○守山市情報セキュリティポリシー（情報セキュリティ基本方針）

第２章　情報セキュリティ基本方針

（情報セキュリティ対策）

第６条　第３条の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

(1) 組織体制　本市の情報資産について、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。

(2) 情報資産の分類と管理　本市の保有する情報資産を機密性、完全性および可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システム全体の強靭性の向上　情報セキュリティの強化を目的とし、業務の効率性および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。

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、端末からの情報の持出し不可設定、端末への多要素認証（情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証をいう。）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ことを基本とし、必要に応じて両システム間で通信する場合には、無害化通信（インターネット本文のテキスト化、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。以下同じ。）を実施する。

ウ　インターネット接続系においては、自治体情報セキュリティクラウドの導入等による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。

(4) 物理的セキュリティ対策　サーバ、サーバ室、通信回線および職員のパソコン等について、管理方法を定める等のセキュリティ対策を講じる。

(5) 人的セキュリティ対策　情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、十分な教育および啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ対策　コンピュータ等の管理、アクセス制御、不正プログラム対策および不正アクセス対策等の技術的対策を講じる。

(7) 運用面におけるセキュリティ対策　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、このポリシーの運用面の対策を講じるものとするとともに、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 業務委託におけるセキュリティ対策　業務委託（外部サービス（クラウド利用）の業務委託を含む。）を行う場合には、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き措置を講じる。

(9) サービス利用におけるセキュリティ対策　クラウドサービス等を利用する場合には、本市の定める例に従い規定を整備し対策を講じるとともに、ソーシャルメディアサービス(以下「SMS」という。)を利用する場合には、SMSの運用手順を定め、SMSで発信できる情報を規定し、利用するSMSごとの責任者を定める。

（情報セキュリティ監査および自己点検の実施）

第７条　このポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査および自己点検を実施する。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ監査および自己点検の結果、このポリシーの見直しが必要となった場合および情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報および利用する情報システムに係る脅威の発生の可能性および発生時の損失等を分析し、リスクを検討したうえで、このポリシーを見直す。

（情報セキュリティ実施手順の策定）

第９条　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を定めた情報セキュリティ実施手順を策定するものとする。