

情報セキュリティ対策に関する特記事項

(総則・遵守義務)

第1条 乙は、本業務の遂行にあたり、甲が定める「浦添市情報セキュリティ基本方針」及び「浦添市情報セキュリティ対策基準」を遵守し、情報資産の機密性、完全性及び可用性を維持しなければならない。

(サービスレベルの保証)

第2条 乙は、本業務において甲が求めるセキュリティ要件及び業務品質を保証しなければならない。

(情報のライフサイクル全般における管理)

第3条 乙は、甲がアクセスを許可する情報の種類と範囲、及びアクセス方法を遵守し、情報の作成、入手、利用、保管、送信、運搬、提供、公表及び廃棄等に至るライフサイクル全般において、適切な管理を実施しなければならない。

(秘密保持及び目的外利用の禁止)

第4条 乙は、本業務を通じて知り得た情報を、甲の承諾なく第三者に漏らしてはならない。本業務終了後、又は乙の従業員が退職した後も同様とする。

2 乙は、甲より提供された情報を、本業務の目的以外に使用してはならない。

(再委託の制限)

第5条 乙は、本業務を第三者に再委託してはならない。ただし、あらかじめ甲の書面による承認を得た場合はこの限りではない。この場合、乙は再委託先に対しても本条項と同等の義務を負わせ、その履行について一切の責任を負うものとする。

(従事者の特定及び教育)

第6条 乙は、本業務に従事する責任者及び作業者を特定し、甲に報告しなければならない。

2 乙は、本業務に従事する者に対し、情報セキュリティ対策に関する教育を定期的実施し、その実施状況を甲に報告しなければならない。

(情報資産の管理及び持ち出しの禁止)

第7条 乙は、甲から提供された情報資産を、甲が指定する場所以外に持ち出してはならない。

2 乙は、業務上やむを得ず情報資産を外部へ持ち出す、又は外部で情報処理を行う場合は、あらかじめ甲の許可を得た上で、パスワード設定や暗号化等の安全管理措置を講じなければならない。

(インシデント発生時の報告・公表)

第8条 乙は、本業務に関連して情報漏えい等のセキュリティインシデントが発生し、又はそのおそれを認知したときは、直ちに甲に報告し、被害拡大防止等の指示に従わなければならない。また、甲が必要と認めた場合、事案の内容を公表できるものとする。

(監査及び点検)

第9条 甲は、必要があると認めるときは、乙における情報資産の管理状況について、実地調査又は監査を行うことができる。乙はこれに協力しなければならない。

(業務終了時の措置)

第10条 乙は、本業務が終了したときは、甲から提供された情報資産(複製物を含む)を速やかに甲に返還し、又は甲の指示する方法により確実に廃棄・抹消しなければならない。また、乙はその完了を証明する書面を甲に提出するものとする。

(損害賠償)

第11条 乙が本条項に違反し、甲又は第三者に損害を与えた場合、乙はその損害を賠償する責任を負う。