国東市情報セキュリティに関する規程

（目的）

第１条　この訓令は、情報セキュリティを確保するための基本方針について必要な事項を定め、本市における情報資産の機密性、完全性及び可用性を維持することを目的とする。

（定義）

第２条　この訓令において、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) 情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

(2) 情報資産　ネットワーク及び情報システムで取り扱う構成機器並びにネットワーク及び情報システムで取り扱う全ての情報（紙等の有体物に出力された情報も含む。）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、ネットワーク及び電磁的記録媒体で構成され、情報処理を行なう仕組みをいう。

(7) ネットワーク　コンピュータを接続してデータを通信するための情報通信網及び当該情報通信網を構成する設備をいう。

(8) 情報セキュリティポリシー　この訓令及びこの訓令に基づく規程等並びに第８条に規定する情報セキュリティ対策基準をいう。

(9) マイナンバー利用事務系（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）又は戸籍事務等に関わる情報システム及びデータをいう。

(10) LGWAN 接続系　総合行政ネットワーク（以下、「LGWAN」という。）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（マイナンバー利用事務系を除く。）。

(11) インターネット接続系　インターネットメール、ホームページ管理システム等に関わるインターネット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。

(12) 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。

(13) 無害化通信　インターネットメール本文のテキスト化や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ない等、安全が確保された通信をいう。

（職員の責務）

第３条　情報資産を取り扱う職員（非常勤職員及び臨時的任用職員を含む。以下「職員」という。）は、情報セキュリティの重要性を認識するとともに、情報資産の利用にあたっては、法令及び情報セキュリティポリシー並びに第９条に規定する情報セキュリティ実施手順（次項において「法令等」という。）を遵守しなければならない。

２　職員は情報システムの整備その他の情報資産に関する業務を外部に委託するときは、当該業務の受託者に法令等を遵守させなければならない。

（適用範囲）

第４条　情報資産の範囲及び分類については別に定めるものとし、職員は、情報資産の重要度に応じた情報セキュリティの確保のための対策に努めるものとする。

（情報セキュリティ対策）

第５条　職員は、次に掲げる情報資産に対する脅威に対処するため、情報セキュリティ対策を実施するものとする。

(1) 不正アクセス、ウイルス攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん及び消去等
(2) 情報資産の無断持出し、無許可ソフトウェアの使用、故障、操作・設定ミス等による情報資産の漏えい、破壊及び消去等
(3) 地震、落雷、火災等の災害による情報システムの停止及びこれに伴う業務の停止等

2　前項の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じるものとする。
(1) 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こと。
(2) 情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づく情報セキュリティ対策を行なうこと。
(3) 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、次の三段階の対策を講じること。
ア マイナンバー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。
イ 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。
ウ 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、県と市のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
(4) 情報システムを設置し、又は管理する場所への不正な立入り、情報資産の損傷等を防止するための物理的な措置を講じること。
(5) 情報セキュリティに関し、職員の遵守すべき事項の策定並びに職員に対する必要な教育及び啓発を行う等の人的な対策を講じること。
(6) 情報資産へのアクセスの制御、ネットワークの監視その他の情報資産の保護に関する技術的な措置を講じること。
(7) 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じること。
(8) 情報資産に対するセキュリティ侵害が発生した場合の対策を講じること。
(9) 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こと。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こと。
　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こと。
(10) 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図るものとする。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）
第６条　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて、情報セキュリティ監査又は自己点検を実施するものとする。

（情報セキュリティポリシーの見直し）
第７条　情報セキュリティ監査又は自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報通信技術の向上、情報資産に対する新たな脅威等に対処するため新たに対策が必要となった場合には、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）
第８条　前３条に規定する情報セキュリティ対策等を実施するため、情報セキュリティに係る具体的な遵守事項等（以下「情報セキュリティ対策基準」という。）を定めるものとする。
２　情報セキュリティ対策基準は、非公開とする。
（情報セキュリティ実施手順の策定）
第９条　情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順（以下「情報セキュリティ実施手順」という。）を定めるものとする。
２　情報セキュリティ実施手順は、非公開とする。
（情報セキュリティ組織）
第１０条　情報セキュリティ対策を総合的に管理し、その効率的かつ効果的な推進を図るため、情報セキュリティに関する組織を置くものとする。
２　情報セキュリティに関する組織及び機能については、全庁的な体制となるよう市長が定めるものとする。
（委任）
第１１条　この訓令に定めるもののほか、情報セキュリティに関し必要な事項は、市長が別に定める。

附　則
（施行期日）
１　この訓令は、公示の日から施行し、平成２２年４月１日から適用する。
（国東市情報セキュリティポリシー実施要領の廃止）
２　国東市情報セキュリティポリシー実施要領（平成１８年国東市訓令第３７号）は、廃止する。

附　則（平成２７年１１月２６日訓令第１４号）
この訓令は、公示の日から施行する。

附　則（平成３１年３月２５日訓令第３号）
この訓令は、公示の日から施行する。

附　則（令和３年３月４日訓令第２号）
この訓令は、公示の日から施行する。