

一般社団法人しまね縁結びサポートセンター

個人情報保護に関する規程

1 目的

個人情報保護に関する指針第7の規定に基づき、個人情報を保護するために必要な事項について本規程のとおり定める。

2 組織的安全管理措置

① 組織体制の整備

○個人情報の保護に関する職員の役割・責任を次のとおり定める。

- ・センター長：個人情報保護安全管理責任者

関係法令や指針に定められた事項を理解し遵守するとともに、職員にこれを理解させ遵守させるための規程の整備、安全対策の実施、教育訓練、委託先への適切な監督等を実施する責任を負う。

- ・コーディネーター：個人情報取扱作業担当者

各センターにおける個人情報の取得、入力、利用、保管、消去等を行う。
パスワード認証によりシステムを利用する権限を有する。

- ・事務局次長：個人情報取扱作業責任者

個人情報が適正に取得、入力、利用、保管、消去等がされているかを確認する。

- ・事務スタッフ：個人情報システム運用管理者

システムに関する問題等が生じた場合、システム保守管理会社との連絡調整を行う。

② 指針等に従った運用

○申込書を受理した個人情報取扱作業担当者が、所属するセンター事務室に設置された専用パソコンから個人情報をシステムに入力する。

個人情報取扱作業責任者は、個人情報が適正に入力されたかを確認する。

個人情報の追加、更新、削除等についても、これに準ずる。

○個人情報の保護を徹底するため、個人情報保護に関する研修実施状況・受講者一覧表を作成し、保管する。

③ 個人情報の安全管理措置の評価及び見直し

○センター長は、個人情報保護に関する規程に基づく安全管理措置が講じられているか、四半期毎に確認する。

また、必要に応じて、外部の専門家に安全管理措置の評価を依頼する。

○安全管理措置については、外部の専門家による指摘、個人情報に対する社会情勢の変化、技術の進歩等に応じ、必要な見直しを行う。

④ 事故等への対応

○事実調査を行い、影響範囲を特定し、影響を受ける可能性のある本人等へ報

告するとともに、原因を究明し、再発防止策等の措置を講じる。

○個人情報の漏洩等の事故が発生した場合、または発生する恐れがあると判断した場合のセンター長への報告連絡体制については、別に定める。

3 人的安全管理措置

①雇用契約時及び委託契約時における非開示の義務付け

○職員の採用時において、雇用契約終了後も有効とする非開示規定を設ける。

○システム保守管理会社との委託契約時において、委託契約終了後も有効とする非開示条項を設ける。

②職員に対する教育訓練の実施

○職員に対して、個人情報保護に関する規程の周知を図る。

安全管理に関するそれぞれの役割と責任について、職員の採用時に適切な教育訓練を実施するとともに、必要に応じ教育訓練を行う。

4 物理的安全管理措置

①センター事務室の適切な管理

○個人情報を取り扱うセンター事務室は、センターの職員及びシステム保守管理会社社員以外の立ち入りを極力制限するとともに、職員は、個人情報が掲載されている書類を机の中に保管する等、職員以外の者が容易に見ることができないようにするものとする。

縁結びボランティア「はぴこ」、縁結び応援団、会員団体等との打合わせを行う場合は、センター応接テーブル又はセンター以外の場所を使用する。

②盗難等の防止

○個人情報を取り扱うパソコン、サーバー及び個人情報を記した書類を保管するキャビネットは、センター事務室の入り口から可能な限り遠ざけ、個人情報取扱作業責任者の席に近接する場所に設置する。

○入会申込書及び本人等確認書類のコピーは、入会受付後速やかにファイルへ綴り、施錠できるキャビネットに保管する。相談記録等入会後の状況を記録した書類についても、同様とする。

○最終退出者は、キャビネットの施錠、センターの施錠を確認し、定められた方法でカギを保管する。

○パソコンから個人情報を外部に持ち出しできないよう USB メモリ等外部記録媒体の接続は、センター長が指示した場合を除き行わないことを徹底するとともに、個人情報は持ち運びできないようにしたサーバーのみで保管し、パソコンに残らないようにする。

○原則として個人情報を記した書類について、コピーや FAX を行わないとともに、センター事務室の外へ持ち出さないことを徹底する。

○離席時には、個人情報を記した書類等を机上等へ放置しないことを徹底する。

5 技術的安全管理措置

①システムへのアクセスにおける識別と認証

○正当なアクセスであることを確認するため、アクセス権限を有する個人情報取扱作業員本人であることをパスワードにより識別、認証する。

②個人情報へのアクセス制御

○アクセス権限を付与する職員は、個人情報取扱作業員に限定する。

○システムを利用できるパソコンは、外部環境と遮断した松江センター2台、浜田センター1台のパソコンに限定する。

○センターの業務時間外は、システムにアクセスできないようにする。

③個人情報へのアクセスの記録

○システムへのアクセスの成功と失敗を記録し、これを適切に保管する。

④システムにおける不正ソフトウェア対策

○ウィルス対策ソフトウェアを導入し、セキュリティパッチを適用するほか、こうした対策の有効性や安定性が確認できるようにする。

⑤システムの動作確認時の対策

○動作確認時のテストデータとして個人情報を利用することを禁止する。

○システムの変更時に、セキュリティが損なわれないことを検証する。

⑥システムの監視

○システムの仕様状況や個人情報へのアクセス状況を定期的に監視する。

6 規程の改廃・委任

この規程の実施に関して必要な事項は、理事長が別に定める。

附則

この規程は、平成28年4月1日から施行する。