以下に示す①外部サービス共通の対策を講じてください。またインターネット環境からサービスを使用する場合は②インターネットパソコン方式の対策も講じてください。

①外部サービス共通

No.	区分	要件概要
1	技術的セキュリティ	外部サービスの停止により市民サービスに多大な影響を与える場合は、外部サービスを安定して利用するために必要な冗長化対策を講じること。
2	技術的セキュリティ	利用する時刻の同期が確実に行われるための対策を講じること。
3	技術的セキュリティ	外部サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的脆弱性に関する情報（OS、その他ミドルウェア等を含めたソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。
4	技術的セキュリティ	アクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。 例）認証方法…ID/PWの設定、生体認証及び多要素認証【推奨】、特定の拠点…IPアドレスの制限、クライアント証明書【推奨】
5	技術的セキュリティ	パスワードを認証要素とする場合は、パスワードの桁数、文字種等、複雑性をシステム側で制御できること。
6	技術的セキュリティ	情報資産へのアクセス履歴、機器への操作履歴、サービスの利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）などを取得し、業務完了後1年間保存すること。履歴を改ざんされないような対策を講じること。
7	技術的セキュリティ	本市の監査及びデジタルフォレンジックに必要となる外部サービス事業者の環境内で生成されるログ等の情報（デジタル証拠）をインシデントが起こった際などに本市の求めに応じて速やかに提供すること。
8	技術的セキュリティ	不正プログラムへの対策を確実に実施すること。（複数の外部サービスを組み合わせて構成する場合において、他の外部サービスが不正プログラムへの対策を実施している場合を除く。ただし、その場合は他の外部サービスが実施する対策に協力すること。）
9	技術的セキュリティ	外部ネットワーク及び内部ネットワークからの不正アクセスを防止する措置を講じること。 例）ファイアウォール又はリバースプロキシの導入
10	技術的セキュリティ	本市の指定するバックアップの頻度、バックアップデータの保存期間、バックアップデータからのリカバリー方法を実施すること。 バックアップの頻度や保存期間について本市の指定する範囲と異なる変更を行う場合はあらかじめ本市の承諾を得ること。
11	技術的セキュリティ	庁内環境から外部に持ち出したデータについて、インターネット環境にある端末等へのダウンロードを禁止すること。 ただし、やむを得ずダウンロードする際は②の端末要件を満たすこと。なお、指定管理者や委託事業者がデータをダウンロードする必要がある場合は、②の端末要件を満たした上で、持ち出すデータの内容を限定し、事前に情報システム管理者の承認を得ること。
12	技術的セキュリティ	特定個人番号を含むデータについて本市と外部サービス環境を接続する際、LGWAN回線またはガバメントクラウド専用線を使用すること。
13	技術的セキュリティ	特定個人番号を含むデータについては、インターネット環境にある端末等へのダウンロードを制限すること。

②インターネットパソコン方式
（インターネット環境にあるパソコンについて以下のセキュリティ対策を講じること。ただし、インターネット仮想パソコンを使用する場合を除く。）

No.	区分	要件概要
1	技術的セキュリティ	外部サービスや内部システムに接続する専用端末（以下、専用端末とする）として、電子メール機能など外部に情報を送付する機能を原則禁止する。 外部記録媒体を使用したデータ持ち出しは厳格に制限する。
2	技術的セキュリティ	許可された専用端末のみ外部サービスに接続できる。
3	技術的セキュリティ	専用端末にログインできる職員を管理する。
4	技術的セキュリティ	ログイン時に使用するパスワードは初期設定のまま使用せず、また安易に推測可能なものを使用しない。
5	技術的セキュリティ	専用端末は有線ケーブルを用いて接続を行い、事務室外への持ち出しを禁止する。
6	技術的セキュリティ	不要なソフトウェアのインストールを禁止する。
7	技術的セキュリティ	専用端末に資産管理ソフトを導入して、操作ログの取得及び保存をする。
8	技術的セキュリティ	専用端末のOS等のアップデートやネットワーク機器のソフトウェア等に脆弱性を残さないように、更新ファイルやパッチ等を適用する。
9	技術的セキュリティ	専用端末の不正プログラム対策として、ウイルス対策ソフトの更新や定期スキャン等を行う。
10	技術的セキュリティ	専用端末に業務と無関係もしくは不要なデータのダウンロードを禁止する。（人的セキュリティ対策を含む）
11	技術的セキュリティ	専用端末に無操作時の画面ロック及びスクリーンセーバー機能を設定する。
12	技術的セキュリティ	専用端末を一定時間操作しない場合、自動的にログオフする。（人的セキュリティ対策を含む）
13	技術的セキュリティ	ハードディスクの暗号化機能を有する端末を許可端末とする。
14	技術的セキュリティ	（複数台でネットワークを組む際は）ファイアウォールを設置するなど外部からのアクセスを制限するほか、ネットワークの通信ログを取得及び保存する。
15	技術的セキュリティ	専用端末内に格納するデータをは必要最小限とし不必要なデータは定期的に消去する。（人的セキュリティ対策を含む） データの格納はできる限り庁内LAN環境において行うなどインターネット環境で保存しないこと。
16	技術的セキュリティ	暗号化通信（SSL通信）を使用した接続とする。
17	技術的セキュリティ	インターネット端末内にバックアップデータを残さないこと。外部サービス等でバックアップを取得、保存すること。
18	技術的セキュリティ	専用端末からやむを得ずデータを持ち出しを行う場合には、事前に承認を得てその記録を残すこと。（人的セキュリティ対策を含む）
19	技術的セキュリティ	専用端末及び外部記録媒体を廃棄する時は物理的に破壊するなど内部データを再度読み込みができない状態で廃棄する。
20	技術的セキュリティ	データを記録した外部記録媒体は使用後に初期化する。（人的セキュリティ対策を含む）
21	技術的セキュリティ	外部記録媒体（USBメモリ等）の所在や使用状況の管理、使用の制限を実施する。（人的セキュリティ対策を含む）
22	技術的セキュリティ	暗号化機能及びウイルス対策機能を有する外部記録媒体を使用する。