（委託事業者用）

渋谷区情報セキュリティポリシー遵守事項

1. セキュリティポリシーの遵守・秘密保持

①「遵守義務」：渋谷区情報セキュリティポリシー及びこれに基づく実施手順における各自の役割を理解し、遵守しなければならない。

②「秘密保持義務」：業務に従事している期間及び業務に従事しなくなった後も、業務上知り得た情報等を外部の第三者へ漏らしてはならない。

③「法令遵守義務」：業務の遂行に必要な法令を遵守しなければならない。

2. 情報資産の管理

①「目的外利用の禁止」：提供された情報の提示目的以外の利用及び受託者以外の者への提供をしてはならない。

②「複写・複製の禁止」：提供された情報を複写及び複製をしてはならない。

③「返還義務」：提供された情報は、契約終了時に全て返還、廃棄又は抹消しなければならない。また、その方法については、事前に区と合意した方法で実施しなければならない。

④「報告義務」：廃棄又は抹消した情報資産は、日時、方法、担当者を記録し、区に報告しなければならない。

⑤「持ち出しの禁止・制限」：業務上の理由なく情報資産を庁舎外に持ち出したり、転送してはならない。また、業務上の理由で庁舎外に情報資産を持ち出すときは、情報セキュリティ管理者の承認を得なければならない。

⑥「情報資産の受け渡し」：情報資産の受け渡しは必要最小限とし、安全な方法によらなければならない。

⑦区の情報システムやパソコン等を使用して保守作業等を行う場合は、機器等の内部に保管されている情報に対して、不必要なアクセス・複製・複写を行ったり、知り得た秘密を外部の第三者に漏らしてはならない。

⑧業務責任者、作業者及び情報管理の責任者を明確にしなければならない。

3　受託業務の実施

①「報告義務」：作業状況を適時報告しなければならない。

②「検査に応ずる義務」：作業内容について検査を求められた場合は、これに応じなければならい。

③「事故報告義務」：事故が発生した場合は、直ちに報告し、指示を受けなければならない。

④「協力義務」：セキュリティ実施手順を運用していく役割を持つ各管理者、担当者および組織の指示に従い、協力しなければならない。

⑤「入退室管理」：入退室管理が行われている庁舎内の管理区域に情報セキュリティ管理責任者の許可なく立ち入ってはならない。

4.1 情報システム等の使用（受託事業者等の社員等が区の情報システムを操作する場合）

①　許可なくパソコンや通信機器を全庁ネットワークその他区のネットワークに接続してはならない。

②　許可なくパソコン等への機器の増設又は改造を行ってはならない。

③　情報セキュリティ管理者より与えられたアクセス権限を遵守し、権限外の不正なアクセスを行ってはならない。

④　業務上の目的以外で情報システム等を使用してはならない。

⑤　許可なくソフトウェアをインストールしてはならない

⑥　ネットワーク監視ソフトウェアやハッキングソフトウェアの使用は絶対に行ってはならない。

⑦　セキュリティ上の事故、システムの欠陥及び誤動作を発見した場合は、直ちに情報セキュリティ管理に報告し、指示を仰がなければならない。

⑧　外部から入手した記録媒体・ダウンロードファイルを使用する場合は、事前にマルウェア等不正プログラムのチェックを行わなければならない。

⑨　ネットワークに接続する場合、不正プログラム対策ソフトを常時起動し、不正プログラム対策ソフトウェアのバージョンを常に最新に更新しておかなければならない。また、パターンファイル方式の場合は、最新のパターンファイルに更新されるよう設定しておかなければならない。

4.2 情報システム等の使用（情報システムの開発・構築をする場合）

①　情報システム等の開発工程において、区の意図しない変更を行ってはならない。また、一貫した品質保証体制の下で管理がなされていることを書類等で確認できるようにしておかなければならない。

②　情報システム等に意図しない変更が行われるなどの不正が見付かったときに、その原因を調査・排除するための体制を整備しておかなければならない。また、その体制が書類等で確認できるようにしておかなければならない。

③　ソフトウェアの作成及び試験を行う情報システムについては、運用中の情報システムと分離して実施しなければならない。

④ 情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、実施した試験の記録を保存すること。

⑤ ソースコードが不正に変更・消去されないよう適切に管理しなければならない。

⑥ 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

⑦ セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施し、区に報告すること。

4.3 情報システム等の使用（情報システムの運用・保守をする場合）

① 情報システムのセキュリティ監視を行う場合は、監視手順について区の合意を得なければならない。

② 運用中の情報システムに脆弱性が存在することが判明した場合は区に報告し、区が対処を求めた場合は、これに従わなくてはならない。

③ソフトウェアのバージョン等、情報システム関連の情報を変更する場合は、速やかに区に報告しなければならない。

5　本事項は、受託事業者のみならず、本受託業務に従事する全ての社員等（区の承諾を得て行う場合の再委託先社員、臨時社員、派遣社員等を含む。）に適用する。

6　上記の各項目のいずれかに違反した場合、契約条項に基づく損害賠償及び渋谷区情報セキュリティポリシーに定められる措置を受ける場合があること。

7　本事項は、受託業務実施期間中および業務終了後も有効であること。