別紙

愛媛県情報セキュリティポリシー

（平成14年６月13日　　愛媛県高度情報化推進本部決定）
（平成18年４月１日　　改正）
（平成18年６月27日　　改正）
（平成21年４月１日　　改正）
（平成23年４月１日　　改正）
（平成25年10月１日　　改正）
（平成28年１月15日　　改正）
（平成30年４月１日　　改正）
（令和２年４月１日　　改正）
（令和３年４月１日　　改正）
（令和４年１月14日　　改正）
（令和５年４月１日　　改正）
（令和７年10月31日　　改正）
（令和８年４月１日　　改正）

愛媛県情報セキュリティポリシー

第１　趣旨

愛媛県情報セキュリティポリシー（以下「ポリシー」という。）とは、愛媛県（以下「県」という。）が所掌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、体系的かつ具体的に取りまとめたものを総称し、県の情報セキュリティ対策の頂点に位置するものである。

第２　構成

ポリシーは、一定の普遍性を備えた部分である「愛媛県情報セキュリティ基本方針」及び情報資産を取り巻く状況の変化に依存する部分である「愛媛県情報セキュリティ対策基準」により構成される。

愛媛県情報セキュリティ基本方針

目　　　　次

愛媛県情報セキュリティ基本方針

第１　目的

近年のデジタル技術の進展に伴い、各種の情報がネットワークや情報システムを通じて処理され､又は伝達されている。特に、県が取り扱う情報には、県民の個人情報のみならず行政運営や学校運営上重要な情報など、外部への漏洩、喪失、毀損､改ざん等が生じた場合に極めて重大な結果を招く情報が多数含まれており、またネットワークや情報システムそのものの不正利用や不正処理による影響により､県民生活に重大な危機を及ぼすおそれも生じている。

こうした情報資産を様々な脅威から防御することは、県民の財産、プライバシー等を保護するとともに、行政事務の安定的な執行や、学校での質の高い教育環境を確保するためにも必要不可欠であり、ひいては、県民からの県行政や県教育に対する信頼の維持向上に寄与するものである。

また、デジタル技術の積極的な活用により、行政事務の効率化、教育のデジタル化、県民生活の質の向上及び地域経済の活性化などの実現を目指し、様々な分野においてＤＸ（Digital Transformation：デジタル変革）に取り組む必要があるが、県がこれらに積極的に対応するためには、すべての情報資産が高度な安全性を有することが不可欠な前提条件である。

このため、県が保有する情報資産の情報セキュリティのための対策（以下「情報セキュリティ対策」という。）を総合的、統一的かつ効果的に実施することが必要であり、その基本的な方針として、この愛媛県情報セキュリティ基本方針（以下「基本方針」という。）を定めるものとする。

第２　定義

基本方針において、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) ネットワーク

県が管理する通信網、通信網を構成する機器（通信の処理を行うハードウェア及びソフトウェアをいう。）及び記録媒体で構成され、処理を行う仕組みをいう。

(2) 情報システム

県が管理する電子計算機（情報処理を行うハードウェア及びソフトウェアをいう。）及び記録媒体で構成され、個別の業務処理を行う仕組みをいう。

(3) 外部サービス（クラウドサービス）

事業者等の県以外の組織が、業務処理を行う仕組みの一部又は全部の機能を提供するものをいう。ただし、当該機能において県の情報が取り扱われる場合に限る。

(4) 情報

ネットワーク、情報システム及び外部サービス（クラウドサービス）で扱うデータをいう。

(5) 情報資産

ネットワーク、情報システム及び外部サービス（クラウドサービス）（これらに付随する

開発、運用及び保守のための資料等を含む。）並びに情報をいう。

(6) 情報セキュリティ

情報資産の機密性、完全性及び可用性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

国際標準化機構(ISO)の定義(ISO7498-2 ： 1989)
○機密性(confidentiality):情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
○完全性(integrity) :情報及び処理の方法の正確さ並びに完全である状態を安全防護すること。
○可用性(availability) :許可された利用者が必要なときに情報にアクセスできることを確実にすること。

第３　実施機関

基本方針に基づき、情報セキュリティ対策を実施する県の機関は、次のとおりとする。

(1) 知事部局
(2) 公営企業管理局
(3) 人事委員会
(4) 議会
(5) 選挙管理委員会
(6) 監査委員
(7) 教育委員会（教育委員会が所管する県立学校を含む。）
(8) 労働委員会
(9) 収用委員会
(10) 海区漁業調整委員会
(11) 内水面漁場管理委員会

第４　職員等の義務

情報資産に関する業務に携わるすべての職員等（特別職、県議会議員、実施機関の委員、会計年度任用職員、特別職非常勤職員、派遣職員及び委託事業者を含む。以下同じ。）は、情報セキュリティの重要性について共通の認識を深めるとともに、業務の遂行に当たって、基本方針を遵守する義務を負うものとする。

第５　情報セキュリティ管理体制

県が所有するすべての情報資産の情報セキュリティを統括するため、別に定めるところにより最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）を置き、ＣＩＳＯの下に、情報セキュリティ対策を推進し、管理するための体制を確立するものとする。

第６　情報資産の分類と管理

情報資産をその内容に応じて分類し、管理責任を明確にするとともに、情報セキュリティ対策基準において定める重要性に応じた情報セキュリティ対策を行うものとする。

第７　情報資産への脅威

情報セキュリティ対策を推進する上で、特に情報資産への脅威は、その発生度合や発生した場合の影響を考慮すると、次のとおりである。

(1) 構成員以外の者による故意の不正アクセス又は不正操作によるデータやプログラムの持出、盗聴、改ざん又は消去、機器又は媒体の盗難等

(2) 構成員による意図しない操作又は故意の不正アクセス若しくは不正操作によるデータやプログラムの持出、盗難、改ざん又は消去、機器又は媒体の盗難、規定外の端末機接続によるデータ漏洩等

(3) 地震、落雷、火災等の災害、事故、故障等によるサービス又は業務の停止

第８　情報セキュリティ対策

第７に掲げる脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

(1) 物理的セキュリティ対策

ネットワーク、情報システム及び外部サービス（クラウドサービス）を設置する施設への不正な立入り並びに情報資産への損傷、妨害等から保護するために必要な物理的な対策

(2) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、すべての構成員にポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるために必要な対策

(3) 技術及び運用におけるセキュリティ対策

ア　情報資産を外部からの不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策及びシステム開発等の業務委託、ネットワークの監視、ポリシーの遵守状況の確認等の運用面の対策

イ　緊急事態が発生した際に、迅速な対応を可能とするための対策

(4) 業務委託と外部サービス（クラウドサービス）の利用におけるセキュリティ対策

ア　業務委託を行う場合には、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、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く措置を求める対策

イ　外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備する対策

ウ　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対策

第９　情報セキュリティ対策基準の策定

県の様々な情報資産について、第８の情報セキュリティ対策を講ずるに当たっては、遵守

すべき行為、判断等の基準を統一的な水準で定める必要があるため、ＣＩＳＯは、情報セキュリティ対策を行う上で必要となる基本的な基準を明記した愛媛県情報セキュリティ対策基準（以下「対策基準」という。）を別途策定するものとする。なお、情報セキュリティ対策基準については、各実施機関において必要に応じ、独自に策定することができる。

第 10　情報セキュリティ実施手順の策定

情報資産管理者（情報資産を所掌する課(室)の長をいう。）は、情報資産に対する脅威及び情報資産の重要性に対応して、対策基準に定める基本的な基準に基づき、その所掌する情報資産について、情報セキュリティ対策の実施手順を策定するものとする。

第 11　評価及び見直しの実施

ＣＩＳＯは、ポリシーが遵守されていることを検証するため、定期的に監査等を実施した上で、その結果に基づきポリシーに定める事項及び情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応させるため、必要であると認めるときは、ポリシーの見直しを実施するものとする。

第 12　違反への対応

この基本方針及び対策基準に違反した者及びその管理者については、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等の対象となる。

第 13　教育委員会所管の県立学校における情報セキュリティ対策

教育委員会が所管する県立学校に係る情報セキュリティ対策のための基本的な方針及び対策の基準については、基本方針及び対策基準の目的及び趣旨の範囲内において、県立学校特有の情報資産に係る情報セキュリティ対策として最適な方針及び基準を、愛媛県教育情報化推進本部において別途策定するものとする。

愛媛県情報セキュリティ対策基準

目　　　次

愛媛県情報セキュリティ対策基準

第１　目的

県が所掌する情報資産のセキュリティ対策を進めるため､愛媛県情報セキュリティ基本方針（以下「基本方針」という。）に基づき、情報セキュリティ対策を行う上で必要となる基本的な基準として、この愛媛県情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

第２　用語

対策基準で使用する用語の意義は、基本方針で使用する用語の例による。

第３　組織及び体制

基本方針第５で規定する情報セキュリティ管理体制として、ＣＩＳＯ及び別に定めるところにより設置される情報セキュリティ委員会（以下「委員会」という。）、情報セキュリティに関する緊急対応チーム（以下「ＣＳＩＲＴ」という。）並びに次の各号に掲げるネットワーク管理者等を置き、当該各号に定める職にある者をもって充てる。この場合において、情報セキュリティに係る組織及び体制は、別図のとおりとする。

(1)　ネットワーク管理者　企画振興部スマート行政推進課長
(2)　情報システム管理者　情報システムを所掌する課(室)の長
(3)　情報システム担当者　情報システムを所掌する課(室)の担当職員
(4)　情報セキュリティ管理者　各課(室)長
(5)　情報セキュリティ担当者　デジタルシフト推進員

第４　情報資産の分類及び管理

１　情報の分類及び管理

(1) 情報の分類

基本方針第６の規定に基づき、対象となる情報の機密性、完全性及び可用性を踏まえ、表の左欄に掲げる情報の内容の区分に応じ、同表の右欄に掲げる重要性分類のとおり分類する。

情報の内容	重要性分類
業務上必要とする最小限の者のみが扱う情報（「愛媛県文書管理規程」に定める秘密文書に相当する文書及び極秘の情報を含む。）	第Ⅳ分類の２
漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報（個人情報を含む。）	第Ⅳ分類の１

公開することを予定していない情報（秘の情報を含む。）	第Ⅲ分類
外部に公開する情報のうち業務上重要な情報	第Ⅱ分類
上記以外の情報	第Ⅰ分類

(2) 情報の管理

情報を所掌する課（室）の長（以下「情報管理者」という。）は、所掌する情報を前号の重要性分類に従って分類し、次に掲げる事項に留意しながら適切に管理しなければならない。

ア　情報の分類の表示

第三者が重要性の識別を容易に認識できないよう留意しつつ、ファイル名、記録媒体等に情報の分類が分かるように表示をする等適切な管理を行うこと。

イ　情報の管理及び取扱い

（ア）情報の重要性分類に応じ、所要のアクセス権限を定めること。

（イ）情報の複製、利用、持出し等については、法令等に別に定めのあるものを除き、必要に応じ情報管理者の許可を得ること。

（ウ）特に重要な情報（重要性分類第Ⅳ分類の１及び第Ⅳ分類の２のものをいう。）については、暗号化等（ファイルへのパスワード設定を含む。以下同じ。）及びバックアップの手法により厳格な管理を行うこと。

（エ）重要な情報（重要性分類第Ⅲ分類以上のものをいう。）の持ち出しに当たっては、暗号化等を行うこと。

（オ）業務上利用しなくなった古い情報については、定期的に消去すること。

ウ　記録媒体の管理

（ア）取出しが可能な記録媒体は、管理簿を設ける等適切な管理を行うこと。

（イ）最終的に確定した情報の記録媒体は、容易に内容を変更できないような措置を講ずること。

（ウ）記録媒体に納められた情報は、複製を作成し分散して保管する等情報の重要性分類に応じ適切な保管及び管理の措置を講ずること。

（エ）記録媒体の輸送に当たっては、契約の相手方として信頼できる者を選定し、当該契約中に複製の禁止及び記録媒体の物理的保護に係る規定並びにこれに違反した場合の賠償責任について定める等、適切な契約を行うこと。

エ　記録媒体の処分

（ア）特に重要な情報（重要性分類第Ⅲ分類以上のものをいう。）を記録した記録媒体の廃棄をしようとするときは、情報管理者の許可を得た上で、情報セキュリティ管理者の承認を得ること。

（イ）記録媒体を廃棄する場合は、当該媒体に含まれる重要な情報（重要性分類第Ⅱ分類以上のものをいう。）は、情報を復元できないような措置を講じた上で廃棄すること。

（ウ）記録媒体を廃棄した場合は、廃棄の日時、担当者及び処理内容を記録し、及び保存すること。

(3) 情報の管理責任

ア　管理責任

情報管理者は、所掌する情報の管理責任を有する。

イ　利用者の責任

情報を利用する者は、情報の重要性分類に従い、これを利用する責任を有する。

ウ　重要性の効力

情報が複製され、又は伝送された場合においては、当該複製等についても、重要性分類に基づき、適切に管理しなければならない。

2　ネットワーク、情報システム及び外部サービス（クラウドサービス）の分類及び管理

(1) ネットワーク、情報システム及び外部サービス（クラウドサービス）の分類

基本方針第６の規定に基づき、対象となる情報の機密性、完全性及び可用性を踏まえ、次の表の左欄に掲げるネットワーク、情報システム及び外部サービス（クラウドサービス）（以下「情報システム等」という。）の内容の区分に応じ、同表の右欄に掲げる重要性分類のとおり分類する。

ネットワーク及び情報システム等の内容	重要性分類
第Ⅳ分類の２の情報を扱うネットワーク及び情報システム	第Ⅳ分類の２
第Ⅳ分類の１の情報を扱うネットワーク及び情報システム等	第Ⅳ分類の１
第Ⅲ分類の情報を扱うネットワーク及び情報システム等	第Ⅲ分類
第Ⅱ分類の情報を扱うネットワーク及び情報システム等	第Ⅱ分類
第Ⅰ分類の情報を扱うネットワーク及び情報システム等	第Ⅰ分類

(2) ネットワーク、情報システム及び外部サービス（クラウドサービス）の管理

ネットワーク管理者及び情報システム管理者（以下「情報システム管理者等」という。）は、所掌する情報システム等を前号の重要性分類に従って分類し、適切に管理しなければならない。

第５　情報セキュリティ対策

情報資産管理者は、その取り扱う情報資産の重要性に応じて、第６から第９までに定めるところにより、物理的､人的、技術的及び運用において必要な情報セキュリティ対策を講ずるものとする。

第６　物理的セキュリティ対策

情報システム管理者等は、情報セキュリティ対策のうち、物理的セキュリティ対策については、次に定める事項を基本として、取り扱う情報資産の重要性等を勘案し、必要な水準の対策を講ずるものとする。

1　サーバ等機器のセキュリティ対策

ネットワーク及び情報システムを構成するサーバ等のシステム機器（以下「サーバ等機器」という。）のセキュリティ対策は、次のとおりとする。

(1) サーバ等機器の取付け等

ア　サーバ等機器を設置する場合は、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な固定等、必要な措置を施すこと。

イ　次に掲げるサーバ等機器は、機器の二重化及びミラーリングによる同一データの常時保持等の措置により、障害発生時にシステムの運用停止を引き起こさないよう考慮すること。

（ア） 重要情報を格納しているサーバ
（イ） セキュリティサーバ
（ウ） 住民サービスに関するサーバ
（エ） その他の基幹サーバ

ウ　サーバ等機器は、ネットワーク管理者、情報システム管理者、情報システム担当者及び契約により操作を認められた外部委託事業者（以下「情報システム運用管理者等」という。）以外の者が容易に操作できないように、利用者のＩＤ、パスワードの設定等によるアクセス制限の措置を講ずること。

エ　サーバ等機器の設置に当たっては、ディスプレイ、配線等から放射される電磁波により特に重要な情報（重要性分類第Ⅲ分類以上のものをいう。）が外部に漏えいすることがないよう配慮すること。

⑵ 電源

ア　サーバ等機器の電源は、当該機器を適切に停止させるまでの間に十分な電力を供給する容量の予備電源を備えること。

イ　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施すこと。

⑶ 配線

ア　配線は、可能な限り、傍受又は損傷等を受けることがないよう必要な措置を施すこと。

イ　主要な箇所の配線は、損傷等についての定期的な点検を行うこと。

ウ　ネットワーク接続口(ハブのポート等をいう。)は、職員等以外の者が容易に発見できない場所に設置すること。

エ　情報システム運用管理者等以外の者が配線を変更し、又は追加できないように必要な措置を施すこと。

⑷ 県各機関外に設置する装置

ア　県各機関外へのサーバ等機器の設置は、ＣＩＳＯの承認を受けるとともに、定期的に当該サーバ等機器の情報セキュリティの水準について確認すること。

イ　県各機関外に持ち出される端末機、記録媒体等については、県各機関外での利用方法を定め、管理簿を設ける等適切に管理すること。

２　管理区域のセキュリティ対策

⑴ 管理区域

ア　ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための場所（以下「情報システム室」という。）については、水害対策及び確実な入退室管理を行うこと。

　また、情報システム室は､外部からの侵入が容易にできないよう無窓の外壁等で囲む等の措置を講ずること。

イ　情報システム室は、制御機能、鍵、警報装置等によって、許可のない者の立入りを防止する措置を講ずること。

ウ　情報システム室には、ビデオカメラ等の監視機能を設置すること。

エ　情報システム室内に設置する機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を施すこと。なお、情報システム室内の機器類の配置は、緊急時の円滑な避難に配慮しておくこと。

オ　情報システム室を囲む外壁等の床下開口部は、すべて塞いであること。

カ　消火剤は、機器及び記録媒体に影響を与えないものを配備すること。

(2) 情報システム室の入退室管理

情報システム室に入退室することができる者は、許可された者のみとし、ＩＣカード等による入退室管理又は入退室管理簿への記載等により管理をすること。なお、入退室を許可された者は、入退室時には、身分証明書等を携帯し、情報システム運用管理者等の求めによりこれを提示すること。

また、情報システム管理者等は、入退室を許可された者が情報システム室に当該情報システムに関連しない端末機、通信回線装置、記録媒体等を持ち込ませないようにすること。

(3) 機器等の搬入及び搬出

ア　情報システム室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、情報システム運用管理者等による確認を受けること。

イ　機器等の搬入及び搬出には、情報システム運用管理者等が同行する等の必要な措置を施すこと。

3　ネットワークのセキュリティ対策

ア　外部へのネットワーク接続は、必要最小限のものに限定し、できる限り接続ポイントの数を減らすこと。

イ　行政系のネットワークは、総合行政ネットワークへの集約に努めること。

4　端末機等のセキュリティ対策

ア　執務室等に職員等がいない場合は、執務室の施錠等により、端末機の盗難防止のための物理的措置を施すこと。

イ　ＮＡＳ等の常設機器は、ワイヤーによる固定等盗難防止のための物理的措置を施すこと。

ウ　端末機のディスプレイ、配線等から放射される電磁波により重要な情報が外部に漏えいすることがないよう措置すること。

5　通信回線及び通信回線装置のセキュリティ対策

ア　庁内の通信回線及び通信回線装置を、適正に管理すること。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すること。

イ　情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施すること。

ウ　第Ⅱ分類以上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上、適正な回線を選択すること。また、必要に応じ、送受信される情報の暗号化を行うこと。

エ　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、不正な通信の有無を監視する等の十分なセキュリティ対策を実施すること。

オ　通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めること。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じること。

カ　第Ⅱ分類以上の情報を取り扱う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こと。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こと。

第７　人的セキュリティ対策

情報セキュリティ対策のうち、人的セキュリティ対策は、次に定める事項を基本として、取り扱う情報資産の重要性等を勘案し、必要な水準の対策を講ずるものとする。

１　権限、責任等

⑴ ＣＩＳＯ

ＣＩＳＯは、別に定めるところにより、県におけるすべての情報資産の情報セキュリティを統括する。

⑵ 委員会委員長

委員会委員長（以下「委員長」という。）は、ＣＩＳＯを補佐する。

⑶ 委員会

委員会は、別に定めるところにより、県のデジタル化施策に関する情報セキュリティ対策を統一的に実施する。

⑷ ＣＳＩＲＴ

ＣＳＩＲＴは、次に掲げる業務を行う権限及び責任を有する。

ア　別に定めるところにより、情報セキュリティインシデントが発生した際の初動対応及び情報収集を行い、事案の把握・分析、被害拡大防止、復旧、再発防止策を実施すること。

イ　ＣＩＳＯ及び委員長を補佐すること。

ウ　インシデント発生時の対応に必要な事前準備、及び予防対策を実施すること。

エ　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こと。

オ　情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省へ報告すること。

⑸ ネットワーク管理者

ネットワーク管理者は、次に掲げる業務を行う権限及び責任を有する。

ア　所掌するネットワークにおける開発、設定の変更、運用、更新等を行うこと。

イ　所掌するネットワークにおける情報セキュリティに関すること。

ウ　情報システム管理者、情報システム担当者、情報セキュリティ管理者及び情報セキュリティ担当者に対して、情報セキュリティに関する指導及び助言を行うこと。

エ　県の情報資産に対する侵害又はそのおそれがある場合は、ＣＳＩＲＴに対し速やかに報告を行い、その指示のもと事案への初動対応を実施するとともに、委員長の指示に従い、委員長が不在の場合には自ら代行して、必要かつ十分な措置を行うこと。

オ　所掌するネットワークに関する実施手順の作成、維持及び管理を行い、第９の４に定める緊急時対応計画の見直しを行うこと。

⑹ 情報システム管理者

情報システム管理者は、次に掲げる業務を行う権限及び責任を有する。

ア　所掌する情報システムにおける開発、設定の変更、運用、更新等を行うこと。

イ　所掌する情報システムにおける情報セキュリティに関すること。

ウ　所掌する情報システムに係る実施手順の作成、維持及び管理を行うこと。

エ　所掌する情報システムの情報資産に対する侵害又はそのおそれがある場合には、Ｃ

ＳＩＲＴに対し速やかに報告を行い、その指示を仰ぐこと。

オ　関係する情報セキュリティ管理者に対して、情報セキュリティに関する指導及び助言を行うこと。

(7) 情報システム担当者

情報システム担当者は、次に掲げる業務を行う権限及び責任を有する。

ア　担当する情報システムに関して、情報システム管理者の指示に従い、開発、設定の変更、運用、更新等の作業を行うこと。

イ　情報システム管理者の下、情報システムにおけるポリシーの遵守に関する業務を担当すること。

ウ　所掌する情報資産に対する侵害又はそのおそれがある場合には、情報システム管理者に対し速やかに報告を行い、その指示を仰ぐこと。

(8) 情報セキュリティ管理者

情報セキュリティ管理者は、次に掲げる業務を行う権限及び責任を有する。

ア　所属内におけるポリシーの遵守に関すること。

イ　所掌する情報資産に対する侵害又はそのおそれがある場合には、ＣＳＩＲＴ、ネットワーク管理者及び情報システム管理者に対し速やかに報告を行い、その指示を仰ぐこと。

(9) 情報セキュリティ担当者

情報セキュリティ担当者は、次に掲げる業務を行う権限及び責任を有する。

ア　情報セキュリティ管理者の下、所属内におけるポリシーの遵守に関する業務を担当すること。

イ　所掌する情報資産に対する侵害又はそのおそれがある場合には、情報セキュリティ管理者に対し速やかに報告を行い、その指示を仰ぐこと。

(10) 職員等

職員等は、次に掲げる事項を遵守しなければならない。

ア　基本方針､対策基準及び情報資産ごとの実施手順において定める事項

イ　使用する端末機や記録媒体について、第三者に使用されること及び許可なく情報を閲覧されることがないよう、適切な措置を施すこと。

ウ　使用する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すること。

エ　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等が生じた場合には、速やかに情報システム管理者及び情報セキュリティ管理者に報告し、その指示等を仰ぐこと。

オ　情報システム管理者及び情報セキュリティ管理者の許可を得ず、端末機や機器等を執務室外に持ち出してはならないこと。

カ　情報システム管理者及び情報セキュリティ管理者の許可を得ず、端末機や機器等を執務室内に持ち込み、業務に使用してはならないこと。

キ　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、返却又は消去しなければならないこと。また、その後も知り得た情報を秘匿しなければならないこと。

(11) 外部委託に関する管理

情報システム管理者等は、情報システム等の開発、保守等を外部委託事業者に発注す

る場合は、当該外部委託事業者の下請け事業者も含めて、当該外部委託事業者との間で、ポリシーのうち外部委託事業者が守るべき内容の遵守及びその守秘義務を明記した契約の締結及び説明を行わなければならない。この場合において、当該契約書には、第９の５(2)に定める契約項目についての規定を定めなければならない。

２　教育及び訓練

職員等に対する教育及び訓練は、次に定めるところにより行うものとする。

(1) ＣＩＳＯは、ポリシーに関して、説明会等による職員等への啓発及び新規採用職員等に対する研修を実施すること。

(2) ＣＳＩＲＴは、最新の技術力を維持するための研修を常に受講しておくこと。

(3) ＣＳＩＲＴは、緊急時対応を想定した職員等に対する訓練を、情報システム管理者等及び情報セキュリティ管理者に計画的に行わせること。

(4) 情報システム管理者等は、ネットワーク管理者向け又は情報システム管理者向けの研修を受講しておくこと。

(5) 情報セキュリティ管理者は、情報セキュリティ管理者向けの研修を受講するとともに、職員等に対する内部研修等の実施に努めること。

(6) 職員等は、定められた研修に参加し、ポリシー及び実施手順を理解し、情報セキュリティ上の問題が生じないようにすること。

３　情報セキュリティインシデントの報告

(1) 職員等は、情報セキュリティインシデントを認知した場合には、速やかに該当する情報システム管理者等に報告し、その指示に従い必要な措置を講じなければならない。

(2) 情報システム管理者等は､前号の報告を受けたときは、ＣＩＳＯ及びＣＳＩＲＴに報告しなければならない。

(3) ＣＳＩＲＴは、前号の報告を受けたときは、情報システム管理者等とともに職員等からの報告を分析してこれらの情報セキュリティインシデント原因を究明し、情報システム管理者等に対して、必要な指示を行わなければならない。また、ＣＳＩＲＴ は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

(4) 情報システム管理者等は、ＣＳＩＲＴとともに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、ＣＩＳＯ及び委員会に報告しなければならない。

(5) ＣＳＩＲＴ及び情報システム管理者等は、これら一連の分析・原因記録等を再発防止のための情報として記録を保存しなければならない。

(6) 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

(87) ＣＩＳＯは、情報システム管理者等及びＣＳＩＲＴから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。

４　ＩＤの管理

職員等は、自己の保有するＩＤに関し、次に掲げる事項を遵守しなければならない。

(1) 自己の保有するＩＤは、本人以外の者に利用させないこと。

(2) 共有ＩＤを利用する場合は、共有ＩＤの利用者以外の者に利用させないこと。

５　パスワードの管理

職員等は、自己の保有するパスワードに関し、次に掲げる事項を遵守しなければならない。

(1) パスワードを秘密にし、パスワードの照会等には、一切応じないこと。

(2) パスワードのメモを作らないこと。

(3) パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。

(4) 情報システム又はパスワードに対する危険のおそれがある場合には、パスワードを速やかに変更すること。

(5) パスワードは定期的に、又はアクセス回数に応じて変更し、古いパスワードの再使用はしないこと。

(6) 複数の情報システムを扱う職員等は、パスワードをシステム間で共有しないこと。

(7) 仮のパスワードは、最初のログイン時点で変更すること。

(8) 端末機にパスワードを記憶させないこと。必要に応じて暗号化等を行うことによって本人以外の者がパスワードを解読できないようにすること。

(9) 職員等間で個人のパスワードを共有しないこと。

6　ＩＣカード等の管理

(1) 職員等は、自己の保有するＩＣカード等に関し、次に掲げる事項を遵守しなければならない。

ア　ＩＣカード等の認証に用いるカード類は、職員等間で共有しないこと。

イ　ＩＣカード等は、カードリーダ又は端末機のスロット等に常時挿入しないこと。

ウ　ＩＣカード等を紛失した場合には、速やかに関係する情報システム管理者等に通報し、その指示を仰ぐこと。

(2) 情報システム管理者等は、所掌するＩＣカード等に関し、次に掲げる事項を遵守しなければならない。

ア　ＩＣカード等の紛失等の通報があり次第、速やかに当該ＩＣカード等を使用したアクセス等を停止すること。

イ　ＩＣカード等を切り替える場合、切替え前のＩＣカード等を回収し、破砕する等の復元不可能な処理を行った上で廃棄すること。

第８　技術的セキュリティ対策

情報セキュリティ対策のうち、技術的セキュリティ対策は、次に定める事項を基本として、取り扱う情報資産の重要性等を勘案し、必要な水準の対策を講ずるものとする。

1　コンピュータ及びネットワークの管理

(1) アクセス記録の取得等

情報システム管理者等は、重要な情報を扱う情報システム等について、次に掲げる措置を講じなければならない。

ア　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（以下「アクセス記録等」という。）をすべて取得し、一定の期間保存すること。

イ　アクセス記録等が窃取、改ざん又は消去をされないように必要な措置を施すこと。

ウ　定期的にアクセス記録等を分析し、及び監視すること。

(2) システム管理記録及び作業の確認

情報システム管理者等は、情報システム等の変更等の処理について、次に掲げる措置を講ずること。

ア　所掌する情報システム等の変更等の作業を行った場合は、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正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。

イ　情報システム担当者及び外部委託事業者が、所掌する情報システム等において作業を行う場合には、２名以上で作業させ、互いにその作業を確認させること。

(3) 障害記録

情報システム管理者等は、職員等からの報告に対する処理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) 情報システム仕様書等の管理

情報システム管理者等は、ネットワーク構成図、情報システム仕様書等について、記録媒体にかかわらず業務上必要とする者のみが閲覧できる場所に保管すること。また、構築に際して事業者に外部委託した場合は、当該事業者に守秘義務を課すこと。

(5) 情報及びソフトウェアの交換

職員等は、所属間において、情報システム等に関する情報及びソフトウェアを交換する場合は、その取扱いに関する事項をあらかじめ定め、情報システム管理者等の許可を得ること。

(6) バックアップ

ア　情報システム管理者等は、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かかわらず、その重要性に応じて期間を設定し、バックアップを実施すること。

イ　情報システム管理者等は、重要な情報を取り扱うサーバ装置について、適切な方法でサーバ装置のバックアップを取得しておくこと。

ウ　情報システム管理者等は、重要な情報を取り扱う情報システムを構成する通信回線装置について、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しておくこと。

(7) メール

ア　職員等は、メールの利用について、次に掲げる事項を行ってはならない。

（ア）情報システム管理者等の許可を得ず、標準（情報システム管理者等が提供するものをいう。）外のメールソフトを使用すること。

（イ）メールの自動転送機能を用いて、職場のメールを外部転送すること。

（ウ）暗号化等を行わずに、メールで重要な情報（重要性分類第Ⅲ分類以上のものをいう。）を送信すること。

（エ）業務上必要のない送信先にメールを送信すること。

（オ）複数人に電子メールを送信する際、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る状態にすること

イ　情報システム管理者等は、メールの処理について、次に掲げる措置を講じなければならない。

（ア）外部から外部へのメール転送（メールの中継処理）を不可能とする等、情報システム全般に悪影響を与えないような設定を施すこと。

（イ）送信できるメールの容量の上限を設定し、大容量のメールの送受信を不可能とすること。

（ウ）職員等が使用できるメールボックスの上限を設定し、上限を超えた場合には、職員等が自らメールを削除する等の措置を採ること。

（エ）スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止すること。

(8) 文書サーバ

情報システム管理者等は、次に掲げる事項に留意しなければならない。

ア　職員等が使用できる文書サーバの１人当たりの上限を設定すること。

イ　文書サーバ内のフォルダ及びファイルを共用できないような設定を施すこと。

ウ　同一課(室)等であっても、県民の個人データ、人事記録等特定の職員等しか取り扱えないデータについては、担当職員以外の職員等が閲覧及び使用できないような措置を施すこと。

(9) 外部の者が利用できるシステム

情報システム管理者等は、外部の者が利用できる情報システム等については、必要に応じ他の情報システム等と物理的または論理的に分ける等、情報セキュリティ対策について特に強固な対策をとること。

(10) 情報システムの入出力データ

情報システム管理者等は、次に掲げる事項に留意しなければならない。

ア　情報システム等に入力されるデータは、適切なチェック等を行い、それが正確であることを確実にするための対策を施すこと。

イ　エラー又は故意の行為により情報が改ざんされるおそれがある場合は、これを検出する手段を講ずるとともに、改ざんの有無を検出し、必要な場合は、情報の修復を行う手段を講ずること。

ウ　情報システム等から出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確保すること。

(11) 電子署名及び暗号化

ア　外部に送るデータが完全であることを担保することが必要な場合には、別に定める電子署名方法及び暗号化方法を使用して送信しなければならない。

イ　暗号化については、別に定める方法以外の方法を用いてはならない。また、暗号のための鍵は、別に定める方法で管理しなければならない。

(12) 業務目的以外の目的のための利用の禁止

ア　職員等は、業務目的以外の目的での情報システム等へのアクセス、メールの利用及びウェブページの閲覧をしてはならない。ただし、県政の施策推進又は業務の円滑な執行の観点から、ＣＤＯが特に必要と認める場合は、この限りではない。

なお、情報システム管理者等は、職員等が業務目的以外の目的で情報システム等へのアクセス、メールの利用及びウェブページの閲覧をした場合は、当該職員等が所属する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。この場合において、それが改善されない場合には、情報システム管理者等は、当該職員等の情報システム等の利用に係る権利を停止し、又は剥奪することができる。

イ　情報システム管理者等は、情報システム等の利用に係る権利を停止し、又は剥奪した場合は、当該職員等が所属する情報セキュリティ管理者にその旨を通知しなければならない。

(13) 無許可ソフトウェアの導入等の禁止

職員等が業務上の必要から標準実装以外のアプリケーションソフトの端末機へのインストールを行う場合には、関係する情報システム管理者等の許可を得なければならない。

(14) 機器構成の変更

職員等は、次に掲げる事項を行ってはならない。

ア　情報システム管理者等の許可を得ず、端末機の改造（セキュリティ機能に係るソフトウェアの設定変更等を含む。）又は機器の増設若しくは交換を行うこと。

イ　情報システム管理者等の許可を得ず、端末機を他のネットワークに接続すること及び外部からのアクセスを可能とすること。

(15) 複合機のセキュリティ管理

ア　情報システム管理者等及び情報セキュリティ管理者は、複合機を調達する場合、当該複合機が備える機能、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、適切な情報セキュリティ要件を策定しなければならない。

イ　情報システム管理者等及び情報セキュリティ管理者は、複合機が備える機能について適切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インシデントへの対策を講じなければならない。

ウ　情報システム管理者等及び情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ記録媒体の全ての情報を抹消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。

(16) ＩｏＴ機器を含む特定用途機器のセキュリティ管理

情報システム管理者等及び情報セキュリティ管理者は、ＩｏＴ機器を含む特定用途機器（テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は記録媒体を内蔵しているもの）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実施しなければならない。

(17) 無線ＬＡＮのセキュリティ対策及びネットワークの盗聴対策

ア　ネットワーク管理者は無線ＬＡＮの利用を認める場合、別に定めるところにより、解読が困難な暗号化及び認証技術の使用を義務付けるほか、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。

イ　ネットワーク管理者は機密性の高い情報を取り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。

(18) Ｗｅｂ会議サービスの利用時の対策

ア　ネットワーク管理者は、Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。

イ　職員等は、利用手順に従い、Ｗｅｂ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

ウ　Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

(19) 電子商取引

業務目的以外の電子商取引を禁止する。

(20) その他

職員等が使用できる通信プロトコルは、業務上必要最小限のものとする。

２　アクセス制御

(1) 利用者登録

ア　情報システム管理者等は、所掌する情報システム等への利用者の登録、変更、抹消等の登録情報の管理及び異動、退職、出向等による職員等の利用者ＩＤの取扱い等については、各情報システム等で定める方法に従って適切な管理を行うこと。なお、共有ＩＤの利用は、業務上又は運用上の理由で必要な場合に限り許可すること。

イ　情報セキュリティ管理者は、必要な利用者の登録又は変更の申請を、情報システム管理者等に対し行うこと。

(2) 管理者権限

ア　ネットワークの管理者権限（ネットワークを管理するための最高権限のＩＤをいう。以下同じ。）は、１人の者に与え厳重に管理しなければならない。この場合において、ネットワークの管理者権限を代行する者は、ネットワーク管理者が指名し、ＣＩＳＯが認めた者でなければならない。

イ　情報システムの管理者権限（情報システムを管理するための最高権限のＩＤをいう。以下同じ。）は、必要最小限の者に与え、厳重に管理しなければならない。この場合において、情報システムの管理者権限を代行する者は、情報システム管理者が指名し、ＣＩＳＯが認めた者でなければならない。

(3) インターネット以外のネットワークにおけるアクセス制御

情報システム管理者等は、アクセス可能なネットワーク及びネットワークサービス等についてネットワークごと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職員等が当該サービスを利用できるようにしてはならない。

(4) ネットワークの接続制御、経路制御等

ア　情報システム管理者等は、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。

イ　情報システム管理者等は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

ウ　情報システム管理者等は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、定期的な確認により見直さなければならない。

(5) 外部からのアクセス

情報システム管理者等は、次に掲げる事項を遵守しなければならない。

ア　外部からのアクセスの許可は、必要最小限にすること。

イ　外部から県の情報システム等にアクセスする場合は、外部アクセスサーバに対してのみ接続を許可することとし、直接内部の情報システム等に接続しないこと。なお、アクセス方法及び利用方法等は、利用者の真正性の確保ができるものであること。

ウ　外部からアクセスする端末機については、コンピュータウイルスに感染していないことやパッチの適用状況等を確認し、情報セキュリティ対策を行っているものを利用すること。

(6) 総合行政ネットワークとの接続

ネットワーク管理者は、「総合行政ネットワーク接続仕様書（地方公共団体情報システム機構）」に基づき、適切な管理をしなければならない。

(7) 外部ネットワークとの接続制限等

ア　外部ネットワーク（県が管理するネットワーク以外のネットワークをいう。以下同じ。）との接続に際しては、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を詳細に検討し、情報資産に影響が生じないと明確に確認した上で、ＣＩＳＯの許可に基づき接続しなければならない。

その利用は、情報システム管理者等の適切な管理の下で行い、情報セキュリティに留意したネットワーク構成を採らなければならない。この場合において、当該外部ネットワークの瑕疵により県のデータの漏えい、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ときに対処するため、当該外部ネットワークの管理責任者の損害賠償責任を契約上担保しなければならない。

イ　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、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、情報システム管理者等の判断に従い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。

(8) 自動識別

公衆回線を介してリモート接続を受けるネットワーク機器は、アクセスの可否を自動的に識別するものでなければならない。

(9) ログイン手順

情報システム管理者等は、ログイン手順中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つ職員等がログインしたことを確認することができる手順を定めなければならない。

(10) パスワードの管理方法

情報システム管理者等は、次に掲げる事項を遵守しなければならない。

ア　職員等のパスワードに関する情報を厳重に管理すること。職員等のパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させること。

イ　パスワードの変更を行わない職員等にパスワードを変更する旨勧告し、当該職員等が勧告に従わない場合は、速やかに当該職員等のアクセス権を一定期間経過後に停止すること。

ウ　当該職員等からパスワード変更の申告があり次第、当該職員等のアクセス権の停止を解除すること。

エ　職員等のパスワードについて、定期的にその妥当性について調査を行うこと。

オ　パスワードが第三者に解読されることのないよう、必要に応じて暗号化等パスワードを扱う方法を定めること。

(11) 接続時間の制限

情報システム管理者等は、管理者権限による情報システム等への接続については、必要最小限の接続時間に制限しなければならない。

3　システムの開発、導入、保守等

(1) 機器等及び情報システムの調達

ア　ＣＩＳＯは、応用ソフトウェア（ＯＳ以外のソフトウェアをいう。）の開発、変更

及び運用についての手順及び基準並びに機器及び基本ソフトウェア（ＯＳ）の導入、保守及び撤去についての手順及び基準を明らかにしなければならない。

イ　情報システム管理者等は、機器等及び情報システムの調達に当たり公開する調達仕様書について、必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

ウ　情報システム管理者等は、機器及びソフトウェアの調達に当たっては、、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。

(2) 情報システムの変更管理

情報システム管理者等は、システム追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。

(3) 情報システムの開発

情報システム管理者等は、情報システムを新たに開発しようとするときには、システム開発及び保守時の事故及び不正行為の対策のため、次に掲げる事項について定めるとともに、適切にこれらを実施しなければならない。

ア　責任者及び監督者の選任

イ　作業者の選任及び作業範囲

ウ　システムの開発及び保守等の事故又は不正行為に係るリスク分析

エ　開発し、及び保守するシステムと運用システムとの分離

オ　開発及び保守に関するソースコードの提出

カ　開発及び保守の際のセキュリティ上問題となり得るおそれのあるＯＳ、ミドルウェア及びアプリケーションソフトの使用禁止

キ　開発及び保守の際のアクセス制限

ク　開発及び保守の際の既知の種類のウェブアプリケーションの脆弱性を排除するための対策

ケ　機器搬出入の際の情報システム管理者等の許可及び確認

コ　開発及び保守の記録の提出義務

サ　マニュアル等の定められた場所への保管

シ　開発及び保守を行った者の利用者ＩＤ、パスワード等の当該開発及び保守の終了後に不要となった時点での速やかな抹消

(4) システムの導入

情報システム管理者等は、新たにシステムを導入する際には、既に稼動しているシステムに接続する前に十分な試験を行わなければならない。なお、試験に使用したデータ及びその結果を厳重に保管しなければならない。

(5) ソフトウェアの保守及び更新

情報システム管理者等は、独自開発ソフトウェア、汎用ソフトウェア、その他のソフトウェア等を更新し、又は修正プログラムを導入する場合は、不具合及び他のシステムとの相性の確認を行い、計画的に更新し、又は導入しなければならない。この場合において、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、速やかな対応を行うとともに、その他のソフトウェアの更新等については、計画的に実施しなければならない。

(6) システムの受託事業者への設定

情報システム管理者等は、次に掲げる事項を遵守しなければならない。

ア　新たなシステムの開発を外部の事業者に委託する場合は、ソースコードの提出を求め、導入前の検査要求事項等を契約に定めること。

イ　信頼のおける事業者に委託するために、必要な資格等を定めること。

ウ　事業者に対し、作業中に身分証明書の提示を求め、契約で定められた資格を有する者が作業に従事しているかどうかの確認を行うこと。

エ　守秘のための契約を事業者と結ぶこと。

(7) 機器の修理及び廃棄等

情報システム管理者等は、次に掲げる事項を遵守しなければならない。

ア　記憶媒体の含まれる機器について、外部の事業者に修理させる場合は、その内容が消去された状態で行わせること。

イ　故障を外部の事業者に修理させる際、情報を消去することが難しい場合は、修理を委託する事業者との間で、秘密を守ることを契約に定めること。

ウ　機器を廃棄、リース契約終了後返却等をする場合は、機器内部の記憶装置におけるすべての情報を復元不可能な状態にする消去措置を施すこと。

(8) 情報システムについての対策の見直し

情報システム管理者等は、愛媛県情報セキュリティポリシーに基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。

4　不正プログラム対策

情報システム管理者等は、次に掲げる事項を実施しなければならない。

(1) 外部のネットワークから受信したファイルは、ネットワーク接続部でウイルス等不正プログラムのチェック（以下「ウイルスチェック」という。）を行い、システムへの侵入を防止すること。

(2) 外部のネットワークへ送信するファイルは、ネットワーク接続部でウイルスチェックを行い、外部へのウイルス拡散を防止すること。

(3) ウイルス情報について職員等に対する注意喚起を行うこと。

(4) 常時ウイルスに関する情報収集に努めること。

(5) サーバ及び端末機にコンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させること。

(6) ウイルスチェック用のパターンファイル及び検索エンジンは、常に最新のものに保つこと。

(7) 外部からデータ又はソフトウェアを取り入れる場合には、必ずウイルスチェックを行うこと。

(8) 差出人が不明なファイル又は不自然に添付されたファイルは、速やかに削除すること。

(9) ウイルスチェックの実行を途中で停止させないこと。

(10) ネットワーク管理者が提供するウイルス情報を常に確認すること。

(11) 添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行うこと。

(12) 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。

5　不正アクセス対策

情報システム管理者等は、次に掲げる事項を実施しなければならない。

(1) 使用終了又は使用される予定がないポートは閉鎖すること。

(2) 不要なサービスについて、機能を削除又は停止すること。

(3) セキュリティホールの発見に努め、メーカー等からパッチの提供があり次第、速やかにパッチを当てること。

(4) 重要なファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

(5) 攻撃を受けることが明白な場合には、システムの停止を含む必要な措置を講ずるとともに、各機関との連絡を密にして情報の収集に努めること。

なお、攻撃を受け、当該攻撃が犯罪その他の法令違反等に該当する可能性がある場合には、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こと。

(6) 職員等による不正アクセスがあった場合は、当該職員等が所属する課(室)等の情報セキュリティ管理者に通知し、適切な処置を求めること。

(7) 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ること。

(8) 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、教育や自動再生無効化等の人的対策や入口対策を講じること。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ること。

6　セキュリティ情報の収集

情報システム管理者等は、次に掲げる事項を実施しなければならない。

(1) サーバ、端末及び通信回線装置等におけるセキュリティホールに関する情報、不正プログラム等のセキュリティ情報等情報セキュリティに関する情報を収集し、県のすべての情報システム等についてソフトウェア更新等、セキュリティ対策上必要な措置を講ずること。

(2) 情報セキュリティに関する情報を定期的に取りまとめ、関係部局等に通知するとともに、ポリシーの改定につながる情報については、委員会に報告すること。

(3) 第９の４に定める緊急時対応計画に係る緊急に連絡すべき情報を入手した場合は、当該計画に定める連絡先に、直ちに連絡すること。

第９　運用

1　情報システムの監視

情報システム管理者等は、次に掲げる事項を実施しなければならない。

(1) セキュリティに脅威を与える可能性を検知するため、常に情報システム等の監視を行うこと。

(2) 外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、監視を行うこと。

(3) 内部のシステムについて、アクセスコントロール等を行い、異常な運用等の監視を行うこと。

(4) 監視により得られた結果については、消去又は改ざんをされないために必要な措置を施し、定期的に安全な場所に保管するとともに、これらの記録の正確性を確保するため、正確な時間の設定を行うこと。

2　ポリシーの遵守状況の確認

(1) 情報セキュリティ管理者は、ポリシーが遵守されているかどうかについて、及び問題が発生していないかについて常に確認を行い、問題が発生している場合には、速やかに情報システム管理者等に報告しなければならない。この場合において、情報システム管理者等は、発生した問題に適切かつ速やかに対処しなければならない。

(2) 職員等は、ポリシーの違反が発生した場合は、直ちに情報セキュリティ管理者に報告しなければならない。この場合において、情報セキュリティ管理者は、情報システム管理者等に報告するものとし、当該報告を受けた情報システム管理者等は、これ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認める場合は、４に定める緊急時対応計画に従って対処しなければならない。

(3) 情報セキュリティ管理者の指導によっても改善されない場合、情報セキュリティ管理者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、情報セキュリティ管理者は、職員等の権利を停止あるいは剥奪した旨をＣＩＳＯに通知しなければならない。

3　運用管理における留意点

(1) 情報システム管理者等は、実施手順中に、アクセス記録、メール等個人のプライバシーに係る情報を閲覧できる権限を有する職員等を定めなければならない。ただし、法令で定められた個人情報の保護に関する情報の閲覧に関しては、当該法令に定められた手続に従うものとする。

(2) 情報セキュリティ管理者は、職員等が常にポリシー及び実施手順を参照できるよう配慮しなければならない。

4　侵害時の対応

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるための緊急時対応計画は、次のとおりとする。

(1) 連絡先

次に掲げる連絡先のうちから、情報システム等ごとに必要な者について実施手順に明記し、対処するものとする。

ア　ＣＩＳＯ
イ　委員長
ウ　ＣＳＩＲＴ
エ　ネットワーク管理者
オ　情報システム管理者
カ　情報システム担当者
キ　情報セキュリティ管理者
ク　情報セキュリティ担当者
ケ　情報システムに係る外部委託事業者等
コ　警察
サ　関係機関

シ　影響が考えられる個人又は法人

(2) 事案の調査

職員等は、セキュリティに脅威を与える可能性を認めた場合には、次に掲げる事項について、速やかに情報システム管理者等に報告し、これを受け情報システム管理者等は、ＣＳＩＲＴに報告しなければならない。この場合において、ＣＳＩＲＴは、情報システム管理者等と連携し、事案の詳細な調査を行うとともに、ＣＩＳＯ及び委員会に対しその結果を報告しなければならない。

ア　事案の内容

イ　事案が発生した原因又は想定される行為

ウ　確認した被害及び影響範囲

(3) 事案への対処

ア　ＣＳＩＲＴ

ＣＳＩＲＴは、報告を受けた事案に関して情報収集・分析を行い、必要な対処策について、情報システム管理者等に指示を行うとともに、必要に応じて情報システム管理者等と連携して、事案への対処を行う。

イ　ネットワーク管理者

ネットワーク管理者は、次の事案が発生し情報資産の防護のためにネットワークの切断がやむを得ない場合は、ＣＳＩＲＴの指示によりネットワークを切断する措置を講じなければならない。

（ア）異常なアクセスが継続しているとき、又は不正アクセスが判明したとき。

（イ）システムの運用に著しい支障を来たす攻撃が継続しているとき。

（ウ）コンピュータウイルス等不正プログラムがネットワーク経由で広がっているとき。

（エ）情報資産に係る重大な被害が想定されるとき。

ウ　情報システム管理者等

情報システム管理者等は、事案に対処するために次に掲げる事項を実施しなければならない。

（ア）次に掲げる場合に該当するときは、それぞれ次に定める連絡先へ連絡すること。

(a) サイバーテロその他の県民に重大な被害が生じるおそれがあるとき　ＣＩＳＯ及び警察

(b) 不正アクセスその他の犯罪があると思慮されるとき　ＣＩＳＯ及び警察

(c) 踏み台（不正侵入され、第三者への攻撃等のために使用されることをいう。）となって第三者に被害を与えるおそれがあるとき　ＣＩＳＯ及び警察

(d) 情報システムに関する被害　情報システムに係る外部委託事業者等

(e) その他情報資産に関する被害　関係部局等

（イ）次に掲げる場合において、情報資産の防護のために情報システム等の停止がやむを得ないときは、ＣＳＩＲＴの指示により情報システム等を停止すること。ただし、情報資産の被害拡大防止のため直ちに停止する必要がある場合には、情報システムを停止するものとし、事後報告とすることができる。

(a) コンピュータウイルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき。

(b) 異常なアクセスが継続しているとき、又は不正アクセスが判明したとき。

(c) システムの運用に著しい支障を来たす攻撃が継続しているとき。

(d) コンピュータウイルス等不正プログラムがネットワーク経由で広がっているとき。
(e) 災害等により電源を供給することが危険又は困難なとき。
(f) その他の情報資産に係る重大な被害が想定されるとき。
(ウ) 事案に係るシステムのアクセス記録及び現状を保存すること。
(エ) 事案に対処した経過を記録すること。
(オ) 事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討すること。
(カ) 再発防止の暫定措置を講じた後、復旧すること。

エ　職員等

職員等は、事案が発生した場合において、個々の端末機をネットワークから切断する必要があるときは、情報システム管理者等の許可を得なければならない。ただし、コンピュータウイルスに感染した場合等、情報資産の被害の拡大を直ちに停止させる必要がある場合には、端末機を速やかにネットワークから切断するものとし、事後報告とすることができる。

(4) 再発防止の措置

ア　情報システム管理者等は、ＣＳＩＲＴとともに当該事案に係るリスク分析を実施し、ポリシー及び実施手順の改善に係る再発防止計画を策定し、委員会へ報告しなければならない。この場合において、当該報告を受けた委員会は、ポリシー及び実施手順の改善に係る再発防止計画が有効であると認めるときは、これを承認するものとする。

イ　情報システム管理者等は、ＣＳＩＲＴとともに各種情報セキュリティ対策の改善に係る再発防止計画を策定し、委員会へ報告しなければならない。この場合において、当該報告を受けた委員会は、これらの再発防止計画が有効であると認めるときは、これらを承認するものとする。

(5) 緊急時対応計画の見直し

ＣＩＳＯ又は情報セキュリティ委員会は、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、必要に応じて緊急時対応計画の規定を見直さなければならない。

5　業務委託

(1) 委託事業者の選定基準

委託契約主管課(室)は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

(2) 業務委託実施前の対策

情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

ア　委託する業務内容の特定
イ　委託事業者の選定条件を含む仕様の策定
ウ　仕様に基づく委託事業者の選定
エ　情報セキュリティ要件を明記した契約の締結（契約項目）

情報システムの開発・運用等を業務委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。この場合において、委託契約主管課(室)は、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について、委託先の責任者から報告を受け、その内容を管理職及び担当者により重複的に確認し、情報システム管理者等に報告するとともに、その重要性に応じてＣＩＳＯに報告しなければならない。

(a) 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

(b) 個人情報漏えい防止のための技術的安全管理措置に関する取り決め

・複数の宛先にメールを送信する場合は、Ｂｃｃを利用し、メールアドレスの流出を防止すること。

・委託事業者の既設ツール等を用いて不特定多数から情報を収集する場合は、情報へのアクセス権限をもつ者を必要最小限とするほか、収集した情報が公開されることがないよう、適切に設定されていること。

(c) 委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

(d) 提供されるサービスレベルの保証

(e) 委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

(f) 従業員に対する教育の実施

(g) 提供された情報の目的外利用及び委託事業者以外の者への提供の禁止

(h) 業務上知り得た情報の守秘義務

(i) 再委託に関する制限事項の遵守

(j) 委託業務終了時の情報資産の返還、廃棄等

(k) 委託業務の定期報告及び緊急時報告義務

(l) 県による監査、検査 (m) 県による情報セキュリティインシデント発生時の公表

(n) 情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

オ　委託事業者に重要情報を提供する場合は、秘密保持契約の締結

(3) 委託実施期間中の対策

ア　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

（ア）選定基準に従った重要情報の提供

（イ）契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

（ウ）重要度に応じてＣＩＳＯへ措置内容の報告

（エ）委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

イ　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）情報の適正な取扱いのための情報セキュリティ対策

（イ）契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

（ウ）委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(4) 業務委託終了時の対策

ア　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

（イ）委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

イ　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

（イ）提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

(5) 情報システムに関する業務委託

ア　情報システムに関する業務委託における共通的対策

情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに県の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

イ　情報システムの構築を業務委託する場合の対策

情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）情報システムのセキュリティ要件の適切な実装

（イ）情報セキュリティの観点に基づく試験の実施

（ウ）情報システムの開発環境及び開発工程における情報セキュリティ対策

ウ　情報システムの運用・保守を業務委託する場合の対策

（ア）情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

（イ）情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

6　外部サービス（クラウドサービス）の利用民間事業者がインターネット上で提供する外部サービス（クラウドサービス）を利用する場合、利用契約主管課(室)は、利用する外部サービスの選定にあたり、情報システムの機能、役割、重要度等に応じて、別に定めるところにより、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。

7　ソーシャルメディアサービスの利用

インターネット上におけるブログやソーシャルネットワーキングサービス等の、双方向で情報のやりとりが可能なソーシャルメディアサービスを利用する各課(室)長は、安全にソーシャルメディアを利用するため、別に定めるところにより、適切に運用しなければならない。

第10　法令遵守

職員等は、職務の遂行において利用する情報資産について、次の法令等を遵守しなければならない。

(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) 個人情報の保護に関する法律(平成 15 年法律第 57 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) 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)
(6) サイバーセキュリティ基本法（平成 26 年法律第 104 号)
(7) 個人情報の保護に関する法律施行条例（令和４年愛媛県条例第 35 号)

第 11　評価及び見直し

１　監査

(1) 情報システム管理者等は、情報システム等の情報セキュリティについて監査を定期的に行わなければならない。
(2) 情報システム管理者等は、外部委託事業者に情報システム等の運用管理を委託している場合は、当該外部委託事業者の下請け事業者も含めて、ポリシーの遵守について監査を定期的に行わなければならない。
(3) 情報システム管理者等は、監査結果をとりまとめ、委員会に報告しなければならない。この場合において、当該報告を受けた委員会は、当該報告の結果をポリシーの更新時の情報として活用しなければならない。

２　点検

(1) 情報セキュリティ管理者及び情報システム管理者等は、ポリシーに沿った情報セキュリティ対策が実施されているかどうかについて職員等にアンケート等による情報の収集及び自己点検を行い、自己点検結果を委員会に報告するとともに、自己点検結果に基づき改善を図らなければならない。この場合において、当該報告を受けた委員会は、当該報告の結果をポリシーの更新時の情報として活用しなければならない。
(2) 職員等は、自己点検結果に基づき、自己の権限の範囲内で改善を図らなければならない。

３　ポリシーの更新

委員会は、新たに必要な対策が発生した場合又は監査若しくは点検の結果必要と認められる場合は、ポリシーの実効性を評価し、必要な部分の見直し等ポリシーの更新を実施しなければならない。

別図（第３関係）

愛媛県情報セキュリティ対策のための組織及び体制