

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こと。

記

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
本業務の作業実施体制・連絡体制を提示すること。
2. 取り扱う情報資産の秘密保持等
本業務の遂行にあたり知り得た全ての情報は、履行期間及び履行後において本業務の目的以外に使用もしくは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、秘密保持及びデータの取扱について、従業員その他関係者への徹底を行うこと。
3. 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。
4. 情報セキュリティ対策の履行状況の報告
受託者は、定期的に前項までの各項目の履行状況を本市へ報告することとし、本市が行う情報資産の管理に関する履行確認に対して適切に応じ、確認事項についての説明を行うこと。
5. 情報セキュリティ監査の実施
本市の要請等に基づき、サービス提供者のセキュリティ対策、運用体制等に関し、監査を行うことができる。
6. 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うえで、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。
7. 委託業務終了時の情報資産の返還、廃棄等
受託者は、業務の完了日又は契約解除の日をもって、情報資産を受託者に廃棄するとともに、その複製複写物を一切保持してはならない。ただし、本市が必要と認めるときは、その廃棄日を延期することができる。
8. 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。
9. 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の一切に責任を追うものとする。