電子情報を書き出した外部記憶媒体については、当該外部記憶媒体に分類を表示するほか、劣化に伴う電子情報の滅失又はき損への措置を講じなければならない。

（電子情報の持ち出し又は外部への提供）
第１５条　職員は、電子情報を執務室外へ持ち出してはならない。業務上やむを得ない理由により執務室外へ持ち出す必要がある場合は、データ持ち出し管理システムにより、情報セキュリティ管理者又は当該電子情報を所管する情報システム管理者にその理由を申し出て、許可を得なければならない。
２　職員は、電子情報を外部へ提供してはならない。業務上やむを得ない理由により関係機関等へ提供する必要がある場合は、提供先において安全保護の措置が講じられることを確認した上で、データ持ち出し管理システムにより、情報セキュリティ管理者又は当該電子情報を所管する情報システム管理者にその理由を申し出て、許可を得なければならない。
３　職員は、電子情報の執務室外への持ち出し又は外部への提供に当たっては、外部記憶媒体の紛失又は盗難等による情報の漏えいを防止するため、当該電子情報へのパスワードの設定による暗号化を行うなどの必要な措置を講じなければならない。また、用務終了後は、当該電子情報を消去の上、速やかに使用した外部記憶媒体を管理責任者に返却しなければならない。
４　情報セキュリティ管理者及び情報システム管理者は、県民に公開する情報資産については、改ざん、き損等を防止し、正確で完全な情報の提供ができるよう適切な措置を講じなければならない。

（台帳の作成）

第１６条　情報セキュリティ管理者及び情報システム管理者は、所管する情報資産のうち、規程第２条第７号イに定める電子計算機、ソフトウェア及びネットワーク並びに規程第２条第７号ロに定める情報を記録した媒体（ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等の光学メディアを除く）については、福岡県情報資産管理システム管理運用要領に基づき台帳を作成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、所管する情報資産のうち機密性１に該当する電子情報（情報システムで処理するものを除く。）については、秘匿性等その内容に応じて、様式第２号により、電子情報管理台帳を作成しなければならない。

３　情報セキュリティ管理者及び情報システム管理者は、第１１条第２項の規定により分類の見直しを行った際は、前項で作成した電子情報管理台帳を速やかに変更しなければならない。

（情報資産の廃棄等）

第１７条　情報セキュリティ管理者及び情報システム管理者は、電子情報を記録した情報資産が不要になった場合は、別表第２に掲げる方法に従い、電子情報を復元不可能な状態にした上で廃棄し、措置が確実に履行されたことを、職員による立会確認又は証明書の受領等により確認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、別表第２に定める措置を講じた場合は、前条に定める台帳に廃棄又は消去年月日、実施者氏名等の必要事項を登録又は記録しなければならない。

第４章　物理的セキュリティ対策

（サーバ等の設置及び保管場所）

第１８条　情報システム管理者は、情報資産の滅失及び漏えい、業務の停止その他の事故を防止するため、サーバ及び外部記憶媒体（以下「サーバ等」という。）を設置及び保管する場所に、次の措置を講じなければならない。庁外の場所に設置及び保管する場合も同様とする。

（１）耐震、防火、防水、耐熱等の必要な措置を講じるとともに、停電に備え情報システムの正常停止に必要な予備電源を用意すること。

（２）常時施錠することにより立入りを制限し、入室が必要な者に対しては、事前に許可を与えた上で、入室許可証を携行させること。

　また、ＩＣカード等による入退室管理を行い、その入退室の事跡を入退室管理簿等に記録すること。

（３）サーバ等の搬入出又は保守点検を行う場合は、職員を立ち会わせる等により、許可していないサーバ等の持ち込み及び持ち出しがないように確認すること。

２　情報システム管理者は、前項に定める場所の確保が困難な場合、サーバ等は、ラックに格納した上で施錠管理しなければならない。

（ネットワーク設備の管理）

第１９条　情報システム管理者は、所管する情報システムのネットワーク設備について、通信の傍受、設備の損傷、業務の停止その他の事故から保護するために必要な措置を講じなければならない。

２　情報システム管理者は、外部のネットワークの利用は必要最小限度とし、所管するネットワークとの接続ポイントを限定しなければならない。

３　情報システム管理者は、所管する情報システムのネットワークの機密性、安全性及び信頼性が保持されるよう適切な回線を選択しなければならない。また、必要に応じて、外部との送受信に際しては、通信の暗号化を行わなければならない。

（執務室の施錠管理）

第２０条　情報セキュリティ管理者は、執務室に職員がいない場合は、業務用パソコン等及び外部記憶媒体等の盗難を防止するため、施錠による管理を確実に行わなければならない。

第５章　人的セキュリティ対策

（職員の遵守事項）

第２１条　職員は、業務目的以外で、業務用パソコン等及び外部記憶媒体の利用、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。

また、業務のために私物のパソコン等を用いて、情報処理作業を行ってはならない。

２　情報政策課長及び情報システム管理者は、職員による業務目的以外の利用を把握したときは、当該職員が所属する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。

３　職員は、業務用パソコン等及び外部記憶媒体の利用に当たっては、次の事項を遵守しなければならない。

（１）原則として庁外に持ち出さないこと。

業務上やむを得ず持ち出す必要がある場合は、外部記憶媒体においては様式第１号に記載すること。また、業務用パソコン等においては様式第３号により、情報セキュリティ管理者又は情報システム管理者に対して、その理由とともに、紛失又は盗難による情報の漏えい防止策を申し出て、許可を得ること。

なお、業務用パソコンのうち福岡県モバイルワークシステム管理運用要領で定めるモバイルワーク端末等については、本号は適用しないものとし、福岡県モバイルワークシステム管理運用要領の規定に基づく手続きを行った上で持ち出すこと。

（２）業務用パソコン等以外のパソコン等及び県が管理していない外部記憶媒体を執務室に持ち込まないこと。

業務上やむを得ず持ち込む必要がある場合は、様式第４号により、情報セキュリティ管理者又は情報システム管理者に対して、その理由とともに、不正プログラムの感染防止策を申し出て、許可を得ること。

ただし、私物のパソコン及び外部記憶媒体等については許可しないものとする。

（３）情報セキュリティ管理者又は情報システム管理者が利用を認めたソフトウェア以外のソフトウェアを導入しないこと。

業務上やむを得ず導入する必要がある場合は、情報セキュリティ管理者又は情報システム管理者に対して、その理由とともに、当該ソフトウェアの安全性を申し出て、許可を得ること。

ただし、情報政策課長が配備するパソコン等にあっては、情報政策課長の許可を得ること。

なお、原則として、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。

（４）改造、機器の増設又はネットワークへの接続を行わないこと。

業務上やむを得ず改造、機器の増設又はネットワークへの接続を行う必要がある場合は、情報セキュリティ管理者又は情報システム管理者に対して、その理由とともに、当該パソコン等への影響度等を申し出て、許可を得ること。

ただし、情報政策課長が配備するパソコン等にあっては、情報政策課長の許可を得ること。

（５）ソフトウェアは、県が保有するライセンス数の範囲内で利用するものとし、不正にコピーしたソフトウェアを利用しないこと。

（６）離席する際は、画面をロックする等により、第三者に業務用パソコン等を使用又は閲覧されないようにすること。

（研修）

第２２条　情報政策課長は、研修の実施等により、職員に対し、定期的に情報セキュリティに関する啓発を行わなければならない。

２　職員は、定められた研修に参加し、情報セキュリティに関する知識の習得及び関連規程等の理解に努めなければならない。

（ＩＣカード等の管理）

第２３条　職員は、本人の確認のために発行されたＩＣカード等の紛失並びにＩＤ及びパスワードの漏えいを防止するため、次の事項を遵守しなければならない。

（１）ＩＣカードの取り扱い

ア　ＩＣカード等を使用しないときは、施錠可能な場所に保管すること。

イ　業務上止むを得ない場合を除き、ＩＣカード等を、職員等間で共有してはならない。

（２）ＩＤの取り扱い

ア　自己が利用しているＩＤは、他人に利用させてはならない。

イ　業務上止むを得ない場合を除き、ＩＤを共用で利用してはならない。

（３）パスワードの取り扱い

ア　パスワードは、他者に知られないように注意するとともに、業務用パソコン等にパスワードを記憶させないようにすること。

イ　容易に推測及び解読されないように、文字列は英数字及び記号を組み合わせて、十分な長さの文字列にすること。

ウ　同一のパスワードを複数の情報システムで使用しないこと。

エ　職員間でパスワードを共有しないこと。（ＩＤを共用している場合を除

く。)

第６章　技術的セキュリティ対策

（情報収集及び技術評価）

第２４条　情報政策課長及び情報システム管理者は、不正アクセス及び不正プログラムによる情報資産の漏えい等の事例並びにソフトウェアの情報セキュリティ上の問題に関する情報の収集とともに、これらに対応するための最新技術の評価に努めなければならない。

２　情報政策課長は、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、情報資産の安全性の維持向上が図られるよう指導を行わなければならない。

第２５条及び第２６条　削除

（ネットワークのアクセス制御）

第２７条　情報システム管理者は、所管する情報システムのネットワークに関し、当該情報システムへの不正アクセスを防止するため、次の措置を講じなければならない。

（１）接続制御及び経路制御

機密性の向上及び不正アクセスによる影響の最小化を図るため、通信可能なネットワークの区域を分割し、適切な接続制御及び経路制御を施すこと。

（２）外部ネットワークとの接続

ア　外部のネットワークと接続しようとする場合には、当該外部ネットワークの構成及び情報セキュリティ技術を調査し、県の情報資産に影響が生じないことを明確にした上で、情報政策課長の許可を得ること。

イ　外部ネットワークとの接続に当たっては、通信方式を制限し、不要な通信経路を閉鎖すること。

ウ　外部からの不正アクセス及び業務妨害のための指令等を検知又は排除する機能を導入し、常にその機能を最新の状態に保つこと。

エ　管理する情報の機密性に応じて、万一不正プログラムが侵入した場合でも、外部への不正な情報の送信を検知し遮断する対策を講じること。

オ　接続している外部ネットワークの情報セキュリティに問題が認められ、県の情報資産に脅威が生じることが想定される場合には、速やかにそのネットワークを物理的に切り離すこと。

カ　業務用パソコン等以外のパソコン等から所管する内部のネットワーク及び情報システムに直接アクセスできないようにすること。

業務上やむを得ず、職員に業務用パソコン等以外のパソコン等から直接アクセスさせる必要がある場合は、少なくとも次の事項が遵守されることを明確にした上で、情報政策課長の許可を得ること。

（ア）利用者本人及び機器の真正性を確認できる機能を設けること。

（イ）暗号化等により通信の安全性を確保すること。
（ウ）利用するパソコン等に不正プログラム対策を実施すること。
（エ）利用するパソコン等にデータを保存しないこと。

（３）不正アクセスを受けた場合の対応

ア　不正アクセスの被害事例の多発等により、不正アクセスを受ける可能性が高いと判断される場合は、アクセス状況の監視体制を強化するとともに、情報政策課長及び関係機関と連絡を密にして情報の収集に努めること。

イ　不正アクセスを受けたときは、アクセス記録を保存の上、速やかに情報政策課長に連絡し、必要な指示を受けること。

なお、その内容が不正アクセス禁止法その他の法令違反の可能性がある場合は、警察及びその他関係機関との連携に努めること。

（不正プログラム対策）

第２８条　情報セキュリティ管理者及び情報システム管理者は、不正プログラムの感染及び感染拡大を防止するため、次の措置を講じなければならない。

（１）所管する業務用パソコン等のすべてに、不正プログラム対策ソフトを導入し、常にその定義ファイルを最新の状態に保つこと。

（２）所管する業務用パソコン等が不正プログラムに感染していないか、定期的に不正プログラム対策ソフトによる全ファイルのチェックを実施すること。

（３）前条第１項第３号イの規定は、不正プログラムを検知した場合又は不正プログラムに感染した疑いがある場合について、準用すること。

２　職員は、不正プログラムの感染及び感染拡大を防止するため、次の事項を遵守しなければならない。

（１）外部記憶媒体の授受、電子メールの添付ファイルの受信又はネットワーク経由でのダウンロードの手段により、外部から電子情報を入手するときは、不正プログラム対策ソフトにより、当該電子情報が不正プログラムに感染していないことを確認すること。

（２）外部に持ち出した業務用パソコン等を再び内部ネットワークに接続するに当たっては、当該パソコン等が不正プログラムに感染していないことを確認すること。

（３）不正プログラムを検知したとき又は不正プログラムに感染した疑いがあるときは、業務用パソコン等を速やかにネットワークから遮断するとともに、情報セキュリティ管理者に報告すること。

（無線ＬＡＮの利用）

第２９条　職員は、情報政策課長が整備する無線ＬＡＮ以外の無線ＬＡＮを利用してはならない。

２　情報セキュリティ管理者及び情報システム管理者は、業務上やむを得ず情報政策課長が整備する無線ＬＡＮ以外の無線ＬＡＮを利用する場合は、情報政策課長の許可を得た上で、指定された安全対策を実施しなければならない。

（インターネットの利用）

第３０条　情報セキュリティ管理者及び情報システム管理者は、業務上インターネットを利用する場合は、職員の業務目的以外の利用を防止するため、適切なフィルタリング及び利用記録の取得を行わなければならない。

ただし、情報政策課長が配備するパソコン等で全庁的に利用するインターネットの利用については、情報政策課長が適切なフィルタリング及び利用記録の取得を行うものとする。

２　情報セキュリティ管理者及び情報システム管理者は、業務上約款による外部サービスを利用する（委託契約等により事業者等に当該サービスを指定し利用させる場合を含む。）場合は、利用するサービスの約款、利用規約及びその他の提供条件等を確認し、利用に当たってのリスクを踏まえ、次の事項を遵守した上で利用しなければならない（第３項の場合を除く。）。

（１）サービス上で取り扱う電子情報は、原則として別表第 1 に掲げる機密性２又は機密性３に分類される情報とすること。

（２）機密性２の情報を取り扱う場合は、取り扱う情報の機密性に応じた情報セキュリティ対策が確保されたサービスを選定し、様式第５号により情報政策課長の許可を得ること。また、次の事項を明記した利用要領等を整備すること。

ア　利用するサービス

イ　利用責任者（利用アカウントの責任者）

ウ　サービス利用者の範囲

エ　利用目的

オ　サービス上で取り扱う電子情報

カ　サービスの利用手順

キ　事故発生時の対処手順

（３）送信又は保存した電子情報の管理状況については、様式第６号により常時把握すること。

（４）アカウントを作成する際にメールアドレスが必要な場合は、業務用のメールアドレスを使用し、私用のメールアドレスは使用しないこと。

また、業務上止むを得ない場合を除き、所属のメールアドレスを使用すること。

（５）運用に当たっては次に掲げる業務を定期的に実施すること。

ア　アカウントのＩＤ及びパスワードの管理状況の確認

イ　サービス機能設定（公開設定等）に関する内容の確認

ウ　電子情報の整理及び不要な電子情報の消去
エ　情報の滅失、破壊等に備えたバックアップの取得
オ　アカウント利用記録等の確認
カ　サービス上で発生した事故及び障害情報等の収集及び対処
キ　サービスの約款、利用規約及びその他の提供条件等の変更の確認
ク　その他情報の安全管理に必要な業務

3　情報セキュリティ管理者及び情報システム管理者は、約款による外部サービスのうち生成AIサービスを利用する（委託契約等により事業者等に当該サービスを指定し利用させる場合を含む。）場合は、利用するサービスの約款、利用規約及びその他の提供条件等を確認し、利用に当たってのリスクを踏まえ、次の事項を遵守した上で利用しなければならない。

（1）サービス上で取り扱う電子情報は、別表第1に掲げる機密性3に分類される情報に限ること。

（2）生成AIサービスを利用する場合は、事前に情報政策課長に協議を行うこと。

（3）アカウントを作成する際にメールアドレスが必要な場合は、業務用のメールアドレスを使用し、私用のメールアドレスは使用しないこと。

また、業務上止むを得ない場合を除き、所属のメールアドレスを使用すること。

4　情報セキュリティ管理者及び情報システム管理者は、クラウドサービスを利用する（委託契約等により事業者等に当該サービスを指定し利用させる場合を含む。）場合は、取り扱う情報の機密性に応じた情報セキュリティ対策が確保されているサービスを選定し、様式第5号により情報政策課長の許可を得ること。

5　ソーシャルメディアの利用に当たっては、「福岡県ソーシャルメディア利用ガイドライン」を遵守すること。

（電子メールの利用）

第31条　職員は、電子メールの利用に当たっては、次に掲げる事項を遵守しなければならない。

（1）情報の持ち出し防止

自動転送機能を用いた電子メールの転送及び次に掲げる業務上必要な電子メール以外の送信を行ってはならない。

また、外部に添付ファイルを送る際は、上長のアドレスをCCに入れなければならない。

ア　文書管理規定に則って施行する電子メール
イ　通信連絡手段としての電子メール（ただし、職員の私用メールアドレスへの送信は、簡易な連絡や所属長が必要と認めた場合に限る。）

（２）不審な電子メールへの対応

ア　添付ファイルの開封等の禁止

差出人の詐称が疑われる等の不審な電子メールを受信した場合は、添付ファイルの開封及び電子メールに記述されたリンク先への接続を行うことなく、情報セキュリティ管理者に報告すること。

イ　情報政策課長への連絡

報告を受けた電子メールについて、情報セキュリティ管理者は、速やかに情報政策課長に連絡し、その指示に従い必要な措置を講じること。

（３）電子メール誤送信の防止

ア　宛先の誤りの防止

電子メールを送信する場合は、宛先の誤りによる情報漏えいが発生しないよう、十分に注意して宛先を指定すること。

イ　複数宛先の電子メールアドレスの表示防止

同時に複数の宛先に電子メールを送信する場合、特に表示の必要がある場合を除いて、他の送信先の電子メールアドレスが表示され、漏えいしないようにすること。

ウ　情報セキュリティ管理者への報告

電子メールを誤送信した場合は、速やかに情報セキュリティ管理者に報告すること。報告を受けた情報セキュリティ管理者は、直ちに送信先に連絡を取り、当該電子メール又は他の送信先の電子メールアドレスの消去を依頼する等必要な措置を講じること。

（４）個人情報の適正な管理

別表第１に掲げる機密性１に分類される電子情報を電子メールで送信する必要がある場合は、当該電子情報へのパスワードの設定による暗号化を行うなどの必要な措置を講じなければならない。ただし、約款による外部サービスであるメールシステムからの送信は原則として認められない。

第７章　運用

第３２条　削除

（緊急時対応手順）

第３３条　情報セキュリティ管理者及び情報システム管理者は、事故発生時における連絡、事故原因の調査、被害拡大の防止等の措置を適切に講じるため、緊急時対応手順を策定しなければならない。

２　緊急時対応手順には、次の内容を定めるものとする。

（１）連絡体制及び責任者

（２）事故に関して報告すべき事項

（３）事故原因の調査方法

（４）被害拡大の防止

（５）事故の形態に応じた復旧方法

（６）その他緊急時対応として必要な事項

３　情報セキュリティ管理者及び情報システム管理者は、随時、緊急時対応手順の見直しを行うほか、必要に応じて緊急時対応訓練の計画を策定し、実施しなければならない。

（事故の対応）

第３４条　職員は、業務用パソコン等及び外部記憶媒体等の紛失、電子メールの誤送信、不正アクセス並びに不正プログラムの感染等による事故の発生を知った時は、前条に定める緊急時対応手順に従い、直ちに情報セキュリティ管理者に報告し、その指示に従い必要な措置を講じなければならない。

２　情報セキュリティ管理者は、報告のあった事故について、前条に定める緊急時対応手順に従い、様式第７号により、速やかに関係する情報システム管理者及び情報政策課長へ報告し、その指示に基づき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及び情報政策課長は、報告のあった事故に関して、互いに協力し、原因の究明と対応策を協議するとともに、当該情報セキュリティ管理者に対して、具体的な対応策を指示しなければならない。

４　情報政策課長は、発生した事故の影響の程度に応じて、最高情報責任者及び企画・地域振興部長に報告しなければならない。

５　情報セキュリティ管理者、情報システム管理者及び情報政策課長は、報告のあった事故について、事故原因の検証に基づく再発防止策を講じるとともに、事故の記録を保存しなければならない。

（外部委託）

第３５条　情報セキュリティ管理者及び情報システム管理者は、委託契約等に

より、情報処理及び情報資産の管理に関する業務を事業者に依頼しようとするときは、この基準の遵守を求め、必要な情報セキュリティ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及び情報システム管理者は、事業者との間で、次の事項を明記した契約を締結しなければならない。

（１）情報の目的外利用、外部への提供及び複製の禁止に関する事項

（２）第１３条第２項に定める情報セキュリティ対策の実施に関する事項

（３）再委託の禁止又は制限に関する事項

（４）委託業務終了時の情報資産の返還、廃棄等に関する事項

（５）事故発生時の県への緊急報告に関する事項

（６）情報セキュリティに関する従業員の教育の実施に関する事項

（７）この基準に違反した場合の契約の解除及び損害賠償に関する規定に関する事項

３　情報セキュリティ管理者及び情報システム管理者は、事業者における情報セキュリティ対策の実施状況を把握しなければならない。

４　情報セキュリティ管理者及び情報システム管理者は、必要な情報セキュリティ対策が実施されていないことを把握した場合には、事業者に対し、速やかに是正措置を講じさせなければならない。

５　事業者に対して業務の再委託を認める場合は、第１項から第４項までの規定は、再委託を受ける事業者にも適用するものとする。

第３６条　削除

（法令遵守）

第３７条　職員は、使用する情報資産を保護するため、次の法令等を遵守し、これに従わなければならない。

（１）地方公務員法（昭和２５年法律第２６１号）

（２）著作権法（昭和４５年法律第４８号）

（３）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）

（４）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）

（５）サイバーセキュリティ基本法（平成２６年法律第１０４号）

（６）特定個人情報の適正な取扱いに関するガイドライン　（行政機関等・地方公共団体等編）（平成２６年特定個人情報保護委員会告示第６号）

（７）個人情報の保護に関する法律（平成１５年法律第５７号）

（８）福岡県個人情報の保護に関する法律施行条例（令和４年福岡県条例第４３号）

（９）福岡県文書管理規程（平成１６年福岡県訓令第１号）

（１０）知事が保有する個人情報の適切な管理のための措置に関する規程（令和４年福岡県訓令第６号）

（この基準の開示）

第３８条　この基準は、情報セキュリティ対策の効果を確実とするため、原則として非開示とする。

２　情報セキュリティ管理者及び情報システム管理者は、業務を実施するに当たり、この基準を事業者等に開示する必要が生じた場合は、契約書又は書面を通じて、この基準の内容について機密を保持するよう求めなければならない。

（違反への対応）

第３９条　この基準に違反した職員は、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。

第８章　監査及び見直し

（情報セキュリティ監査）

第４０条　企画・地域振興部長は、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て、定期的に、又は必要に応じて、所管する情報資産に関する情報セキュリティ対策の実施状況を確認するため、情報セキュリティ監査（以下「監査」という。）を実施するものとする。

２　監査における実地調査及び改善指導は、企画・地域振興部長の指示に基づき、情報政策課長が行うものとする。

３　監査対象となる所属及び情報システムを所管する情報セキュリティ管理者及び情報システム管理者は、監査の実施に協力しなければならない。

４　情報政策課長は、監査結果を監査報告書に取りまとめ、企画・地域振興部長に報告しなければならない。

５　情報セキュリティ管理者及び情報システム管理者は、監査の結果、改善が必要とされた事項については速やかに是正措置を講じなければならない。

６　事業者に委託して監査を実施する場合、中立性及び独立性を確保するため、委託先は、監査対象である情報システムの開発又は運用保守業務を委託又は再委託されている事業者であってはならない。

（自己点検）

第４１条　情報セキュリティ管理者及び情報システム管理者は、所管する情報資産における情報セキュリティ対策の実施状況について、定期的に、又は必要に応じて、自己点検を行い、その結果を情報政策課長に報告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、自己点検の結果、改善が必要と判断される事項については、速やかに是正措置を講じなければならない。

（調査）

第４２条　情報政策課長は、不正プログラムの侵入、通信量の急激な増加その他の異常を検知し、又はこの基準に違反する行為により事故の発生のおそれがあると判断したときは、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て、報告を求め、又は調査を行い、必要な改善措置を指導することができる。

（情報セキュリティ対策基準の見直し）

第４３条　企画・地域振興部長は、情報セキュリティに関係する社会状況の変化等を踏まえ、必要があると認めた場合、この基準の見直しを行うものとする。

附　則

（施行期日）

１　この基準は、平成１４年１２月２７日から施行する。

（福岡県セキュリティ対策基準の廃止）

２　福岡県セキュリティ対策基準（平成１１年８月２日施行）は、廃止する。

附　則

（施行期日）

１　この基準は、平成１９年１１月１日から施行する。

附　則

（施行期日）

１　この基準は、平成２４年１０月１日から施行する。

附　則

（施行期日）

１　この基準は、平成２６年４月１日から施行する。

附　則

（施行期日）

１　この基準は、平成２７年１０月５日から施行する。

附　則

（施行期日）

１　この基準は、平成２９年１月１日から施行する。

附　則

（施行期日）

１　この基準は、平成２９年４月１日から施行する。

附　則

（施行期日）

１　この基準は、平成３０年２月５日から施行する。

附　則

（施行期日）

１　この基準は、令和２年２月１０日から施行する。

附　則
（施行期日）
１　この基準は、令和２年４月１日から施行する。

附　則
（施行期日）
１　この基準は、令和２年１２月２８日から施行する。

附　則
（施行期日）
１　この基準は、令和３年９月１日から施行する。

附　則
（施行期日）
１　この基準は、令和４年４月１日から施行する。

附　則
（施行期日）
１　この基準は、令和５年４月１日から施行する。

附　則
（施行期日）
１　この基準は、令和５年５月１１日から施行する。

附　則
（施行期日）
１　この基準は、令和７年４月１日から施行する。

別表第１（第１１条関係）

備考　１　情報資産は、機密性、完全性及び可用性の３つの観点から、それぞれの分類基準に応じて、重要性の高い順に３段階又は２段階に分類するものとする。

（１）機密性　認められた者だけが情報資産を利用できるようにすること。

（２）完全性　情報資産に毀損、改ざん、誤り等のない正確で完全な状態を保つこと。

（３）可用性　認められた者が必要なときにいつでも情報資産を利用できるようにすること。

２　同一の外部記憶媒体に、分類の異なる複数の情報が記録されている場合は、最高度の分類に応じて、当該外部記憶媒体を取り扱わなければならない。

機密性による分類

分類	分類基準
機密性１	福岡県情報公開条例第７条第１項各号の非開示情報のうち、個人情報に該当する情報
機密性２	機密性１を除く非開示情報及び公開していない情報
機密性３	上記以外の情報

完全性による分類

分類	分類基準
完全性１	改ざん若しくは誤りがあると住民の権利が侵害され、又は行政事務の適確な遂行に支障を及ぼすおそれがある情報
完全性２	上記以外の情報

可用性による分類

分類	分類基準
可用性１	利用できないと住民の権利が侵害され、又は行政事務の安定的な遂行に支障を及ぼすおそれがある情報
可用性２	上記以外の情報

別表第２（第１７条関係）

情報資産の種類（リース機器・クラウドサービス利用含む）	廃棄時の措置	事業者等に廃棄時の措置を行わせる場合の確実な履行の担保方法
（１）特定個人情報が記録された情報資産又はマイナンバー利用事務専用システム管理運用要領第２条第４項に定める利用事務系ネットワークに接続する情報資産	原則、物理的な破壊（分解、粉砕、溶解、焼却及び細断等）により、当該情報資産内部の記憶装置を復元不可能な状態にすること。	職員が措置の完了まで立会による確認を行うこと又は庁舎内において後述（３）の方法により電子情報の抹消を行った後、事業者等に情報資産を引き渡し、破壊の証拠写真が添付された物理的破壊の完了証明書を受領すること。 ※職員による措置の完了までの立ち会いについては、委託先事業者の作業状況が確認出来る場合、カメラによるリアルタイムでの監視やカメラ映像の記録の確認などで代替できる。
（２）（１）以外の機密性１の電子情報又は機密性２の電子情報が保存された情報資産	物理的又は磁気的な破壊により当該情報資産を復元不可能な状態にすること又は後述（３）のアからエいずれかの方法により、情報資産内部の記憶装置に記録された電子情報を抹消すること。	庁舎内において後述（３）の方法により電子情報の抹消を行った後、事業者等に情報資産を引き渡し、措置の完了証明書を受領すること。
（３）機密性３の電子情報が保存された情報資産	次のいずれかの方法により、情報資産内部の記憶装置に記録された電子情報を抹消すること。 ア　HDD 内蔵のコマンド（Enhanced SECURITY ERASE）実行による上書き消去 イ　SSD 内蔵のコマンド（BLOCK ERASE）実行によるブロック消去 ウ　暗号化消去（データを暗号化して保存している場合のみ） エ　ＯＳ等からのアクセスが不可能な領域も含めた領域のデータ消去ソフトウェア等による上書き消去 オ　ＯＳ等からアクセス可能な全ての領域のデータ消去ソフトウェア等による上書き消去	庁舎内において消去を実施し、職員が作業完了を確認すること。