兵庫県情報セキュリティ対策指針

令和８年兵庫県告示第295号の２

第１章　情報セキュリティ対策基本方針

（目的）

第１条　この指針は、兵庫県（以下「県」という。）の情報資産を適切に保持するため、情報システムの信頼性及び安全性の確保に必要な情報セキュリティ対策の基本方針及び具体的な対策を講ずるに当たっての基準を定めるものとする。

（定義）

第２条　この指針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) 情報資産　情報システムの開発、運用、利用等に係る全ての電磁的に記録されたデータをいう。

(2) 情報セキュリティ対策　情報資産の機密性、完全性及び可用性を保持し、適正な利用を確保することをいう。

(3) 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。

(4) 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。

(5) 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。

(6) 情報システム　コンピュータ、通信機器、通信回線及び記録媒体で構成され、業務に関する情報処理を行う仕組みをいう。

(7) ネットワーク　複数のコンピュータを通信回線により、互いに資源を共有することができるように結合させた仕組みをいう。

(8) サーバ　情報システムを構成する機器のうち、特定のサービスを提供するコンピュータをいう。

(9) ＩＤ　情報システムの利用者を識別するための記号をいう。

(10) ＩＤカード　情報システムの利用者を識別するための磁気カード又はＩＣカードをいう。

(11) パスワード　情報システムの利用者であることを確認するために使用される記号をいう。

(12) 不正アクセス　情報システムを利用する権限のない者が不正な手段でこれを利用することをいう。

(13) バックアップ　データのき損、滅失等に備えた複製をいう。

(14) コンピュータウィルス　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。

(15) 外部サービス　一般の事業者等の県以外の組織が情報システムの一部又は全部

の機能を提供するクラウドサービス、ホスティングサービス、ハウジングサービス、ソーシャルメディアサービス等のサービスをいう。

（対象範囲）

第３条　この指針は、県の各機関が開発、運用等を行う全ての情報システムを対象とする。

２　前項の機関の範囲は、知事、議会、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会並びに公営企業及び病院事業の管理者とする。

３　この指針は、前項の機関の全ての職員等（特別職、会計年度任用職員、臨時的任用職員、再任用職員等を含む。）及び前項の機関から情報システムの開発、運用等を委託された外部委託事業者等（以下「利用者」という。）に適用する。

（情報資産の分類）

第４条　情報セキュリティ対策は、情報資産をその内容に応じて分類し、その重要度に応じて行うものとする。

（情報資産への脅威）

第５条　情報セキュリティ対策は、県が保有する情報資産を次の各号に掲げる脅威から的確かつ効率的に保護することを目的とする。

(1) 情報システムへの不正アクセス又は不正操作、利用者による意図しない操作、コンピュータウィルスの頒布、過剰な負荷をかける行為等によるデータ及びプログラムの持出し、盗聴、改ざん又は消去、機器及び媒体の盗難、情報システムの中断又は停止等

(2) 利用者による記録媒体の持出し、規定外の端末接続等によるデータ及びプログラムの漏洩、流出等

(3) 地震、落雷、火災等の災害又は事故、故障等による情報システムの損傷、中断又は停止

（情報セキュリティ対策）

第６条　情報システムにおいては、前条各号に掲げる脅威から情報資産を保護するため、次の各号に掲げる対策を講ずるものとする。

(1) 物理的セキュリティ対策

情報システムを構成する機器の管理、これらの機器その他の設備を設置する施設の入退室管理等情報システムの設置に伴う安全性を確保するために必要な対策を講ずる。

(2) 人的セキュリティ対策

情報システムの利用者の責務を明らかにするとともに情報セキュリティ対策に関する研修及び啓発を行うなど情報システムの適正な利用を確保するために必要な対策を講ずる。

(3) 技術的セキュリティ対策

情報システムへの不正アクセスの防止、コンピュータウィルス対策、情報システムにおけるアクセス制御等の情報システムの開発及び運用における技術的信頼性を確保するために必要な対策を講ずる。

(4) 運用面の対策

情報システムの監視、指針の遵守状況の確認、緊急事態に対応した危機管理等により情報システムの運用面における信頼性を確保し、この指針を効果的に運用するために必要な対策を講ずる。

（情報システム全体の強靭性の向上）

第７条　情報セキュリティの強化のため、行政情報を取り扱うネットワークに接続された情報システムの全体に対し、次の各号に掲げる対策を講ずるものとする。

(1) 住民情報の流出を防ぐため、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）第２条第５項に規定する個人を特定する番号をいう。）を利用する業務システムにおいては、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先を除き、原則として、他の領域との通信を遮断する対策を講ずる。

(2) ＬＧＷＡＮ（高度なセキュリティを確保した上で各地方公共団体の内部システムを相互接続する行政専用のネットワークをいう。）に接続された業務システムにおいては、インターネットに接続された業務システムとの通信経路を遮断し、両システム間で通信する場合には、インターネットメール本文のテキスト化、端末への画面転送等の無害化処理を実施する。

(3) インターネットに接続された業務システムにおいては、県及び県内市町のインターネットとの通信を集約した兵庫県情報セキュリティクラウドを活用した高度な情報セキュリティ対策を講ずる。

(4) 業務の効率性及び利便性の向上のため、主たる職員端末、業務システム、重要な情報資産等をインターネットに接続して利用する場合は、事前に外部による監査を実施し、必要な情報セキュリティ対策を講じた上で、利用中も定期的に外部による監査を実施する。

（最高情報セキュリティ責任者及び最高情報セキュリティ副責任者）

第８条　第３条第１項に定める範囲の情報システムに係る情報資産の管理及び情報セキュリティ対策に関する措置を統一的に実施するため、当該措置に関する指導、助言及び調整を行う責任者として、最高情報セキュリティ責任者を置く。

２　最高情報セキュリティ責任者には、知事の指定する副知事をもって充てる。

３　最高情報セキュリティ責任者を補佐し、又は最高情報セキュリティ責任者が不在の場合には自らの判断に基づき、第１項の措置に関する指導、助言及び調整を行う責任者として、最高情報セキュリティ副責任者を置く。

４　最高情報セキュリティ副責任者には、企画部長をもって充てる。

５　最高情報セキュリティ責任者は、この指針に定められた自らの担務を、最高情報セキュリティ副責任者その他この指針に定める責任者に担わせることができる。

（情報セキュリティ対策統括者）

第９条　この指針に基づき、全庁的な情報セキュリティ対策を統括する者として、情報セキュリティ対策統括者（以下「統括者」という。）を置く。

２　統括者には、企画部デジタル改革課システム企画官をもって充てる。

３　統括者は、情報資産の流出、漏えい又は改ざん、情報システムの障害又は誤動作等の事故等（以下「事故等」という。）に対処するための体制を整備し、役割を明確化するものとする。

４　前項に掲げる体制に関し必要な事項については別に定める。

（情報セキュリティ対策委員会）

第 10 条　県における情報セキュリティ対策を円滑に推進するため、情報セキュリティ対策委員会（以下「委員会」という。）を置く。

２　委員会の委員長には、統括者をもって充てる。

３　委員会は、情報セキュリティ対策の推進方策、指針の見直し等について協議及び調整を行う。

４　その他委員会の運営に関し必要な事項については別に定める。

（運用管理者の責務）

第11条　この指針に基づき、情報システムの適正な運用を図るため、各情報システムに情報セキュリティ対策の運用管理者（以下「運用管理者」という。）を置く。

２　運用管理者には、当該情報システムの業務主管課室長をもって充てる。ただし、当該情報システムにおいて他の業務管理者が定められている場合はこの限りではない。

３　運用管理者は、当該情報システムの適正な運用を図るために必要な情報セキュリティ対策の実施手順（システム運用管理要綱）を策定しなければならない。

４　運用管理者は、この指針及び実施手順の遵守状況を点検チェックシートにより適宜点検し、これらの実効性が保たれるよう必要な措置を講じなければならない。

（利用責任者の責務）

第12条　情報システムの適正な利用を確保するため、各所属に情報システムの利用責任者（以下「利用責任者」という。）を置く。

２　利用責任者には次の各号に掲げる者をもって充てる。

(1) 本庁においては課室長とする。

(2) 地方機関においては地方機関の長、教育機関の長、県立学校の校長とする。ただし、県民局及び県民センターにあっては室等の長及び事務所の長等とする。

３　利用責任者は、各所属においてこの指針及び運用管理者が定める実施手順が遵守されるよう必要な措置を講じなければならない。

（利用者の責務）

第13条　利用者は、この指針及び実施手順を遵守し、情報システムを適正に利用しなければならない。

（評価及び見直し）

第14条　運用管理者は、この指針を踏まえた情報セキュリティ対策の遵守状況について定期的に又は必要に応じて監査及び自己点検を実施し、その結果を統括者に報告しなければならない。

２　統括者は、前項の報告等を踏まえ、脅威の発生の可能性、発生時の損失等を分析し、リスクを検討しなければならない。

３　最高情報セキュリティ責任者は、前項の分析及び検討の結果、必要と認める場合は、指針の見直しを行うものとする。

第２章　情報セキュリティ対策基準

第１節　情報資産の管理

（情報資産の分類方法）

第15条　機密性による情報資産の分類は、次の表のとおりとする。

分類	分類基準	取扱制限
機密性３Ａ	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・支給された端末以外での作業の原則禁止（機密性３の情報資産に限る。） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信時又は情報資産の運搬・提供時における暗号化・パスワード設定又は鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性３Ｂ	行政事務で取り扱う情報資産のうち、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又は性質の上で、取扱いに非常に留意すべき情報資産	
機密性３Ｃ	行政事務で取り扱う情報資産のうち、機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、事務又は業務の規模又は性質の上で、取扱いに留意すべき情報資産	
機密性２	行政事務で取り扱う情報資産のうち、機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	

機密性 1	機密性２又は機密性３の情報資産以外の情報資産	―

２　完全性による情報資産の分類は、次の表のとおりとする。

分類	分類基準	取扱制限
完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性 1	完全性２の情報資産以外の情報資産	―

３　可用性による情報資産の分類は、次の表のとおりとする。

分類	分類基準	取扱制限
可用性 2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性 1	可用性２の情報資産以外の情報資産	―

（情報資産の管理）

第16条　運用管理者は、その所管する情報資産について管理責任を有する。

２　運用管理者は、所管する情報システムに対して、当該情報システムの情報セキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

第２節　物理的セキュリティ対策

（機器の設置）

第17条　運用管理者は、情報システムの機器の設置について、次の各号に掲げる措置を講じなければならない。

(1) 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、容易に取り外せないよう固定する等の措置を講ずること。

(2) 情報システムを設置する事務室への不正な侵入及び盗難を防止するため施錠の徹底等必要な措置を講ずること。
(3) 利用者以外の者が容易に操作できないように、利用者のＩＤ及びパスワードの設定等の措置を講ずること。
(4) 当該機器を適切に停止す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つけること。
(5) 落雷等による過電流に対して機器を保護するために必要な措置を講ずること。
(6) 機器の配線に当たっては、損傷等を受けることがないよう必要な措置を講ずること。

（情報システム室の設置管理）
第18条　運用管理者は、重要な情報システムの設置、運用及び管理を行うための施設（以下「情報システム室」という。）を設置する場合は、次の各号に掲げる対策を講じなければならない。
(1) 情報システム室には、耐震対策、防火対策、防犯対策等の措置を講ずること。
(2) 情報システム室の入退室はあらかじめ許可した者のみとし、ビデオカメラによる監視装置、カード、指紋認証等による入退室管理又は入退室管理簿の記載を行うこと。
(3) 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確認を行うこと。
(4) 情報システム室内の機器の配置は、緊急時に利用者が円滑に避難できるように配慮すること。
２　情報システム室に入室する者は、身分証明書等を携帯し、運用管理者の指定する担当職員の求めに従い提示しなければならない。
３　情報システム室に機器等を設置しようとする者は、当該情報システム室を設置する運用管理者の指示に従わなければならない。
４　運用管理者は、民間事業者等他の機関が管理する施設に情報システムを設置して運用を委託するときは、次の各号に掲げる事項を遵守しなければならない。
(1) 当該施設が第１項に規定する対策が講じられていることを確認すること。
(2) 当該施設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監査すること。
(3) その他この指針で定める対策基準に基づき適正な外部委託の管理を行うこと。

第３節　人的セキュリティ対策

（情報資産の利用）
第19条　利用者は、情報資産の利用に当たって、次の各号に掲げる事項を遵守しなければならない。
(1) データのき損、滅失等に備えるため、保管するデータのバックアップを定期的に作成すること。
(2) 重要な情報資産はパスワードを施すなど適切な管理を行うこと。

(3) 退庁時及び長時間離席する場合は、使用する端末等の電源を切ること。
(4) 運用管理者の許可を得ず、情報システムで処理するデータ及びその複製を定められた場所から移動させないこと。
(5) 運用管理者又は利用責任者の許可を得ず、機密性２以上の情報資産を外部に持ち出さないこと。
(6) 運用管理者又は利用責任者の許可を得ず、機密性２以上の情報資産を第三者に提供しないこと。
(7) その他自己の管理する情報が他に流出しないよう保護すること。

（記録媒体の管理等）
第20条　利用者は、情報資産をハードディスク、ＵＳＢメモリ等の記録媒体で管理する場合は、次の各号に掲げる措置を講じなければならない。
(1) 取り出し可能な記録媒体は、盗難及び損傷の防止のために適切な管理を行うこと。機密性２以上の情報が記録された当該記録媒体を定められた場所から持ち出す場合は、運用管理者又は利用責任者の許可を得ることとし、データの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等の措置を講ずること。
(2) 記録媒体は、防犯、耐火、耐熱、耐水、耐湿等の対策を講じた施錠可能な場所に保管し、管理簿を設けるなど適切な管理を行うこと。
(3) 記録媒体が不要となった場合は、当該媒体に含まれる情報は、記録媒体の初期化など情報を復元できないように消去を行った上で廃棄すること。
２　運用管理者は、記録媒体、機器等の廃棄、返却等を行う場合は、記録媒体、機器内部の記録装置等から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（利用禁止行為）
第21条　利用者は、情報システムの利用について次の各号に掲げる行為を行ってはならない。
(1) 業務に関連しない目的で情報システムを利用すること。
(2) 法令又は公序良俗に反した利用を行うこと。
(3) 他の利用者又は第三者の著作権、人権及びプライバシーを侵害するおそれのある利用を行うこと。
(4) 情報の改ざん、き損及び滅失並びに虚偽の情報提供を行うこと。
(5) 通信を阻害する行為及び情報資産に損害又は不利益を及ぼす利用を行うこと。
２　運用管理者は、前項に該当する利用が行われていると認める場合は、当該利用者に対して情報システムの利用を停止することができる。

（生成ＡＩシステムの利用）
第22条　利用者は、生成ＡＩ（人工的な方法により学習、推論、判断等の知的機能を備え、かつ、質問その他のコンピュータに対する入力情報に応じて当該知的機能の活用により得られた文章、画像、音声等の結果を自動的に出力するよう作成されたプログ

ラム及び当該プログラムと連携して動作するプログラムをいう。以下同じ。）を用いた情報システム（無償で提供される外部サービスを含む。以下「生成ＡＩシステム」という。）の利用について、前条第１項の規定のほか、次の各号に掲げる事項を遵守しなければならない。

(1) 運用管理者が利用者を定める生成ＡＩシステムを除き、利用について運用管理者又は利用責任者（無償で提供される外部サービス等で運用管理者及び利用責任者の定めのない場合は、第12条第２項各号に掲げる者）の許可を得ること。

(2) 安全性が確認されたものとして統括者が許可した生成ＡＩシステムを除き、入力情報に機密性２以上の情報を含めないこと。

(3) 生成ＡＩから出力された結果の正確性を確認すること。

（ＩＤ及びパスワードの管理）

第23条　利用者は、自己の保有するＩＤ及びパスワードに関し、次の各号に掲げる事項を遵守しなければならない。

(1) 他の利用者のＩＤは使わないこと。

(2) パスワードは十分な長さとし、文字列はアルファベット、数字及び記号を混在させるなど容易に推定できないものとすること。

(3) パスワードを更新する際には、古いパスワードの再利用はしないこと。

(4) 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。

(5) パスワードの盗用又は漏えいがあった場合は、直ちに利用責任者に連絡すること。

(6) その他ＩＤ及びパスワードの適正な管理を行うこと。

２　利用者はＩＤカードの利用について、次の各号に掲げる事項を遵守しなければならない。

(1) ＩＤカードを利用者間で共有しないこと。

(2) ＩＤカードを、カードの読み取り装置又は端末に常時挿入しないこと。

(3) ＩＤカードを紛失した場合は、速やかに利用責任者に通報し、指示を仰ぐこと。

（教育・訓練）

第24条　統括者は、全ての職員等がこの指針について理解を深め、遵守を徹底するよう、情報セキュリティ対策に関する研修の実施及び普及啓発を行わなければならない。

２　運用管理者は、情報システムに不測の事態が発生した場合に備えた訓練を計画的に行わなければならない。

（事故等の報告）

第25条　利用者は、事故等を発見した場合は、直ちに利用責任者に報告し、その指示に従い必要な措置を講じなければならない。

２　利用責任者は、事故等の報告を受けた場合は、直ちに当該事故等の内容を運用管理者に報告しなければならない。

３　運用管理者又は利用責任者は、事故等の報告を受けた場合は、直ちに統括者に報告するとともに、必要に応じて関係機関に報告しなければならない。

（外部委託に関する管理）

第26条　運用管理者は、情報システムの開発、運用等を外部委託事業者に委託する場合は、この指針を踏まえ当該外部委託事業者が遵守すべき事項を明記した契約を締結しなければならない。

２　運用管理者は、個人情報取扱事務その他の個人情報を取り扱う事務を外部委託事業者に委託しようとするときは、当該外部委託事業者との契約書に、個人情報取扱特記事項（「個人情報を取り扱う事務の委託に伴う措置について（平成９年11月21日付け文第294号知事公室長通知）」）を規定しなければならない。

３　運用管理者は、外部委託事業者との契約書には、この指針及び実施手順が遵守されなかった場合の損害賠償等の規定を定めなければならない。

４　運用管理者は、外部委託事業者の選定時において、この指針に定める情報資産の安全管理措置と同等の措置が講じられているかを確認しなければならない。

５　外部委託事業者は、情報システムの開発、運用等の外部委託において再委託（三次委託以降を含む。以下「再委託等」という。）が行われる場合は、再委託先（三次委託以降の委託先を含む。以下「再委託事業者等」という。）の名称、業務範囲、再委託等を行う必要性等、県が求める項目を書面（当該書面に記載すべき事項を記録した電磁的記録を含む。以下同じ。）で運用管理者に提出し、再委託等の許可を求めなければならない。

６　運用管理者は、外部委託事業者から前項に規定する再委託等の許可を求める書面が提出された場合は、その内容を確認し、再委託等に問題がないと認める場合に限り承認できるものとする。

７　外部委託事業者は、前２項の手続きにより再委託等が承認された場合は、再委託事業者等の行為について、県に対し全ての責任を負うものとする。

８　外部委託事業者は、この指針で定める運用管理者の遵守事項（再委託事業者等への対応を含む。）について、その実現のために協力しなければならない。

９　運用管理者は、外部委託事業者からこの指針の遵守状況（再委託事業者等の遵守状況を含む。）について定期的な報告を受けるなど、適切な監督を実施し、支障を認めた場合は必要な措置を講じなければならない。

10　運用管理者は、情報システムに誤ったプログラム処理が組み込まれることを防止するため、外部委託事業者において、不具合を考慮したテスト計画の策定及び確実な検証が実施されるよう、必要かつ適切な監督を行わなければならない。

11　運用管理者は、外部委託事業者及び再委託事業者等とのデータの受け渡しに係る内容、日付等を記録しなければならない。

12　運用管理者は、外部委託事業者及び再委託事業者等の責任者及び業務に携わる社員の名簿を作成するとともに、その作業場所を特定しなければならない。

13　運用管理者は、身分証明書の提示を外部委託事業者及び再委託事業者等に求めるなどにより、契約で定められた資格を有するものが作業に従事しているか確認を行わなければならない。

14　運用管理者は、外部委託事業者及び再委託事業者等の従業員に対する教育が実施されているかを確認しなければならない。

15　運用管理者は、業務委託の終了に際して、次の各号に掲げる対策を講じなければならない。

(1)　業務委託の実施期間を通じて情報セキュリティ対策が適切に実施されたことを確認すること。

(2)　外部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を確認すること。

第４節　技術的セキュリティ対策

（バックアップの作成）

第27条　運用管理者は、情報システムのデータベース、ファイルサーバ等に記録された情報について、必要に応じて定期的にバックアップを作成しなければならない。

２　運用管理者は、重要な情報を取り扱うサーバについては、適切な方法でサーバのバックアップを作成しなければならない。

３　運用管理者は、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は、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作成しなければならない。

（アクセス記録の取得等）

第28条　運用管理者は、各種アクセス記録及び情報セキュリティ対策に必要な記録を全て取得し、１年以上の期間を定めて、保存しなければならない。

２　運用管理者は、定期的にアクセス記録等を分析、監視しなければならない。

３　運用管理者は、アクセス記録等が窃取、改ざん、消去されないように必要な措置を講じなければならない。

（情報システムの入出力データ）

第29条　運用管理者は、当該情報システムに入力されるデータの正確性を確保するための対策を講じなければならない。

２　運用管理者は、利用者又は利用者以外の者の故意又は過失による誤ったデータの入力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じなければならない。改ざんを検出した場合は、情報の修復を行う手段を講じなければならない。

３　運用管理者は、情報システムから出力されるデータが、正しく情報処理され、出力されることを確保しなければならない。

４　運用管理者は、ウェブアプリケーション及びウェブコンテンツについて、次の各号に掲げる対策を講じなければならない。

(1)　ウェブアプリケーション及びウェブコンテンツを利用する者の情報セキュリティ水準の低下を招かないよう、その提供方式等を検証し、必要に応じて見直すこと。

(2)　運用中のウェブアプリケーション及びウェブコンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講ずること。

(3) ウェブアプリケーション又はウェブコンテンツにおいて、故意又は過失による情報の改ざん又は漏えいのおそれがある場合に、これを検出する機能を組み込むよう情報システムを設計する等情報の改ざん又は漏えいの防止に必要な措置を講ずること。

（暗号化及び電子署名）

第30条　運用管理者は、機密情報及び重大な情報については、機密性を保護するために暗号化をするとともに、必要に応じて改ざんを防止するために電子署名を付さなければならない。

２　電子署名に係る運用管理については別に定める。

（機器構成の変更）

第31条　運用管理者は、情報システムの機器に業務上必要でないプロトコル（通信手順）を設定してはならない。

２　利用者は、運用管理者の許可なく、端末の改造及び機器の増設又は交換を行ってはならない。

３　利用者は、運用管理者の許可なく、その使用する端末にＩＤの追加、共有データの設定、ソフトウェアの追加等の設定変更を行ってはならない。

（利用者の管理）

第32条　運用管理者は、情報システムの利用者の登録、変更、抹消等登録情報の管理、異動又は退職をした職員等のＩＤ及びパスワードの管理等により、利用者を適正に管理しなければならない。

（情報システムにおけるアクセス制御）

第33条　運用管理者は、情報システムにおけるアクセス制御について次の各号に掲げる事項を遵守しなければならない。

(1) アクセス権限の許可は必要最小限にすること。

(2) 不正アクセスを防止するため、ユーザ認証、論理的なネットワークの分割、ファイアウォール（組織内の情報通信機器及び端末に外部からの侵入を防ぐ目的で設置するセキュリティシステムをいう。以下同じ。）の設置等の適切なネットワーク経路制御を講ずること。

(3) アクセス方法等は利用者の真正性が確保できるものにすること。

(4) 接続した情報通信機器について情報セキュリティに問題が認められ、情報システムの情報資産に脅威が生じることが想定される場合には、速やかに当該情報通信機器を内部ネットワークとの接続から物理的に遮断すること。

(5) 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するとともに、その情報セキュリティ対策を定期的に確認し、必要に応じて見直すこと。

（外部ネットワークとの接続）

第34条　運用管理者は、県の情報システムと県以外の機関が管理する情報システム（以下「外部ネットワーク」という。）との接続については、次の各号に掲げる事項を遵守しなければならない。

(1) 不正アクセスを防止するためのファイアウォールの設置、利用者の認証、論理的なネットワークの分割等適切なネットワーク経路制御を講ずること。

(2) 外部から情報システムにアクセスする場合は、ユーザ認証、ファイアウォールの設置等のネットワーク上の制御を講ずること。

(3) 外部ネットワークとの接続により情報システムの運用及び情報資産の保持に支障が生じるおそれがある場合は、直ちに当該情報システムと外部ネットワークとの接続を物理的に遮断すること。

(4) ネットワークに使用する回線について、伝送途上に情報の破壊、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情報セキュリティ対策を講ずること。

(5) 通信回線装置が動作するために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ずること。

（情報システムの開発）

第35条　運用管理者は、情報システムの開発について次の各号に掲げる事項を実施しなければならない。

(1) 情報システムの開発、保守等に関する事故及び不正行為に係るリスク（危険性）の評価を行うこと。

(2) プログラム、設定等のソースコードを整備すること。

(3) セキュリティの確保に支障が生じるおそれのあるソフトウェアは使用しないこと。

(4) 情報システムの開発及び保守に係る記録を作成するとともに、運用、管理等に必要な説明書等の書類は定められた場所へ保管すること。

(5) 不要になった利用者ＩＤ、パスワード等は速やかに抹消すること。

（情報システムの調達）

第36条　統括者は、機器等の選定基準を整備し、必要に応じて、選定基準において機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。

２　運用管理者は、情報システムの開発、運用等の調達に当たっては、情報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情報セキュリティ機能その他必要とする技術的な情報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。

３　運用管理者は、機器及びソフトウェアを調達する場合は、当該製品の安全性及び信頼性を確認しなければならない。

（ソフトウェアの保守及び更新）

第37条　運用管理者は、独自開発ソフトウェア、オペレーティングシステム等を更新し、

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適合性の確認を行い、計画的に更新し、又は導入しなければならない。

2　運用管理者は、情報セキュリティに重大な影響を及ぼす不具合に関して常に情報を収集し、発見した場合は、修正プログラムの導入等速やかな対応を行わなければならない。

3　運用管理者は、ウェブアプリケーションの開発において、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を講じなければならない。

（コンピュータウィルス対策）

第38条　運用管理者は、コンピュータウィルスによる情報システムの安全性を確保するため、次の各号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データを取り入れる際には、ファイアウォール、メールサーバ等においてウィルスチェック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データを送信する際にも、前号と同様のウィルスチェックを行い、外部へのコンピュータウィルスの拡散を防止すること。

(3) コンピュータウィルス情報について利用者に対する注意喚起を行うこと。

(4) 端末においてウィルス対策用のソフトウェアを導入すること。

(5) ウィルスチェック用のパターンファイルを常に最新のものに保つこと。

(6) コンピュータウィルスに対する修正プログラムの入手に努め、サーバ及び端末に速やかに適用すること。

(7) コンピュータウィルスの感染のおそれの少ないソフトウェアの選定を行うこと。

2　利用責任者は、利用者がコンピュータウィルスを発見した場合又はコンピュータウィルスにより障害が生じたと認められる場合は、直ちに運用管理者に連絡し、その指示に従わなければならない。

3　利用者は、コンピュータウィルスによる被害を防止するため、次の各号に掲げる事項を遵守しなければならない。

(1) 差出人が不明な電子メール又は不審なファイルが添付された電子メールを受信した場合は開封せず、直ちに削除すること。

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

(3) 外部から入手したデータは、必ずウィルスチェックを行うこと。

(4) 万一のコンピュータウィルス被害に備えるため、データのバックアップを作成すること。

(5) 運用管理者が提供するウィルスチェック用のパターンファイルを常に最新のものに更新すること。

(6) 運用管理者が提供するコンピュータウィルス情報を常に確認すること。

（不正アクセス対策）

第39条　運用管理者は、不正アクセスを防止するため、次の各号に掲げる対策を講じなければならない。

(1) 使用が終了した又は使用される予定のないポート（ネットワーク上のサーバがサービスを区別するために使っている番号をいう。）を長時間空けた状態のままにし

ないこと。
(2) 情報通信機器及び端末の不要なＩＤは速やかに削除すること。
(3) 不要なアクセス権限が付与されていないか定期的に確認すること。
(4) 管理者権限等の特権を付与されたＩＤの利用者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理すること。
(5) 管理者権限等の特権を付与されたＩＤ及びパスワード、ＩＤカードその他の認証に用いられる情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び当該情報を使用した内部からの不正操作又は誤操作を防止するための措置を講ずること。
(6) ソフトウェアの不備に伴うセキュリティホールに対しては、速やかに修正プログラムを適用すること。
(7) 不正アクセスによるウェブページの改ざんを防止するため、ウェブページの改ざんを検出し、運用管理者へ通報する設定を講ずること。
(8) 重要な情報システムの設定に係る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。
(9) 不正アクセスを受けるおそれが認められる場合は、情報システムの停止を含む必要な措置を講ずること。

２　運用管理者は、不正アクセスを受けた場合は、直ちに統括者及び関係機関に連絡を行い、情報システムの復旧等必要な措置を講じなければならない。

３　利用責任者は、不正アクセスを受けた場合は、直ちに運用管理者に連絡し、その指示に従わなければならない。

（セキュリティ情報の収集）

第40条　統括者は、情報セキュリティに関する情報を積極的に収集し、運用管理者、利用責任者等に速やかに周知し、必要な措置を講じなければならない。

２　統括者は、前項の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、この指針の改定につながる情報については最高情報セキュリティ責任者に報告しなければならない。

（無線ＬＡＮの対策）

第41条　運用管理者は、無線ＬＡＮの利用に当たり、利用者に対し、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

２　運用管理者は、無線ＬＡＮに対する情報の盗聴等を防ぐため、ハードウェア及びソフトウェアの迅速な更新、定期的な監査等を実施しなければならない。

（在宅勤務等の対策）

第42条　運用管理者は、在宅勤務、職場外勤務等により、外部から県内部の業務システムにアクセスするためのシステム（以下「在宅勤務等システム」という。）を構築し、又は利用する場合は、通信途上の盗聴を防ぐために暗号化、利用経路の閉域化等の対策を講じなければならない。

２　運用管理者は、在宅勤務等システムの利用を認める場合は、利用者の本人確認を行う機能を確保しなければならない。
３　運用管理者は、外部からアクセスするために利用するモバイル端末を貸与する場合は、情報セキュリティの確保のために必要な措置を講じなければならない。
４　利用者は、在宅勤務等システムを利用する場合は、運用管理者の許可を得なければならない。
５　その他在宅勤務等システムに関し必要な事項については別に定める。

（外部サービス利用の対策）
第43条　運用管理者は、外部サービスを利用しようとする場合は、利用目的及び業務範囲を明確にするとともに、取り扱う情報の内容に応じ、情報の保存場所、裁判管轄、準拠法等のリスクの対策を検討した上で、外部サービスの提供者を選定しなければならない。
２　運用管理者は、外部サービスにおいて機密性２以上の情報を取り扱う場合は、あらかじめ統括者の許可を得なければならない。この場合において、外部サービスの提供者が不特定多数の利用者に対して提供する画一的な約款、規約等への同意のみで利用が可能となる外部サービスでは、原則として機密性２以上の情報を取り扱ってはならない。
３　運用管理者は、利用する外部サービスの情報セキュリティ対策について、外部サービスの提供者との責任の分担を定め、その実施状況を定期的に確認しなければならない。
４　統括者は、県の各機関における外部サービスの利用状況を把握し、必要な措置を講じなければならない。
５　その他外部サービスの利用に関し必要な事項については別に定める。

（生成ＡＩシステムの対策）
第44条　運用管理者は、生成ＡＩシステムの導入及び運用をするに当たり、入力情報が運用管理者の許可なく生成ＡＩの学習に用いられない環境の整備その他情報セキュリティの確保のために必要な措置を講じなければならない。

第５節　運用面の対策

（情報システムの監視）
第45条　運用管理者は、情報システムの円滑な運用を確保するため、情報システムを定期的に監視するとともに、情報セキュリティの機能を適切に運用し、障害が起きた際は速やかに対応しなければならない。
２　運用管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適宜検討し、必要な措置を講じなければならない。
３　運用管理者は、重大な事故等の発生時に適切な対処が行えるよう、情報システムを運用しなければならない。
４　運用管理者は、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、24時間監視を行わなければならない。
5　運用管理者は、情報システム内部において、適正なアクセス制御を行い、運用状況について監視を行わなければならない。
6　運用管理者は、監視した結果を正確に記録するとともに、消去又は改ざんをされないよう必要な措置を施し、安全な場所に保管しなければならない。

（指針の遵守状況の確認）
第46条　利用者は、この指針に違反した場合及び違反の発生を確認した場合は、直ちに利用責任者に報告を行わなければならない。
2　利用責任者は、この指針の遵守状況及び情報資産の管理状況について常に確認を行い、支障を認めた場合には速やかに運用管理者に報告しなければならない。
3　運用管理者は、情報システムにおけるこの指針の遵守状況及び情報資産の管理状況について定期的に確認を行い、支障を認めた場合には、迅速かつ適切に対処しなければならない。

（監査結果への対応）
第47条　統括者は、第14条第１項の規定による監査の結果を踏まえ、指摘事項があった情報システムの運用管理者に対し、当該指摘事項に係る改善計画の策定等の対処を指示しなければならない。措置が完了していない改善計画については、定期的に進捗状況の報告を指示しなければならない。
2　統括者は、指摘事項があった情報システム以外の情報システムの運用管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（緊急時対応計画等）
第48条　運用管理者は、情報資産への侵害が発生した場合に備えて、あらかじめ関係機関との連絡体制、復旧対策等の緊急時対応計画を策定しなければならない。
2　利用責任者は、情報資産への侵害発生又は侵害発生の危険性を発見した場合は、事案の内容、原因、被害の状況等を速やかに運用管理者に報告しなければならない。
3　運用管理者は、情報資産への侵害に起因して、住民に重大な被害が生じるおそれがある場合又は行政の運営に重大な支障が生じる場合は、統括者に直ちに報告するとともに、関係機関に速やかに連絡しなければならない。
4　運用管理者は、情報システムに障害が発生し、情報資産の保持のために情報システムの停止がやむを得ないと認められる場合は、ネットワークを切断することができる。
5　運用管理者は、各種セキュリティに関する事案の詳細な調査を行うとともに、再発防止計画を策定しなければならない。

（法令遵守）
第49条　利用者は、情報システムの運用については、次の各号に掲げる法令を遵守し、これに従わなければならない。
(1) 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）

(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) その他情報セキュリティ対策に関する法令

（補則）
第50条　教育委員会の県立学校における情報セキュリティ対策基準については、この章の規定によるほか、教育委員会が別に定めるところによる。

附　則
この告示は、令和８年４月１日から施行する。