

函館市電子計算機処理に係る保有個人情報等の管理に関する要領
(目的)

第1条 この要領は、別に定めるもののほか、電子計算機処理に係る保有個人情報等の管理に関し必要な事項を定めるものとする。

(定義)

第2条 この要領における用語の定義は、函館市電子計算機処理に係るデータ保護管理規程（平成元年函館市訓令第1号）の例による。

(アクセス制御)

第3条 電子計算機設置課の長は、保有個人情報等の秘匿性等その内容に応じて、パスワード等（パスワード、ICカード、生体情報等を用いる。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講じなければならない。

2 電子計算機設置課の長は、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備するとともに、パスワード等の読取防止等を行うために必要な措置を講じなければならない。

(アクセス記録)

第4条 電子計算機設置課の長は、保有個人情報等の秘匿性等その内容および必要に応じて、当該保有個人情報等へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存しなければならない。

2 端末管理責任者は、必要に応じてアクセス記録を分析するものとする。

3 電子計算機設置課の長は、アクセス記録の改ざん、窃取または不正な消去の防止のために必要な措置を講じなければならない。

(管理者権限の設定)

第5条 電子計算機設置課の長は、保有個人情報等の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化および内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講じなければならない。

(外部からの不正アクセスの防止)

第6条 電子計算機設置課の長は、保有個人情報等を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講じなければならない。

(不正プログラムによる漏えい等の防止)

第7条 電子計算機設置課の長は、不正プログラムによる保有個人情報等の漏えい、滅失または毀損等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置を講じなければならない。

(情報システムにおける保有個人情報等の処理)

第8条 職員は、保有個人情報等について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報をすみやかに消去するものとし、端末管理責任者は、当該保有個人情報等の秘匿性等その内容に応じて、随時、消去等の実施状況を確認するものとする。

(暗号化)

第9条 端末管理責任者は、保有個人情報等の秘匿性等その内容に応じて、暗号化のために必要な措置を講じるものとし、職員は、これを踏まえ、その処理する保有個人情報等について、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化を行うものとする。

(入力情報の照合等)

第10条 職員は、保有個人情報等の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報等の内容の確認等を行うものとする。

(バックアップ)

第11条 電子計算機設置課の長は、保有個人情報等の重要度に応じ、バックアップを作成し、分散保管するために必要な措置を講じなければならない。

(端末機の限定)

第12条 端末管理責任者は、保有個人情報等の秘匿性等その内容に応じ

て、その処理を行う端末機を限定しなければならない。

(端末機の盗難防止等)

第13条 端末管理責任者は、端末機の盗難または紛失の防止のため、端末機の固定、執務室の施錠等の必要な措置を講じなければならない。

2 職員は、端末管理責任者が必要であると認めるときを除き、端末機を外部へ持ち出し、または外部から持ち込んではならない。

(第三者の閲覧防止)

第14条 職員は、端末機の使用に当たっては、保有個人情報等が第三者に閲覧されることがないように、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講じなければならない。

(記録機能を有する機器・媒体の接続制限)

第15条 総務部情報システム課長は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等の漏えい、滅失または毀損等の防止のため、スマートフォン、USBメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限(当該機器の更新への対応を含む。)等の必要な措置を講ずるものとする。

附 則

この要領は、令和5年4月1日から施行する。