指定管理業務に係る特記仕様書

【労働関係法令等遵守に関する留意事項】

第1　指定管理者は、指定管理者としての業務（以下「指定管理業務」という。）に従事する労働者について、労働基準法、労働安全衛生法、最低賃金法、健康保険法、厚生年金保険法、雇用保険法、労働者災害補償保険法などの関係法令を遵守すること。

2　指定管理者は、指定管理業務の一部を第三者に委託するときは、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）及び中小受託取引適正化法などの関係法令を遵守すること。

【公契約（指定管理者による公の施設の管理に関する協定を含む）**に関する留意事項】**

第1　指定管理者は、公契約に係る基本方針を定め、市及び事業者等の責務を明らかにするとともに、公契約に関する基本的事項を定めることにより、市及び事業者等が一体となって公契約に関する制度の適正な運用を図り、良質な公共サービスが提供され、市民が豊かで安心して暮らすことができる地域社会及び地域経済の健全な発展に寄与することを目的とした岐阜市公契約条例を遵守すること。

【不当介入への対応に関する留意事項】

第1　指定管理者は、指定管理者としての業務（以下「指定管理業務」という。）の履行に当たって、暴力団若しくは暴力団員又はこれらと密接な関係を有する者から、事実関係及び社会通念等に照らして合理的な理由が認められない不当若しくは違法な要求又は指定管理業務の適正な履行を妨げる妨害（以下「不当介入」という。）を受けたときは、当該不当介入を管轄する警察署長に通報するとともに、市に報告しなければならない。

【障害者差別解消法への対応に関する留意事項】

第1　指定管理者は、利用者の利便性向上等の観点から、障がいのある人に対し、「障害を理由とする差別の解消の推進に関する法律（平成二十五年法律第六十五号）」第11条第1項に規定する指針に基づき対応すること。また、指定管理者が提供すべき合理的配慮については、岐阜市と指定管理者の間で大きな差異が生じないよう努めること。

【個人情報の取扱いに関する留意事項】

（基本的事項）

第1　指定管理者は、個人情報の保護の重要性を認識し、指定管理者としての業務（以下「指定管理業務」という。）を実施するに当たっては、個人情報の保護に関する法令及び岐阜市情報セキュリティポリシーの規定を遵守し、個人の権利利益を侵害することのないよう、個人情報の取扱いを適切に行わなければならない。

（責任体制の整備）

第2　指定管理者は、個人情報の安全管理について、内部における責任体制を構築し、その体制を維持しなければならない。

（責任者等の届出）

第3　指定管理者は、指定管理業務の実施における個人情報の取扱いの責任者（以下この条において「責任者」という。）及び事務に従事する者（以下「事務従事者」という。）を定めなければならない。

2　指定管理者は、責任者に、本特記仕様書に定める事項を適切に実施するよう事務従事者を監督させなければならない。

3　指定管理者は、事務従事者に、責任者の指示に従い、本特記仕様書に定める事項を遵守させなければならない。

4　指定管理者は、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9項に規定する特定個人情報を取り扱う業務にあっては、責任者及び事務従事者をあらかじめ書面により市に届け出なければならない。責任者又は事務従事者を変更する場合も同様とする。

（教育及び研修の実施）

第4　指定管理者は、全ての事務従事者に対し、個人情報を取り扱う場合に遵守すべき事項、当該事項に違反した場合に負うべき責任その他指定管理者として行う業務の適切な履行に必要な教育及び研修を実施しなければならない。

（取得の制限）

第5　指定管理者は、指定管理業務を行うために個人情報を取得する場合は、事務の目的を明確にし、その目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

2　指定管理者は、指定管理業務を行うために個人情報を取得する場合は、本人から直接取得し、又は本人以外から取得するときは本人の同意を得た上で行わなければならない。ただし、市の承諾があるときは、この限りでない。

（利用及び提供の制限）

第6　指定管理者は、指定管理業務に関して知り得た個人情報を当該業務の目的以外の目的に利用し、又は第三者に提供してはならない。ただし、市の承諾があるときは、この限りでない。

（改ざん、漏えい、滅失及び毀損の防止等）

第7　指定管理者は、指定管理業務に関して知り得た個人情報について、改ざん、漏えい、滅失及び毀損の防止その他の個人情報の適正な管理のために必要な措置を講ずるものとする。

2　指定管理者は、市が承諾した場合を除き、指定管理業務に関して知り得た個人情報を、当該業務において当該個人情報を取り扱う場所（以下「作業場所」という。）から持ち出してはならない。

（廃棄等）

第8　指定管理者は、指定管理業務に関して知り得た個人情報について、保有する必要がなくなったときは、確実かつ速やかに廃棄し、又は消去しなければならない。

（秘密の保持）

第9　指定管理者は、指定管理業務に関して知り得た個人情報の内容を、法令等で認められた場合を除いては、他人に知らせてはならない。指定管理業務が終了し、又は指定を取り消された後においても、同様とする。

（複写又は複製の禁止）

第10　指定管理者は、指定管理業務を処理するために市から引き渡された個人情報が記録された資料等を複写し、又は複製してはならない。ただし、市の承諾があるときは、この限りでない。

（事務従事者への周知）

第11　指定管理者は、事務従事者に対して、在職中及び退職後においても、当該事務に関して知り得た個人情報の内容を、法令等で認められた場合を除いては、他人に知らせ、又は不当な目的に使用してはならないことなど、個人情報の保護に必要な事項を周知させるものとする。

（資料等の返還等）

第12　指定管理者は、指定管理業務を処理するために、市から提供を受け、又は指定管理者自らが取得し、若しくは作成した個人情報が記録された資料等は、指定管理業務が終了し、又は指定を取り消された後直ちに市に返還し、又は引き渡すものとする。ただし、市が別に指示したときは、当該方法によるものとする。

（報告）

第13　指定管理者は、指定管理業務の履行について、市に定期的に報告しなければならない。

2　指定管理者は、指定管理業務に係る協定に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに市に報告し、市の指示に従うものとする。

（再委託の禁止）

第14　指定管理者は、指定管理業務を再委託してはならない。ただし、市の承諾を受けたときは、この限りでない。

2　指定管理者は、再委託の相手方に指定管理業務に基づく一切の義務及び本特記仕様書に定める全ての事項を遵守させるとともに、指定管理者と再委託の相手方との契約関係にかかわらず、市に対して再委託の相手方による個人情報の取扱いに関する責任を負うものとする。

3　指定管理者は、市の承諾を得て再々委託を行う場合において、再々委託の契約内容にかかわらず、市に対して個人情報の取扱いに関する責任を負うものとする。

（情報セキュリティ対策）

第15　指定管理者は、情報セキュリティ対策の実施状況について、協定締結後一週間以内に「（別紙）情報セキュリティ対策チェックシート」を作成し、提出すること。再委託する場合、再委託先も「情報セキュリティ対策チェックシート」による点検を実施し、指定管理者の責任で問題ないことを確認の上、提出すること。

（派遣労働者等の利用時の措置）

第16　指定管理者は、指定管理業務を派遣労働者によって行わせる場合、労働者派遣契約書に、秘密保持義務等個人情報の取扱いに関する事項を明記しなければならない。この場合において、守秘義務の期間は、第9の規定に準じるものとする。

2　指定管理者は、派遣労働者に指定管理業務に関する一切の義務を遵守させるとともに、指定管理者と派遣元との契約内容にかかわらず、派遣労働者による個人情報の処理に関し、市に対して責任を負うものとする。

（立入調査）

第17　市は、指定管理者が指定管理業務の執行に当たり取り扱っている個人情報の状況について、個人情報の保護のため必要な措置が講じられているか確認する必要があると認めるときは、指定管理者に報告を求め、又は指定管理者の作業場所を立入調査することができる。

（事故発生時等の公表）

第18　市は、個人情報の漏えい、滅失、毀損等の事故を把握した場合には、必要に応じ、指定管理者及び再委託先（再々委託先を含む。）の名称並びに当該事故の概要その他の必要事項を公表するものとする。

（契約の解除）

第19　市は、指定管理者が本特記仕様書に定める義務を果たさない場合は、指定管理者としての指定を取り消し、又は業務の全部若しくは一部を停止することができる。

2　指定管理者は、前項の規定に基づく指定の取消し及び業務の停止により損害を被った場合においても、市にその損害の賠償を求めることはできない。

（損害賠償）

第20　指定管理者は、指定管理業務において、本特記仕様書の定めに反した取扱いにより市又は第三者に損害を与えた場合は、その損害の全額を賠償しなければならない。

別紙●

情報セキュリティ対策チェックシート

	チェック内容	はい	いいえ	該当無
1. 契約時の「情報セキュリティ要件」等の遵守状況				
	貴社は、契約時の「情報セキュリティに関する要件」や「個人情報取扱特記仕様書」などの諸規定を、本業務に従事する技術者等（再委託先を含む。以下、「従事者」という。）に遵守させるよう教育し、教育・指導の記録を管理していますか？※特定個人情報取扱業務については、発注者の指示に従い、個人情報保護研修の実施状況、従事者の署名入りの研修記録を提出してください。	□	□	□
2. 組織的安全管理				
2-1	情報セキュリティ対策に関わる責任者と担当者の役割や権限が明確になっていますか？具体的には、個人情報保護責任者、個人情報保護担当者は任命されていますか？	□	□	□
2-2	重要な情報またはそれを管理する物品等について、入手、利用、保管、交換、提供、作成、消去、破棄における取扱手順を定めていますか？	□	□	□
2-3	情報資産の業務目的以外の使用及び第三者への提供の禁止を、従事者に対して遵守させていますか？	□	□	□
2-4	契約期間中及び契約終了後においても、業務で知り得た秘密を他に漏らしてはならないことを、従事者に対して遵守させていますか？	□	□	□
2-5	個人情報管理台帳等により、管理すべき重要な情報資産を把握し、区分していますか？また、その更新を行っていますか？	□	□	□
2-6	再委託を行う場合、発注者の事前の承認を得ていますか？また、再委託先の個人情報保護管理体制を確認し、機密保持契約を締結するとともに、本チェックシートによる点検をしていますか？	□	□	□
2-7	内部点検を定期的に実施していますか？また、点検に基づく改善を行っていますか？	□	□	□
2-8	情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はそれと同等の認証を取得し、適切に更新していますか？（受注者及び再委託先の事業者）（※特定個人情報取扱業務については、受注者及び再委託先の事業者についても認証証明書の写しを提出してください）	□	□	□
3. 人的安全管理				
3-1	委託業務に関わる従業員（契約社員、パート、アルバイトを含む）から機密保持に関する誓約書など取得していますか？	□	□	□
3-2	派遣社員を使用している場合、派遣会社と機密保持契約を結び、自社の個人情報保護の仕組み・手順を理解させ、誓約書を取得していますか？	□	□	□
3-3	アクセス権限を付与する従業員は必要最小限に限定し、かつアクセス権限の範囲も必要最小限に限定していますか？	□	□	□
4. 物理的安全管理				
4-1	私物のパソコン及び不正な記録媒体の接続を禁止していますか？	□	□	□
4-2	パソコン等の端末、記録媒体、情報資産及びソフトウエア等を外部に持ち出す場合、情報セキュリティ対策に関わる責任者等の許可を得ていますか？	□	□	□
4-3	重要な情報を含む書類、記憶媒体、モバイルPC等の保管場所やそれらを扱う場所について、施錠管理や入退管理を行っていますか？	□	□	□
4-4	重要な情報を含む書類、記憶媒体、モバイルPC等について、整理整頓を行うとともに、取り扱う場所への監視カメラ設置などの盗難防止対策や確実な廃棄を行っていますか？	□	□	□
4-5	市や外部の組織と情報をやり取りする際に、情報の取扱いに関する注意事項について合意し、管理簿等で保管期限（5年）を定めた上で、記録をとって実施していますか？	□	□	□
5. 技術的安全管理				
（1）情報システム及び通信ネットワークの管理				
5-1	情報システム（本業務システムだけでなく、貴社が管理するシステム、パソコン等も含む。）のセキュリティ対策に関する運用ルールを策定していますか？	□	□	□
5-2	ウイルス対策ソフトは常時最新のパターンファイルに更新していますか？	□	□	□
5-3	導入している情報システムに対して、最新のパッチを適用する等の脆弱性対策を行っていますか？	□	□	□
5-4	通信ネットワークを流れる重要なデータ、電子メールに添付する機密情報などに対して、暗号化等の保護策を実施していますか？	□	□	□
5-5	情報システムを扱う機器からUSBメモリ等へデータを外部に持ち出す場合、データ持出し制限、承認者による持出し許可、持出し記録の管理を行っていますか？	□	□	□
5-6	モバイルPCやUSBメモリ等の記憶媒体でデータを外部に持ち出す場合、盗難、紛失等に備えて、適切なパスワード設定や暗号化等の対策を実施していますか？	□	□	□
5-7	インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISPサービス等）や不正な通信、不正操作の有無を確認するため、ログ（通信記録）の取得や管理、監視を行っていますか？	□	□	□
5-8	無線LAN のセキュリティ対策（強力な暗号化方式（WPA2またはWPA3）と認証方式（AES方式））を行っていますか？	□	□	□
5-9	メール誤送信を防ぐ対策（メール送信前確認や強制BCC化）及び運用ルールを設けていますか？	□	□	□
（2）アクセス制御				
5-10	情報システム（本業務システムだけでなく、貴社が管理するシステム、パソコン等も含む）へのアクセスを制限するために、利用者IDの管理を行っていますか？	□	□	□
5-11	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セキュリティ対策（推測可能なパスワード、初期パスワードの設定禁止、認証の総当たり攻撃対策、機器内のセキュリティパラメータの保護）を行っていますか？	□	□	□
5-12	重要な情報に対するアクセス権限の設定を行っていますか？ また、アクセス記録は保管期限（5年）を定め取得し、保管していますか。	□	□	□
5-13	改ざんや漏えい防止のため、リスクが大きい振る舞いを検知する仕組みや、各種ログの点検を定期的に行う体制が整備されていますか？不要なポートを閉じ、外部からアクセスできる通信経路を必要最小限に絞っていますか？	□	□	□
6. 事故対応				
6-1	情報セキュリティに関する事件や事故等（情報漏洩、ウィルス感染等）の緊急時対応の手続き、報告書の様式、連絡体制は整備できていますか？また、事故の再発防止への取組はされていますか？	□	□	□
6-2	情報システムに障害が発生した場合、業務を再開するため緊急時対応計画、緊急時連絡網の整備を策定し、訓練をしていますか？	□	□	□

※「いいえ」に該当する項目については、業務着手までに対策を実施してください。対策については、発注者と協議の上実施してください。
※「該当無」に該当する項目については、特に対策は必要ありません。