

指定管理業務における情報セキュリティ対策に関する特記仕様書

(目的)

- 第1 この仕様書は、管理業務において、コンピュータ等の情報機器を用いて利用者の個人情報及びその他管理業務に関する情報を取り扱う場合、その適切な取扱いを確保し、情報の機密性、完全性、可用性を維持するために必要な事項を定めるものとする。

(定義)

- 第2 この仕様書において、「電子計算機」とは、ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器並びに記録媒体（磁気ディスク等並びに入出力帳票及び情報システム仕様書等）をいう。
- 2 この仕様書において、「業務情報」とは、利用者の個人情報及びその他管理業務に関する情報をいう。
- 3 この仕様書において、「市所管システム」とは、本市が所管する電子計算機及びネットワークをいう。

(管理体制)

- 第3 乙は、電子計算機及び業務情報を管理する責任者（以下「管理責任者」という。）を定め、甲に報告するものとする。
- 2 管理責任者は、電子計算機及び業務情報の取扱いにあたり、あらかじめ従事する職員（以下「作業従事者」という。）を指名し、それ以外の者に取り扱わせてはならない。
- 3 管理責任者は、市所管システムの取扱いについては、本市当該システム管理者の指示に従い、適切に行なわなければならない。
- 4 管理責任者は、電子計算機及び業務情報の取扱いについて、情報セキュリティが確保されているか定期的に点検し、必要に応じて改善措置を講じなければならない。

(電子計算機及び業務情報の取扱い)

- 第4 管理責任者は電子計算機及び業務情報の取扱いについて、以下の事項について必要な措置を施さなければならない。
- ① 電子計算機及び業務情報について、作業従事者以外に使用させないこと、又は許可なく情報を閲覧させないこと。
 - ② 電子計算機に盗難防止用ワイヤーの設置等の盗難防止対策を必要に応じて行なうこと。
 - ③ 電子計算機の配線について、傍受又は損傷等を受けることがないように必要な対策を行なうこと。
 - ④ 業務情報が許可なく持ち出され、又は必要のない者が利用することができないよう、施錠可能な保管庫に保管するなど適切に管理すること。
 - ⑤ 電子計算機の設置場所に関して、上記①から④の事項が満たされるよう、物理的対策等を考慮すること。
 - ⑥ 電子計算機のID、パスワードを厳重に管理すること。
 - ⑦ 電子計算機に業務情報を入力する際、情報の正確性が保たれる対策を講じること。
 - ⑧ 電子計算機及び業務情報に障害が発生し、管理業務に支障をきたす場合、障害内容を調査し、甲へ速やかに報告すること。

2 クラウドサービスを用いて業務情報を取り扱う場合、管理責任者はその取扱いについて、以下の事項について必要な措置を施さなければならない。

- ① クラウドサービスの利用にかかる法律関係は、日本国内法が適用されること。
- ② 日本国の法令の範囲内で運用できるクラウドサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。
- ③ 通信経路並びに業務情報を保存するサイバー空間（バックアップを含む）について、暗号化その他これに準ずる適切な安全管理措置が講じられていること。
- ④ SaaS 提供事業者（当該 SaaS を管理する者を含む。）及び指定管理者が当該 SaaS の管理画面等にログインする場合において、次のいずれか又はこれらに準ずる不正アクセス防止措置が講じられていること。
 - ・ 複数要素認証又は二段階認証
 - ・ 一定回数以上の認証失敗時にアカウントをロックする機能
 - ・ その他同等の安全性を有すると認められる措置
- ⑤ 業務情報を保存するサーバは、日本国内法が適用される場所に設置されていること。
ただし、これを満たさない場合には、次のいずれかの要件を満たすこと。
 - ・ 海外のデータセンターに個人情報を含む業務情報が保存される場合において、当該個人情報の本人から、法令に基づき適切に同意を取得していること。
 - ・ 海外のデータセンターに個人情報を含む業務情報が保存される場合であって、日本と同等水準の個人情報保護に関する法制度が整備されている国又は地域に当該データセンターが設置されていること。
 - ・ 海外のデータセンターに業務情報が保存される場合であって、保存される情報が公開情報その他個人の権利利益又は本市の行政運営に影響を及ぼすおそれがないと本市が認めた情報に限られること。
- ⑥ 契約終了時又はサーバの廃棄時において、指定管理者又は IaaS/PaaS 事業者が実施する業務情報の消去については、当該業務情報を復元できない方法により確実に行われること。

（作業従事者への指導）

第5 管理責任者は電子計算機及び業務情報を取り扱う作業員に対して、以下の事項を遵守させるため、教育、訓練その他必要な指示・指導を行なわなければならない。

- ① 電子計算機及び業務情報を業務目的以外に利用してはならないこと。
- ② 業務情報の複製又は送付・送信は、作業上必要な場合であって、管理責任者の許可を得た場合を除き、行ってはならないこと。
特に、業務情報の自宅への持ち帰りや電子メールによる自宅への送信は行ってはならないこと。
- ③ 電子計算機及び業務情報を管理責任者の許可なく執務室外へ持ち出してはならないこと。
- ④ 業務情報を部外者へ提供してはならないこと。
- ⑤ 電子計算機の操作のために与えられたパスワードについて、他人に教えたり、目につく場所にメモを貼ったりしないようにするなど、パスワードの秘密保持に努めること。
- ⑥ 電子計算機を利用しない時は、ログアウトを行なうこと。

- ⑦ 市所管システムの操作等について、当該システムに関する各実施手順書に定めている事項を遵守すること。

(電子計算機及び業務情報の取扱いに関する調査)

- 第6 甲は、電子計算機及び業務情報の取扱いの状況について、乙の作業場所その他の施設について、定期又は不定期に調査を行うことができる。
- 2 甲は、前項の調査により、乙の電子計算機及び業務情報の取扱いに不適切な点を認めるときは、乙に対して、必要な是正措置をとるべきことを求めることができる。
- 3 乙は、前項の是正措置の求めに対して、速やかに対応し、甲の承認を受けなければならない。