

西荻地域区民センター協議会 情報セキュリティポリシー

1. 目的

協議会情報セキュリティポリシー(以下「情報セキュリティポリシー」という)は、西荻地域区民センター協議会(以下「協議会」という)の管理する情報資産を適切に保護するために実施すべき情報セキュリティ対策について定めることを目的とします。

2. 情報セキュリティ対策の管理責任者

協議会の情報セキュリティ対策に関する管理責任者は会長とします。ただし、会長は管理責任者の役割の一部を協議会の事務局長に行わせることができるものとします。

3. 情報セキュリティに関する対策

協議会は、物理的、人的、技術的な面から、以下の情報セキュリティ対策を講じます。

(1) 物理的セキュリティ

① 個人情報等の適切な管理

協議会は、個人情報等の紛失、破壊、改ざん及び漏えい等を防止するため、個人情報等を含む紙媒体及び記録媒体(以下「個人情報等を含む媒体」という)は、施錠できる書庫等に保管します。

② 個人情報等を保管する書庫等の管理

協議会は、個人情報等を含む媒体を保管する書庫等について、第三者が容易に入室できない執務室内等に設置します。

③ 業務及び活動で、利用するパソコン等の管理

協議会は、業務及び活動で利用するパソコン、タブレット端末等(以下「パソコン等」という。)について、ワイヤーによる固定、施錠できる書庫等での保管等、盗難防止のための物理的措置を講じます。

④ ログインパスワードの設定

協議会は、個人情報への不正アクセスを防止するため、パソコン等について、ログインパスワードの入力を必要とするように設定します。

⑤ 記録媒体のパソコン等への接続

協議会は、パソコン等へ接続するUSBメモリ等の記録媒体をあらかじめ管理責任者の許可したものに限り使用することとします。

⑥ インターネット回線の通信ケーブルの配線

協議会は、個人情報の改ざん及び漏えい等を防止するため、インターネット回線に接続するための通信ケーブルは、床下配線又は執務室内への敷設等、第三者が容易に触れることができないようにします。

(2) 人的セキュリティ

① 情報セキュリティポリシー等の掲示等

協議会は、情報セキュリティポリシー及び別に定める協議会情報セキュリティ

実施手順を協議会委員及び協議会事務局職員(以下「協議会委員等」という)が常に閲覧できるように掲示等します。

② 情報セキュリティの研修

協議会は、協議会委員等に対し情報セキュリティについて十分理解して運用できるように必要な知識を習得するための研修を年1回行います。

③ 業務及び活動以外の目的での使用禁止

協議会委員等は、業務及び活動以外の目的で個人情報等を含む媒体の外部への持ち出し、協議会のメールアドレスの使用及びパソコン等からのインターネットへのアクセスを行いません。

④ 持ち出しの記録

協議会は、協議会委員等が業務のために個人情報等を含む媒体を地域区民センター外に持ち出す場合には、記録を作成し保管します。

⑤ ログインパスワードの管理

協議会委員等は、自己の管理するログインパスワードについて、協議会外部の者に知られないように管理します。

⑥ 退会時等の遵守事項

協議会委員等は、退会等により業務及び活動を離れる場合には、利用していた情報資産を廃棄又は返却します。

(3) 技術的セキュリティ

① コンピュータウイルス等の不正プログラムへの対策

協議会は、コンピュータウイルス等の不正プログラムへの対策として、パソコン等に不正プログラム対策ソフトウェアを導入し、パターンファイルを常に最新の状態に保つものとします。

② ソフトウェアのインストールの事前承認

協議会委員等は、パソコン等にソフトウェアをインストールする場合は、事前に管理責任者の承認を得ることとします。

③ 個人情報の暗号化

協議会は、講座等の応募者にホームページ上に個人情報を入力していただく場合には、通信に際して情報の暗号化を行います。

4. 情報セキュリティポリシー及び関係規程等の見直し

協議会は、情報セキュリティポリシー及び関係規程等について、有効かつ適正な運用が持続的になされるよう継続的な見直しと改善を図ります。