別紙

外部委託における情報セキュリティ遵守事項

1. 基本事項

草加市は、保有する情報資産の機密性、完全性及び可用性を維持するため、市が実施する情報セキュリティ対策の基本的事項を「情報セキュリティ基本方針」として定めている。また、当該セキュリティ対策の有効性及び効率性の確保を目的として、遵守すべき行為、判断等に関する基本的事項を「情報セキュリティ対策基準」として定めている。

市の情報資産を取扱う業務の受注者は、当該基本方針及び対策基準の適用範囲に含まれることから、次の事項を遵守し、市の情報資産の機密性、完全性及び可用性を維持するよう努めなければならない。

2. 情報の分類

受注者は、原則として次の分類を行った上で、情報を保護すること。

市保有情報	市から貸与された情報のこと。
重要情報	市から貸与された情報の内、個人情報、特定個人情報及び非公開情報を含む情報のこと。

3. 情報の保護

受注者は、次の対策に努めること。

共通	➢ 市の承諾なしに、市保有情報の一部又は全部を第三者へ提供することのない制御すること。
市保有情報	➢ 市保有情報を取扱う作業従事者を明確にし、その範囲内でのみ取扱うよう制御すること。 ➢ 市保有情報を保管する場所は、作業従事者のみが取扱えるよう制御すること。 ➢ 契約満了時等で市保有情報を市へ返却する際は、受注者内にデータ等が残らないよう消去する手順が確立すること。 ➢ 市保有情報を受注者のファイルサーバ等で電子データとして保有する場合、作業従事者のみがアクセスできるよう制御すること。 ➢ 市保有情報を作業従事者が市に無断で持ち出すことがないよう管理を徹底すること。 ➢ 市保有情報を市と電子メールでやり取りする場合、暗号化等の情報漏えい対策を行った上でやり取りすること。 ➢ 市保有情報を運搬することがある場合、盗難及び紛失対策を行った上でやり取りすること。
重要情報	【**市保有情報における制限に加えて**】 ➢ 業務従事者のパソコンは、関係者以外からの覗き見防止等の対策を行うこと。 ➢ 業務従事者が USB メモリ等の電磁的記録媒体を使って不正に情報がコピーされることがないよう適切に制御すること。 ➢ 業務従事者のパソコンは、OS 等を最新の状態とすること。ただし、システムの動作検証のため、過去のＯＳを使用する必要があるなど、理由がある場合については、この限りでない。 ➢ 業務従事者のパソコンは、盗難及び紛失時にデータが漏えいしないよう対策が施すこと。

4. ネットワークの強靭化対策

受注者は、重要情報を取扱う作業環境を様々な情報セキュリティリスクから保護しなければならない。また、特定個人情報を取扱う環境はインターネットから分離した環境を用意し、そこでのみ取扱うこと。その他、総務省が発行する「地方公共団体における情報セキュリティポリシーに関するガイドライン（以下「総務省ガイドライン」という。）」で示された基準を遵守すること。

5. 物理的セキュリティ

受注者は、原則として次の物理的対策を講じること。

管理区域	➢ サーバ等の機器を設置する場所は、管理区域とし管理すること。 ➢ 外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止すること。 ➢ 管理区域への入室は、入退室を許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行うこと。 ➢ 管理区域に入室する場合、身分証明書等を携帯し、求めにより提示すること。 ➢ 当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないこと。
装置のセキュリティ	➢ サーバ等の機器の取付けを行う場合、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正に固定する等、必要な措置を講じること。 ➢ 通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じること。 ➢ 電磁的記録媒体を内蔵する機器を受注者以外に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、管理責任者は、外部の事業者に故障を修理させるにあたり、修理を行う事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行うこと。
通信回線・機器	➢ ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施すること。 ➢ 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らすこと。

6. 人的セキュリティ

受注者は、業務従事者に対し必要な情報セキュリティ教育・トレーニングを行うこと。また、市の求めに応じてその実施記録の提示を行うこと。なお、業務従事者に対し、異動、退職等により業務を離れる場合には、利用していた機器等を返却させるとともに、その後も業務上知り得た情報を漏らしてはならない旨を合意させること。

7. 技術的セキュリティ

受注者は、次の情報セキュリティ対策を行うこと。

アクセス制御	➢ 原則として、情報システム及びパソコンを使用する際は、業務従事者ごとに ID を発行すること。 ➢ 業務従事者の ID は、本人以外がアクセスできないよう認証方法は最良の方法を選択すること。
開発・導入	➢ 開発で用いる環境に対して、管理責任者の管理の元で適切な対策を行うこと。 ➢ システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除すること。 ➢ システム開発、保守及びテスト環境とシステム運用環境を分離すること。 ➢ 重要情報を、テストデータに使用しないこと。
不正プログラム対策	➢ 業務従事者が操作するパソコン等は、コンピュータウイルス等の不正プログラム対策ソフトウェアを導入し、パソコン等に常駐させること。 ➢ 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保つこと。
不正アクセス対策	➢ 外部からの不正アクセス及び内部不正に備え、情報漏えいを防止するために必要な対策を講じること。 ➢ 不正通信、不正操作等を牽制するための必要な監視を行うこと。

8. 監査等への協力

受注者は、市の求めに応じて立入検査等に応じること。

9. その他

受注者は、上記以外の基準が必要となった場合は、総務省ガイドラインを参照するとともに、市と協議し対策を行うこと。

以 上