愛媛県情報セキュリティポリシー

（公開用）

（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５年10月５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

近年の情報技術の進展に伴い、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、情報通信技術（ＩＴ）革命の進展に伴い、行政事務や教育環境の電子化等新しい行政需要への対処が期待されているが､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) 情報

ネットワーク及び情報システムで扱うデータをいう。

(4) 情報資産

ネットワーク及び情報システム（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。

(5) 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) 人事委員会事務局
(4) 議会事務局
(5) 選挙管理委員会事務局
(6) 監査事務局
(7) 教育委員会事務局（教育委員会が所管する県立学校を含む。）
(8) 労働委員会事務局

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（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) 職員等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) 職員等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

ネットワーク及び情報システム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、すべての職員等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外部委託、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

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。

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

（セキュリティ上非公開）

第４　情報資産の分類及び管理

（セキュリティ上非公開）

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　装置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機器のうち、システムのセンターマシン等（以下「センター装置」という。）のセキュリティ対策は、次のとおりとする。

(1) センター装置の取付け等

ア　センター装置を設置する場合は、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　次に掲げるセンター装置は、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　センター装置は、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措置を講ずること。（セキュリティ上一部内容変更）

エ　センター装置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が外部に漏えいすることがないよう配慮すること。（セキュリティ上一部内容変更）

(2) 電源

ア　センター装置の電源は、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。

(3) 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。

(4) 県各機関外に設置する装置

ア　（セキュリティ上非公開）

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、適切に管理すること。（セキュリティ上一部内容変更）

2　管理区域のセキュリティ対策

(1) 管理区域

（セキュリティ上非公開）

(2) 情報システム室の入退室管理

（セキュリティ上非公開）

(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　（セキュリティ上非公開）

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。

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

(1) ～ (10)　（セキュリティ上非公開）

(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

（セキュリティ上非公開）

３　情報セキュリティインシデントの報告

（セキュリティ上非公開）

４　ＩＤの管理

（セキュリティ上非公開）

５　パスワードの管理

（セキュリティ上非公開）

６　ＩＣカード等の管理

（セキュリティ上非公開）

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　（セキュリティ上非公開）

(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処理について、記録を作成するとともに、行った作業を記録し、適切に管理すること。

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

（セキュリティ上非公開）

(6) バックアップ

（セキュリティ上非公開）

(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）～（ウ）（セキュリティ上非公開）

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。

(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　（セキュリティ上非公開）

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、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。（セキュリティ上一部内容変更）

(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

（セキュリティ上非公開）

(13) 無許可ソフトウェアの導入等の禁止

（セキュリティ上非公開）

(14) 機器構成の変更

（セキュリティ上非公開）

(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) 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、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) 電子商取引

業務目的以外の電子商取引を禁止する。

(18) 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、適切な管理を行うこと。（セキュリティ上一部内容変更）

イ　（セキュリティ上非公開）

(2) 管理者権限

ア　ネットワークの管理者権限は、厳重に管理しなければならない。（セキュリティ上一部内容変更）

イ　情報システムの管理者権限は、厳重に管理しなければならない。（セキュリティ上一部内容変更）

(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

（セキュリティ上非公開）

(4) 強制的な経路制御

情報システム管理者等は、不正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、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。（セキュリティ上一部内容変更）

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

（セキュリティ上非公開）

(7) 外部ネットワークとの接続

ア　（セキュリティ上非公開）

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

（セキュリティ上非公開）

(9) ログイン手順

（セキュリティ上非公開）

(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。（セキュリティ上一部内容変更）

イ　（セキュリティ上非公開）

ウ　（セキュリティ上非公開）

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、パスワードを扱う方法を定めること。（セキュリティ上一部内容変更）

(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) 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、情報システム等の調達に当たり公開する調達仕様書について、情報セキュリティを十分に確保しておかなければならない。

ウ　情報システム管理者等は、機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上適切かどうか、あらかじめ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　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

ケ　開発及び保守の記録の提出義務

コ　マニュアル等の定められた場所への保管

サ　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。

4　コンピュータウイルス対策

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) 外部のネットワークから受信したファイルは、ウイルスチェックを行い、システムへの侵入を防止すること。（セキュリティ上一部内容変更）

(2) 外部のネットワークへ送信するファイルは、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。（セキュリティ上一部内容変更）

(3) （セキュリティ上非公開）

(4) （セキュリティ上非公開）

(5) サーバ及び端末機において、ウイルスチェックを行うこと。

(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) （セキュリティ上非公開）

(9) （セキュリティ上非公開）

(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。

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) 使用終了の又は使用される予定のないポートを長時間空けた状態のままにしないこと。

(2) 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。

(3) 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。

(4) 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。

(5) （セキュリティ上非公開）

(6) 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。

(7) 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、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、対策を講じること。（セキュリティ上一部内容変更）

6　情報セキュリティに関する情報の収集

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) 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にパッチを当てる等、セキュリティ対策上必要な措置を講ずること。

(2) （セキュリティ上非公開）

(3) （セキュリティ上非公開）

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) ～ (4) （セキュリティ上非公開）

2　ポリシーの遵守状況の確認

（セキュリティ上非公開）

3　運用管理における留意点

（セキュリティ上非公開）

4　侵害時の対応

（セキュリティ上非公開）

5　外部委託

(1) 外部委託事業者の選定基準

委託契約主管課(室)は、外部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) 契約項目

情報システムの運用等を外部委託する場合には、外部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、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、その内容を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。

ア　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
イ　外部委託事業者の責任者、委託内容、作業者、作業場所の特定
ウ　提供されるサービスレベルの保証
エ　従業員に対する教育の実施
オ　提供された情報の目的外利用及び受託者以外の者への提供の禁止
カ　業務上知り得た情報の守秘義務
キ　再委託に関する制限事項の遵守
ク　委託業務終了時の情報資産の返還、廃棄等
ケ　委託業務の定期報告及び緊急時報告義務

コ　県による監査、検査

サ　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)

6　外部サービスの利用

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) 著作権法（昭和45年法律第48号)
(2) 個人情報の保護に関する法律(平成15年法律第57号)
(3) 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)
(4) 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)
(5) サイバーセキュリティ基本法（平成26年法律第104 号)
(6) 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) （セキュリティ上非公開）

2　点検

（セキュリティ上非公開）

3　ポリシーの更新

（セキュリティ上非公開）