公益財団法人世田谷区スポーツ振興財団安全対策基準

改正令和元年６月１日

公益財団法人世田谷区スポーツ振興財団安全対策基準（平成１８年５月３０日）の全部を改正する。

この基準は、公益財団法人世田谷区スポーツ振興財団個人情報保護規程（以下「規程」という。）第５条第１項第３号オに定める個人情報保護マネジメントシステムを実現する文書の一部とし、公益財団法人世田谷区スポーツ振興財団個人情報保護施行規則（以下「規則」という。）第５条第１項第３号ウに規定された安全対策は、この基準による。

（目的）

第１条　本基準は、当財団における情報資産の管理におけるリスク（情報資産への不正アクセス、紛失、破壊、改ざんおよび漏洩）を低減し、情報資産を確実に保護するための安全対策を規定するものである。本基準は、当財団の全職員（正規職員、契約職員、派遣職員、非常勤職員、パート、アルバイト、嘱託、役員、評議員、顧問等も含む）の行う業務に適用する。

（安全管理の組織体制）

第２条　安全対策の責任は、個人情報保護管理者とする。

（入退室の安全対策）

第３条　不審者の侵入による個人データの盗難、破壊、改ざんのリスクを低減する為に、当財団の施設への入退室の許可は、当財団に勤務する全職員のみとする。また、特定個人情報取扱区域においては、事務取扱担当者及び特定個人情報保護管理者のみが作業可能とする。

（安全管理）

第４条　物理的アクセス管理、論理的アクセス管理／ネットワーク管理、サーバー／端末管理、情報システムの利用においては、本条第１項第１号から第８号に定めるリスク対策を周知徹底すること。

（１）施設全体について

個人情報の取扱い内容	リスク対策
不審者侵入対策	・身分および用件を確認のうえ、不審者と判断した場合は、早急に退出させる。
入退室管理	・一番初めに事務所内へ入室する職員と、一番後に事務所内を退出する職員は「入退室チェックリスト」に従って内容を記入する。 ・個人情報保護管理者は、3 か月に 1 度、「日常点検チェックシート」を使用して、きちんと記録が取られているか確認する。
受付からの視界・来訪者動線	・受付等で身元および用件を確認の上で入室を許可し、当財団職員が同伴する。

［使用する様式］

「入退室チェックリスト」

「日常点検チェックシート」

（２）取得・入力について

個人情報の取扱い内容	リスク対策

本人からの手渡し	・一時保管する際は、安全な保管場所を定める。 ・同意を得る仕組みを整える。
宅配便等で取得する	・一時保管する際は、安全な保管場所を定める。 ・郵便受けの施錠管理を行う。 ・宅配者が事務所内に入室する場合には職員が同行する。 ・宅配業者が入れる領域を定める。
FAX で取得する	・受信した FAX を放置せず、担当者を定めて速やかに回収する。
電話で取得する	・使用した電話メモは確実に廃棄又は保管する。 ・重要な情報は復唱する。 ・聞き取った内容を記録する。 ・通話時に本人へ通知する。 ・通話録音の利用目的を本人へ通知する。
取得した情報を、紙媒体へ記入する	・記入後入念な確認を行う。
電子メールで取得する	・添付ファイルにパスワードを設定する。 ・離席時はスクリーンセーバーの起動、またはログオフを行う。 ・メールの保管期間を定める。
WEB サイトを経由して取得する	・WEB サーバ間で暗号化をする。 ・SQL インジェクション対策、クロスサイトスクリプティング対策が取れているか確認する。 ・離席時はスクリーンセーバーを起動、またはログオフする。 ・送信前の同意確認ボタンの設置をする。
取得した情報を情報システムへ入力する	・入力後入念な確認を行う。
紙媒体を PDF 化する	・スキャンした書類は放置せず、速やかに回収する。 ・ウイルス対策ソフトを導入する。 ・サーバにアクセス制限をかける。
サーバから取得する	・添付ファイルにパスワードを設定する。 ・ウイルス対策ソフトの導入、Windows Update の設定/実行
データを印刷して取得する	・印刷後、速やかに回収する。

特定個人情報を取得する	・税・社会保障・災害対策の法令によって限定された範囲のみで利用する旨を明示する。 ・原本は取得しない。 ・取得時に「身元確認」と「番号確認」を行う。 ただし、雇用契約成立時等に本人であることの確認を行っており、知覚（対面で確認）することにより本人に相違ないことが明らかと判断できる場合には、身元確認のための書類提示の必要はなく、番号確認のみ行う。 【身元確認方法】 「運転免許証」、「パスポート」、「個人番号カード（表面）」等の顔写真付きの身分証明書または、「健康保険証」と「年金手帳」等 2 種類以上の書類の提示にて身元確認を行う。 【番号確認方法】 「通知カード」、「個人番号カード（裏面）」、「住民票（番号が記載されているもの）」等の提示にて番号確認を行う。
委託元、提供元にて取得する	・委託元、提供元から情報を取得するとき、適正な手段で取得しているかを確認する。

（3）移送・送信について

個人情報の取扱い内容	リスク対策
事務所内で持ち運ぶ	・放置しない。 ・入退室管理を行う。
職員が移送する	・肌身離さず携帯する。（置き忘れ、盗難などに注意する。なお、電車での移送の場合は、網棚へは置かず確実に移送する） ・外部記憶媒体にはパスワードを設定する。
配送業者を利用し、個人情報を郵送する	・宛先、封入物の入念な確認を行う。 ・発送記録を残す。
各自で所持し続ける（名刺など）	・移動中は不用意に取り出さない。
電子メールで送信する	・宛先と内容に間違いはないか十分に確認を行う。 ・添付ファイルにパスワードを設定する。 ・組織外の複数人へメールを送る場合、BCC を利用し他の方からアドレスを見えないようにする。
ネットワークを経由して送信する	・無線 LAN を暗号化する。 ・Web サーバに送信する個人情報を VPN や SSL などで暗号化する。
USB メモリなどの外部媒体を利用して送信する	・添付ファイルを暗号化する。 ・使用する外部媒体は財団貸与に限定し、ウイルスチェック等安全対策を行ったものを使用する。
FAX で送信する	・送信前に宛先、内容を確認する。 ・FAX 送信記録を確認する。 ・FAX 送信後、速やかに回収する。
授受の記録	・個人情報を記録した媒体を手渡ししたり、郵便、宅配便等で受け渡したりする時は、授受の記録を取得すること。
返却する	・返却時に返却先の確認を行う。

（4）利用・加工について

個人情報の取扱い内容	リスク対策
取得・入力後に個人情報を利用する	・利用目的を具体的に特定する。 ・職員へ教育を行い、個人情報保護に対する意識を高める ・事務所内のルールを職員に遵守させる。 ・重要な情報の編集後は入念な確認を行う。
閲覧する	・不要な書類はシュレッダーにかけるように教育する。 ・事務所内のルールを職員に遵守させる。
採用選考に用いる	・利用目的を具体的に特定する。
紙媒体に記録された情報を利用する	・利用場所を制限する。 ・入退室管理を行う。 ・利用者の制限をかける。
サーバやパソコンに格納された個人情報を利用する	・スクリーンセーバーの起動、またはログオフをする。 ・重要な情報の編集後は入念な確認を行う。 ・事務所内のルールを職員に遵守させる。 ・アクセス権限を設ける。
連絡する、閲覧する（携帯電話など）	・入念に確認してから電話をかける。 ・職員へ教育を行い、個人情報保護に対する認識を高める。
復元のために利用する（バックアップ）	・アクセス制限を設ける。
特定個人情報の利用	・税・社会保障・災害対策の法令によって限定された範囲のみで利用する。 ・特定個人情報を取扱う者は、特定個人情報保護管理者及び、特定個人情報保護管理者が指名した事務取扱担当者に限定する。 ・特定個人情報を取扱う場合は、周囲の者に見られないよう隔離された場所で作業を行う。

（5）委託・提供について

個人情報の取扱い内容	リスク対策
渡す時	・配達記録付郵便などを利用して必ず追跡のできる方法で送付すること。
受取る時	・個人情報の授受がある場合には、場所、双方の責任者、数量の把握・確認をする。
返却・廃棄	・委託先との覚書締結及び評価を行い、確実な運用を求める。
委託中	・委託先と個人情報保護に関する契約を締結する。 ・プライバシーポリシー、約款、利用規約等の確認を行う。 ・委託先の選定評価を行う。
第三者に提供する	・本人の同意を得て第三者に提供する手順を定める。 ・提供先が目的外利用しないことをプライバシーポリシー、約款、利用規約等で確認する。
特定個人情報を委託する	・委託先と特定個人情報の取扱いに関する契約書等を締結する。 ・プライバシーポリシー、約款、利用規約等を確認する。 ・委託先の選定評価を行う。
特定個人情報の提供禁止	・何人も、番号法で限定的に明記された場合を除き、特定個人情報を「提供」してはならない。

（6）保管・バックアップについて

個人情報の取扱い内容	リスク対策
キャビネットに保管する（紙媒体、外部記憶媒体など）	・媒体の保管場所を定めて施錠等の盗難防止策を講じる。 ・中が見えるキャビネット等に保管しない。
パソコンに個人情報を保管する。	・PC から長時間離れる際は電源を切る。 ・離席時には必ずログオフまたはスクリーンセーバーの起動を行う。 ・当財団が指定するウイルス対策ソフトを導入し、常時スキャンできるようにする。 ・アクセスログは定期的にチェックし、不正アクセス等に備える。 ・ノート PC は鍵付きのキャビネットへ保管する。
サーバや HDD に保管する。	・アクセス権限を設ける。 ・ウイルス対策ソフトを導入する。 ・見知らぬ人からの添付ファイルを開封しない。 ・データをバックアップする。 ・ID、パスワードを設定する。
クラウドサーバに保管する	・ID、パスワードにより管理する。 ・アクセス権限を設ける。 ・職員へ教育を行い、個人情報保護に対する認識を高める。 ・委託先と個人情報保護に関する契約を締結する。 ・プライバシーポリシー、約款、利用規約等を確認する。 ・委託先の選定評価を行う。 ・家族と共用している PC を使用するときは、必ず PC に安全対策（ウイルス対策ソフトの導入や Windows Update の設定/実行）が取られているか確認する。 ・自宅及び組織外でクラウドサービスのファイルサーバを利用するとき、他人に見られるような場所での作業は禁止とする。 ・個人情報を含んでいるファイルにはパスワードをかける。
外部媒体に保管する	・添付ファイルを暗号化する。 ・事務所内のルールを職員に遵守させる。
媒体内に保管する（携帯電話、スマートフォン）	・パスワードロックにより管理する。 ・紛失発覚時は、キャリアに連絡し、遠隔ロックを行う。
バックアップを取る	・情報システム管理者が同一ネットワーク上のファイルサーバまたは DAT テープにバックアップを取る。 ・保管世代は、3 世代前までの保管を行う。
特定個人情報を保管する	・特定個人情報保護管理者及び事務取扱担当者以外アクセスできないよう措置を講じる。

（7）廃棄・消去について

個人情報の取扱い内容	リスク対策
紙媒体を廃棄する。	・保管期間を定めて確認の上廃棄する。 ・シュレッダーにて廃棄する。
溶解処理業者に委託して廃棄する	・立会いをする。 ・重要な情報は破棄証明を取得する。
事務所内のサーバに格納された個人情報を消去する	・物理的に破壊する。 ・業者に依頼し、消去してもらう。
組織外のサーバやクラウドに格納された個人情報を消去する	・重要な情報は廃棄証明を取得する。 ・バックアップを取っておく。 ・委託先と個人情報保護に関する契約を締結する。 ・プライバシーポリシー、約款、利用規約等を確認する。 ・委託先の選定評価を行う。
外部記録媒体の廃棄	・保管期間を定めて確認の上廃棄する。 ・物理的に破壊する。 ・重要な情報は廃棄証明を取得する。 ・CD、DVD、USB メモリ等の外部記録媒体の廃棄は、データ削除の上、物理破壊する。
リース機器の返還	・ハードディスクのデータを完全に消去した後、返却する。 ・データ消去の証明書を発行してもらい、データが確実に消されていることを確認する。 ・重要な情報は廃棄証明を取得する。 ・委託先と個人情報保護に関する契約を締結する。 ・プライバシーポリシー、約款、利用規約等を確認する。 ・委託先の選定評価を行う。
PC に格納された個人情報を消去する	・保管期間を定めて確認の上廃棄する。 ・物理的に破壊する。 ・重要な情報は廃棄証明を取得する。
特定個人情報を廃棄する	・社会保障及び税に関する手続書類の作成事務を処理する必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、特定個人情報をできるだけ速やかに廃棄又は削除する。

（8）情報システムについて

次のネットワーク及びコンピュータ・システムを対象とする。

ア）事務所内 LAN に接続された、汎用的なパソコン及びソフトウエアと運用

イ）組織外サーバを利用する場合インターネット及び電子メールの運用

ウ）単独で稼動する汎用的なパソコン及びサーバのソフトウエアと運用

個人情報の取扱い内容	リスク対策
物理的環境	・ワイヤーロックでの固定、床への固定などよる、盗難・地震対策を施すこと。
盗難・破壊・破損などの安全管理上の脅威、及び漏水、火災・停電・地震などの環境上のため対策	・スプリンクラー、給湯施設などの位置を考慮し、防水対策を施すこと。 ・消火器の設置、防炎資材の導入などによる防火対策を施すこと。 ・無停電装置等の設置により、停電対策を必要であれば施すこと。
外部記憶媒体の持ち出し・持ち込み（FD、USB メモリ、CD 等）	・自己で購入したパソコン、USB メモリ等機器の持ち出し・持ち込みは禁止とする。 ・個人情報保護管理者の許可を得た場合を除き、外部記憶媒体をパソコン等の機器に接続してはならない。 ・財団貸与のものを使用し、業務終了後には鍵付きキャビネットに保管する。
ノート PC の利用・持ち込み持ち出し	・個人情報が保存されたパソコン、記憶媒体などは、原則組織外への持ち出しは禁止とする。 ・個人のノートパソコンは持込を禁止する。 ・ノート PC を使わない時は、盗難防止策として施錠保管する。
アクセス権、ID・パスワード	・ID は個人情報保護管理者が発行・更新・廃棄の管理を行う。 ・組織の変更または退職等により、情報を使用しなくなったユーザーのアクセス権は直ちに抹消する。 ・各パソコンに、ログインのためのパスワードを設定する。 ・パスワードは英数含む 6 桁以上とし、英数混合で各自が設定する。 ・パスワードは 6 か月に 1 度の頻度で更新を行う。 ・パスワードを設定の際には前回設定したパスワードの再利用や類似したパスワードを利用してはならない ・複数のサービスで同一のパスワードを使いまわしてはならない。 ・ID とパスワードは本人のみが使用し、他人に貸与してはならない。 ・ID とパスワードを付箋に記載して貼り付けるなど、目に触れる位置に記載してはならない。 ・ID とパスワードが他人に知られた場合は、速やかに ID とパスワードを再設定する。

個人情報の取扱い内容	リスク対策
ウイルス対策	・事務所内で指定されたウイルス対策ソフトをインストールし、常駐設定（リアルタイム監視状態）にする。 ・OS の自動アップデート機能を有効にし、最新の修正ソフトが適用されるようにする。 ・ウイルス対策ソフトは自動アップデート機能を有効にし、常に最新バージョンに更新されるよう設定する。 ・ウイルスなどに侵された可能性のある場合は、速やかにネットワークケーブルを抜き個人情報保護管理者へ報告すること。その際 PC には一切手を触れはならない。
セキュリティパッチ	・パソコンおよびサーバへのセキュリティパッチを定期的に適用する。
スクリーンセーバー	・スクリーンセーバーの設定は 15 分以内とする。 ・個人情報保護管理者は、3 か月に 1 度、「日常点検チェックシート」を使用して、きちんと設定されているか確認する。
ソフトのインストール	・フリーソフトなどのダウンロードおよびインストールを行ってはならない。ただし、業務上必要な圧縮解凍ソフト、アクロバットリーダーなどのソフトはこの限りではない。その他、ダウンロードの必要がある場合、個人情報保護管理者に相談の上、指示を仰ぐこと。 ・Winny 等のファイル共有ソフトはいかなる場合もインストール、使用してはならない。
アクセスログ	・システム担当者は月 1 度、イベントログの確認を行う。ログインの失敗、勤務時間外のログイン、外部からの不正アクセスがあれば、速やかに情報システム管理者に報告し、指示を仰ぎ、詳細に調べることとする。
WEB サイトの閲覧	・インターネットを利用する場合、業務に関係の無いサイトへアクセスしてはならない。 ・掲示板、ブログなどに個人情報および個人情報に結びつく情報を記述してはならない。
WEB ページの暗号化	・少なくとも個人情報を送信するページ（問合せページ等）には、SSL など、暗号化を施す。
リモートアクセス制限	・ID、パスワードを設定し、権限のあるものしか利用できないよう設定する。 ・VPN 接続を利用する。その際、ID を個人情報保護管理者が設定する。 ・職員は自宅及び個人のルーター及び無線 LAN に固定ルートを設定し、固定のルーター及び無線 LAN からしか接続ができないよう設定をする。

個人情報の取扱い内容	リスク対策
無線 LAN	・無線 LAN の暗号化措置は WPA2 以上 SSID を設定する。
携帯電話の利用	・パスワードロックを設定する。 ・使用時には個人情報が周囲に聞こえないよう注意を払う。 ・登録された電話番号やメールアドレスが周囲に見えないよう注意を払う。 ・個人情報を外部媒体にコピーしない。 ・私的な電話番号やメールアドレスは登録しない。 ・紛失した場合は、速やかに個人情報保護管理者に報告し、遠隔操作ロックのサービス又は使用停止の手続きを行う。 ・携帯ショップに返却する際は、データの完全消去ならびに本体の破壊処理を依頼する。
スマートフォンおよびタブレットの利用	・私物のスマートフォンの持込、使用は可能とする。しかし、事務所内のパソコンに USB ケーブルにて接続し、充電やアクセスすることを禁止する。 ・私物のスマートフォン内に業務に関わる情報は入れない。 ・財団用のスマートフォンおよびタブレットには、安全性の低いアプリケーションのインストールを禁止する。 ・パスワードロック又はパターンロックを設定する。 ・使用時には個人情報が周囲に聞こえないよう注意を払う。 ・登録された電話番号やメールアドレスが周囲に見えないよう注意を払う。 ・個人情報を外部媒体にコピーしない。 ・私的な電話番号やメールアドレスは登録しない。 ・紛失した場合は、速やかに個人情報保護管理者に報告し、遠隔操作ロックのサービス又は使用停止の手続きを行う。 ・携帯ショップに返却する際は、データの完全消去ならびに本体の破壊処理を依頼する。

附則

この基準は令和元年６月１日から施行する。