

セキュリティ保全に係る事項

受託業務の履行にあたっては、本市の情報資産の漏洩、紛失、滅失、毀損、盗難等を防止するため、本市の指示に基づき、セキュリティ保全のための対策を下記のとおり実施するようお願いいたします。

記

セキュリティ保全のための対策	
1	<p>情報セキュリティを確保するための体制の整備</p> <p>本受託業務の従事者については、事前に本市へ届出を行い、届出ている従事者以外の者に情報資産を取扱う作業を実施させない。なお、従事者の届出を行う場合は、本受託業務の業務責任者および情報セキュリティ対策の責任者を明確にすること。</p>
2	<p>取り扱う情報資産の秘密保持等</p> <p>本業務の遂行にあたり知りえたすべての情報は、履行期間及び履行後において第三者に漏らしてはならない。データの取扱についても同様とする。また、以下の事項を遵守すること。</p> <ul style="list-style-type: none"><li>(1) 本市の許可なく、所定の保管場所から持ち出すことの禁止</li><li>(2) 本受託業務の目的以外で利用することの禁止</li><li>(3) 本市の情報資産が記録されたデータ又はドキュメントを許可なく複写及び複製することの禁止</li></ul>
3	<p>運用・保守・点検における情報セキュリティ対策の実施</p> <p>本市が用意した環境で作業を実施する際には、以下の事項を遵守すること。</p> <ul style="list-style-type: none"><li>(1) 端末・周辺機器の利用<ul style="list-style-type: none"><li>ア 本業務の作業場所に個人所有の端末や周辺機器などの持込禁止</li><li>イ 端末・周辺機器の本業務の目的以外利用の禁止</li><li>ウ 端末への情報資産保存の禁止</li><li>エ 端末へのソフトウェアのインストール・アンインストールの禁止</li><li>オ プリンタ設定変更の禁止</li><li>カ 業務終了時又は利用終了時におけるログオフ又は端末機のシャットダウンの励行</li><li>キ 離席時における端末機等ロックの励行</li><li>ク 端末の室内・室外への移設禁止</li><li>ケ 端末への周辺機器の接続禁止</li></ul></li><li>※ 禁止事項についてやむを得ず実施が必要な場合は、本市の許可を得て行うこと。</li></ul> <p>(2) 作業環境・作業場所の利用</p>

- ア 本市によって定められた入退室・在庁の手続きを遵守し、入退室管理を行うこと。
- イ 本市の管理下にある作業場所では常に社員証を周囲から容易に識別できる位置に着用すること。
- ウ 貸与されたICカードは破損、紛失、盗難にあわないよう管理する。
- エ 貸与されたICカードを他の者に貸与し、又は他の者と共用してはならない。
- オ 貸与されたICカードの記録情報の解析等を試みる行為を行ってはならない。
- カ 貸与されたICカードのパスワードが他の者に認知されることのないよう厳重に管理する。

### (3) システム上の環境の利用

- ア 本市から展開される環境関連のドキュメントを確認し、制約事項を遵守する。
- イ 本市から貸与された作業用ユーザーID のパスワードが他の者に認知されることのないよう厳重に管理する。

## 4 外部委託する業務以外の情報資産の保全

本業務で使用する情報資産以外へのアクセスは行わないこと。

## 5 情報セキュリティインシデントが発生した場合の対処

情報セキュリティインシデントが発生した場合には速やかに本市へ報告すること。また、本市が行う調査や対応に協力すること。

## 6 情報セキュリティ対策の履行状況の報告

前項までの各項目の履行状況について「セキュリティ保全状況報告書」により定期的に本市へと報告すること。

## 7 情報セキュリティ監査の実施

情報セキュリティ対応について本市から指示があった場合には、受託者にて監査を実施し、本市へと報告すること。また、個人情報など重要性の高い情報資産を取り扱う場合には、少なくとも年1回は本市が直接監査もしくは実地調査を行うため、受託者は積極的に協力すること。

## 8 情報セキュリティ対策の履行が不十分であると思われる場合の対処

受託者の情報セキュリティ対策の履行が不十分であることが認められた場合、本市と協議した上で、本業務の一時中断や損害賠償等、必要な措置を講ずること。

## 9 委託業務終了時の情報資産の返還、廃棄等

本業務に使用するために本市から貸与されたドキュメントやシステム成果物などの情報資産については、従事者以外が閲覧できないように厳重に管理し、業務責任者は定期的に管理状況を確認して本市に報告すること。また、貸与された情報資産は本業務終了時に返却または廃棄すること。廃棄する場合には廃棄したことを証明するドキュメントを本市に提出すること。

10 委託元及び委託先の責任の明記

本業務の作業を受託者の保有する環境で実施する際には、受託者の責任においてセキュリティ対策を行ったうえで作業を実施すること。

11 再委託に関する事項

本業務において再委託は原則禁止であるが、業務の一部を合理的な理由及び必要性により再委託する場合には、セキュリティ対策が確認できる資料を提出し、本市の承認を受けること。また、受託者は、再委託先の行為について一切の責任を負うものとする。

令和 年 月 日

様

(届出者)  
住 所  
会社・所属

### セキュリティ保全申出書

受託業務の履行にあたっては、貴市の情報資産の漏洩、紛失、滅失、毀損、盗難等を防止するため、貴市の指示に基づき、下記のとおり、セキュリティ保全のための対策を実施いたします。

記

受託業務名	
受託期間	令和 年 月 日 ~ 令和 年 月 日
情報セキュリティ 対策責任者	
セキュリティ保全のための対策	
1 情報セキュリティを確保するための体制の整備 ・	
2 取り扱う情報資産の秘密保持等 ・	
3 運用・保守・点検における情報セキュリティ対策の実施 ・	
4 外部委託する業務以外の情報資産の保全 ・	
5 情報セキュリティインシデントが発生した場合の対処 ・	
6 情報セキュリティ対策の履行状況の報告 ・	

7 情報セキュリティ監査の実施

・

8 情報セキュリティ対策の履行が不十分であると思われる場合の対処

・

9 委託元及び委託先の責任の明記

・

10 再委託に関する事項

・

11 ドキュメントの管理

・

12 個人情報等の取扱い並びにセキュリティ教育の実施

・

以上

令和 年 月 日

様

(情報セキュリティ対策責任者)

会社・所属

氏 名

## セキュリティ保全状況報告書

当該業務において、「セキュリティ保全申出書」に基づき、セキュリティ対策を適切に実施しています。また、前回報告書（初回の場合は上記文書）からの変更有無等について、以下のとおり報告いたします。

### 記

受託業務名	
受託期間	令和 年 月 日 ~ 令和 年 月 日
報告対象期間	令和 年 月 日 ~ 令和 年 月 日
セキュリティ保全のための対策	
1	情報セキュリティを確保するための体制の整備 【変更なし/変更あり】 《変更内容》
2	取り扱う情報資産の秘密保持等 【変更なし/変更あり】 《変更内容》
3	運用・保守・点検における情報セキュリティ対策の実施 【変更なし/変更あり】 《変更内容》
4	外部委託する業務以外の情報資産の保全 【変更なし/変更あり】 《変更内容》
5	情報セキュリティインシデントが発生した場合の対処 【変更なし/変更あり】 《変更内容》

以上