「個人情報・情報資産取扱特記事項」

1　基本的事項

受託者は、この契約に基づき委託された業務（以下「委託業務」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律（平成15年法律第57号。以下「法」という。）、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。以下「番号法」という。）、福岡市情報セキュリティに関する規則（平成23年福岡市規則第51号）及び情報セキュリティ共通実施手順その他関係法令を遵守し、個人情報及び情報資産の機密性、完全性、可用性を損なうことのないよう、個人情報及び情報資産を適正に取り扱わなければならない。

特に個人情報については、法第66条第２項において、受託者に行政機関等と同様の安全管理措置が義務付けられていることから、その保護の重要性を認識し、適正に取り扱わなければならない。

2　定義

（１）個人情報

法第２条第１項に規定する個人情報をいう。

（２）情報資産

次に掲げるものをいう。

・ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

・ネットワーク及び情報システムで取り扱う情報（ＯＡソフトウエアで取扱われるファイルを含む）並びにそれらを印刷した文書

・ネットワーク及び情報システムに関連する文書

（３）機密性

情報の利用を認められた者だけがその情報を利用することができることをいう。

（４）完全性

情報が破壊、改ざん又は消去されていないことをいう。

（５）可用性

情報の利用を認められた者が、必要な場合に中断されることなく、情報を利用することができることをいう。

3　秘密保持

受託者は、委託業務に係る個人情報並びに情報資産及び情報資産に関する情報を他人に知らせてはならない。この契約が終了し、又は解除された後においても同様とする。

4　従業者の監督等

受託者は、その従業者に委託業務に係る個人情報及び情報資産を取り扱わせるに当たっては、当該個人情報及び情報資産の安全管理が図られるよう、次に掲げる事項を周知し、その他必要かつ適切な監督を行わなければならない。

・委託業務に係る個人情報及び情報資産について、その適正な取扱い及び機密性、完全性、可用性の維持に必要な事項を遵守すること。

・個人情報を正当な理由なく利用したり、他人に提供したり、盗用した場合、法に規定する罰則が適用される場合があること。
・上記の各事項は、委託業務に従事中のみならず、従事しなくなった後も同様であること。
・従業者の情報資産へのアクセス権限は、担当業務の内容に応じた最小限の権限に限定するとともに、取扱う情報資産の重要度に応じて複数人による確認の実施等を行うこと。

5　作業場所の制限

受託者は、定められた履行場所以外で委託業務に係る個人情報及び情報資産を取り扱ってはならない。ただし、福岡市（以下「市」という。）の書面による承認があるときは、この限りではない。

6　収集に関する制限

受託者は、委託業務の実施に当たって個人情報を収集するときは、この契約の目的を達成するため必要な範囲内で、適法かつ公正な手段により行わなければならない。

7　使用及び提供に関する制限

受託者は、委託業務以外の目的のために委託業務に係る個人情報及び情報資産を利用し、又は第三者へ提供してはならない。ただし、市の書面による承認があるときは、この限りではない。

8　安全確保の措置

受託者は、委託業務に係る個人情報及び情報資産の適切な管理のために、市が求める個人情報保護及び情報セキュリティの体制を備えるとともに、その他必要な措置を講じなければならない。

9　複写、複製又は加工の制限

受託者は、委託業務に係る個人情報及び情報資産が記録された文書、電磁的記録等を複写、複製又は加工してはならない。ただし、市の書面による指示又は承認があるときは、この限りではない。

10　再委託の制限

受託者は、委託業務に係る個人情報及び情報資産については、自ら取り扱うものとし、第三者に当該個人情報及び情報資産の取扱いを委託してはならない。ただし、市の書面による承認があるときは、この限りでない。なお、市の承認により第三者に委託する場合は、当該第三者に対して、契約書及び特記事項に規定する個人情報及び情報資産の取扱いの義務を遵守させるものとする。

11　委託業務終了時の返還、廃棄等

受託者は、この契約が終了し、又は解除されたときは、委託業務に係る個人情報及び情報資産を、市の指示に従い、市に返還し、若しくは引き渡し、又はその廃棄、消去等をしなければならない。なお、廃棄又は消去等をしたときは、廃棄又は消去等を行った旨の証明書を提出しなければならない。

12　報告及び監査・検査の実施

市は、受託者における委託業務に係る個人情報及び情報資産の取扱いの状況について、契約内容の遵守を確認するため、年に１回以上、原則として実地検査を行うほか、定期的に書面による報告を求

め、必要に応じて監査又は検査をすることができる。

なお、実地検査を行うに当たっては、別添「個人情報・情報資産の委託先監督チェックリスト」により確認を行うものとする。

13　事故等発生時の報告

受託者は、個人情報及び情報資産の機密性、完全性、可用性を損なう、又は損なうおそれのある事故並びに欠陥及び誤動作を発見したときは、直ちに市に報告し、市の指示に従わなければならない。

14　事故等発生時の公表

市は、個人情報及び情報資産の機密性、完全性、可用性を損なう事故等が発生した場合、市民に対して適切な説明責任を果たすために必要な当該事故等の情報の公開を行うことができる。

15　契約の解除及び損害の賠償

市は、受託者がこの特記事項の内容に違反したときは、この契約の解除及び損害賠償の請求をすることができる。この場合において、受託者に損害を生じることがあっても、市はその責めを負わないものとする。

決裁	・・	課長	係長	担当者

個人情報・情報資産の委託先等監督チェックリスト

このチェックリストは、契約書添付の「個人情報・情報資産取扱特記事項」の各項目に関し、委託先等において適切に実施されていることを確認するためのものです。実地検査を行う場合は、このチェックリストに基づいて、委託先等の安全管理措置状況を確認してください。

契約件名		確認者	
委託先等		補助者	

適→○　否→×　該当なし→／

確認項目			確認結果	実施日	確認内容
1	組織体制等	**①個人情報等の管理体制を確認**			
		ア.個人情報等の取扱責任者や取り扱う担当者は明確になっているか。			
		イ.取り扱う文書・データの種類、個人情報等の記載項目は明確にされているか。			
		②漏えい事故等発生時の体制を確認			
		ア.委託業者内での報告体制は明確になっているか。			
		イ.委託業者から市への報告体制は明確になっているか。			
		③従事者に対する研修の実施状況を確認			
		ア.研修資料、対象者、実施回数は適切か。			
		④業務の再委託は原則として認められないことを踏まえた確認			
		ア.業務の再委託を行う場合、市からの承諾を得ているか。			
		イ.再委託先で個人情報の取り扱いがある場合、再委託先でも同等の措置が行われることを確認しているか。			
2	作業場所、保管場所	**①個人情報等を取扱う作業場所を確認**			
		ア.個人情報等を取り扱う区域や場所を明確に定めているか。			
		イ.入退室管理を適切に行っているか。			
		ウ.十分なスペースが確保され、整理整頓されているか。			
		②個人情報等の保管場所を確認			
		ア.個人情報等の保管場所・保管方法は適切か。（個人番号が記載された書類は、施錠できる場所に保管しているか。）			
		イ.USBメモリ等の電磁的記録媒体を使用する場合、施錠できる場所に保管されているか。			
		ウ.本契約に関係のない他の書類、電磁的記録媒体等と区分されているか。（自社のものや他契約のもの）			
		③個人情報を含むデータの保存場所や取り扱いの状況を確認			
		ア.個人情報等を含むデータが、アクセス権やパスワード等により、許可された者のみが閲覧できる場所に適切に保存されているか。			
		イ.サーバーおよび端末において、修正プログラムが適切に適用され、ウイルス対策ソフトが最新状態で運用されているか。			

確認項目			確認結果	実施日	確認内容
3	個人情報の収受、利用	**①漏えい等の事故を防止するための対策を確認**			
		ア.個人情報等の収受や送付について、記録等の管理が行われているか。（日時・書類名・担当者等）			
		イ.郵送時に、封入物のダブルチェックをするなど誤送付対策が適切に行われているか。			
		ウ.メール送信時には、事前に複数人で確認するなど誤送付対策が適切に行われているか。			
		エ.WEBへの公開時には、事前に複数人で確認するなど公開情報の確認等の対応を行っているか。			
		②作業場所以外への持ち出し時の安全対策を確認			
		ア.契約書等で定められた場所以外に持ち出しを行っていないか。持ち出す場合は、市に書面で承認を得ているか。			
		イ.持ち出す場合、責任者に許可をとるとともに、日時、書類・データの名称、持出先、持ち出し者名などを記録しているか。			
		ウ.施錠可能なバッグを使用するなど、紛失・盗難対策を行っているか。			
		エ.USBメモリ等でデータを持ち出す場合、暗号化やパスワード設定を行っているか。			
		③業務目的以外での利用、外部提供、複製を確認			
		ア.業務以外の目的で複製や加工を行う場合、市に書面で承諾を得ているか。			
		イ.業務以外の目的外利用をする場合（自社の営業活動など）、市に書面で承諾を得ているか。			
4	返還・廃棄・消去	**①個人情報の返還や廃棄が適切に行われていることを確認**			
		（個人情報を市に返還する場合） ア.返還が必要な書類や電磁的記録媒体等の引き渡しを受けたか。			
		（個人情報を委託業者で廃棄・消去する場合） イ.媒体に応じて適切な方法で、復元不可能な方式により廃棄等を行った旨の証明書は提出されているか。			

【確認要領】

① 特記事項に基づき、少なくとも年１回以上、原則として実地検査により確認を行ってください。
※委託先が遠隔地にある等の理由により現地に赴くことが難しいような事情がある場合は、例えばテレビ通話や写真等で管理の現況を確認するなど、代替方法により確実に検査を実施してください。
※確認項目１及び４については、提出された書類等の確認を持って検査に代えることもできますが、必要に応じて実地検査により確認を行ってください。

② 実地検査は原則として本契約の監督員が実施してください。やむを得ず監督員以外の者が実施する場合は、事前に所属長に承認を受けた者が実施してください。また、必要に応じて補助者を指名し、複数人で確認を行ってください。

③ 確認項目ごとに、確認結果及び実施日、確認内容を記載してください。
【確認結果】 適→〇　否→×　該当なし→／　※業務内容により確認する必要がない項目は「該当なし」を選択
【実 施 日】 実地検査を行い確認した日を記載
【確認内容】 実地検査において確認した内容（適否判定の根拠）を記載

④ 確認結果が「否（×）」の場合は、委託先等と協議の上、改善に要する期間を定め、改善を指導してください。
また、改善結果を報告させるとともに、必要に応じて再度実地検査を実施するなどして、改善状況を確認してください。
なお、改善が確認できた場合は、確認内容欄にその旨（再確認日・改善結果）を追記してください。

⑤ 全ての項目の確認が終了した後、課長まで決裁のうえ、契約書に編綴してください。

※ 業務内容に応じて項目の追加が必要な場合は、適宜確認項目を追加（行を追加）して実施してください。
ただし、既存の確認項目について削除または改変する場合は、事前に情報セキュリティ統括管理者に協議が必要です。
（情報セキュリティ共通実施手順８(1)①ウ）