

個人情報保護規程

社会福祉法人赤間福祉会

赤間保育園

第二赤間保育園

個人情報保護規程

第1章 総則

(目的)

第1条 この規程は、「個人情報の保護に関する法律」(以下「個人情報保護法」という。)その他の法令等にもとづき、社会福祉法人 赤間福祉会(以下、当法人という。)が取り扱う個人情報について適正な管理を行うことにより、個人の人格を尊重し、その権利および利益を保護することを目的とする。

なお、「行政手続における特定の個人を識別するための番号の利用等に関する法律」にもとづく個人番号やその内容を含む個人情報に関しては「特定個人情報取扱規程」において、別途定めるところに従うものとする。

(定義)

第2条 この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる以外は、個人情報保護法第2条各号または第16条各号に定める意味を有する。

(1)「個人情報」とは、生存する個人に関する情報であつて、次のいずれかに該当するものをいう。

① 当該情報に含まれる氏名、生年月日その他の記述等(文書、図画もしくは電磁的記録(電磁的方式(電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。)で作られる記録をいう。)に記載され、もしくは記録され、または音声、動作その他の方法を用いて表された一切の事項(個人識別符号を除く。)をいう。以下同じ。)により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)

② 個人情報保護法2条2項で規定する個人識別符号が含まれるもの

(2)「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして、個人情報保護法施行令第2条で定める記述等が含まれる個人情報をいう。

(3)「個人情報データベース等」とは、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した、個人情報を含む情報の集合物をいうほか、紙面で処理した個人情報を一定の規則に従って整理・分類し、目次、索引、符合等を付し容易に検索可能な状態においているものをいう。ただし、利用方法からみて個人の権利利益を害するおそれが少ないものとして次のいずれにも該当するものを除く。

① 不特定かつ多数の者に販売することを目的として発行されたものであつて、かつ、その発行が法または法にもとづく命令の規定に違反して行われたものでないこと

② 不特定かつ多数の者により随時に購入することができ、またはできたものであること

③ 生存する個人に関する他の情報を加えることなくその本来の用途に供しているものであること

(4)「個人データ」とは、個人情報データベース等を構成する個人情報をいう。

(5)「保有個人データ」とは、開示、内容の訂正、追加または削除、利用の停止、消去および第三者への提供の停止を行うことのできる権限を有する個人データであつて、以下に掲げるもの以外のものをいう。

① 当該個人データの存否が明らかになることにより、本人または第三者の生命、身体または財産に危害が及ぶおそれがあるもの

- ② 当該個人データの存否が明らかになることにより、違法または不当な行為を助長し、または誘発するおそれがあるもの
 - ③ 当該個人データの存否が明らかになることにより、国の安全が害されるおそれ、他国もしくは国際機関との信頼関係が損なわれるおそれまたは他国もしくは国際機関との交渉上不利益を被るおそれがあるもの
 - ④ 当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧または捜査その他の公共安全と秩序の維持に支障が及ぶおそれがあるもの
- (6) 「個人情報取扱業務」とは、当法人における個人情報の取得および個人データの保護管理に関する業務をいう。
- (7) 「本人」とは、個人情報によって識別される特定の個人をいう。
- (8) 「職員」とは、当法人の組織内において直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある職員(正職員、契約職員、嘱託職員、パート、アルバイト等)のみならず、理事、監事、派遣労働者等も含まれる。
- (9) 「個人情報管理責任者」とは、当法人の個人データの管理に関する責任を担う者をいう。
- (10) 「個人情報管理者(園責任者)」とは、各施設の個人データの管理に関する責任を負う者をいう。
- (11) 「事務取扱担当者」とは、当法人内において、個人番号を取り扱う事務に従事する者をいう。
- (12) 「管理区域」とは、個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域をいう。
- (13) 「取扱区域」とは、個人データを取り扱う事務を実施する区域をいう。
- (14) 「個人関連情報」とは、生存する個人に関する情報であって、個人情報、仮名加工情報および匿名加工情報のいずれにも該当しないものをいう。
- (15) 「個人情報保護法」とは、個人情報の保護に関する法律(平成 15 年法律第 57 号)をいう。
- (16) 「政令」とは、個人情報の保護に関する法律施行令(平成 15 年政令第 507 号)をいう。
- (17) 「規則」とは、個人情報保護に関する法律施行規則その他の個人情報保護委員会が定める規則をいう。
- (18) 「ガイドライン」とは、「個人情報の保護に関する法律についてのガイドライン(通則編/外国にある第三者への提供編/第三者提供時の確認・記録義務編/仮名加工情報・匿名加工情報編)」ならびに個人情報保護委員会その他の権限ある機関が策定するガイドラインを総称したものをいう。
- (19) 「法令等」とは、個人情報保護法、政令、規則およびガイドラインを総称していう。

第2章 安全管理措置

第1節 組織的安全管理措置

(個人情報管理責任者)

第3条 当法人における個人データの取扱いに関する責任部署は、赤間保育園(法人本部)とする。

2. 当法人に、個人情報管理責任者1名をおく。

3. 個人情報管理責任者は、理事長とする。

4. 個人情報管理者には、個人データを取り扱う各園の園長、副園長又は主任がその任にあたる。

(個人情報管理責任者の責務)

第4条 個人情報管理責任者は、個人情報取扱業務を統括するとともに、本規程に定められた事項を理解し、遵守するとともに、事務取扱担当者にこれを理解させ、遵守させるための教育訓練、安全対策の実施ならびに周知徹底等の措置を実施する責任を負う。

2. 個人情報管理責任者は、職務分掌等の関係規程の定めるところにより個人情報取扱業務を所掌する。
3. 個人情報管理者(園責任者)である各園の園長、副園長又は主任は、当該園における個人情報の取得および個人データを適切に管理する任にあたり、個人データの適切な管理のために必要な措置を講じ、個人データの安全確保に努める責任を負う。
4. 個人情報管理責任者は、法令遵守の観点から、各園の個人情報管理者(園責任者)に対して指導、助言する。

(事務取扱担当者等の監督)

第5条 個人情報管理責任者は、事務取扱担当者が個人データを取り扱うにあたり、必要かつ適切な監督を行うものとする。

2. 個人情報管理者は、自らの園に属する事務取扱担当者に対し、個人データの取扱いに関して必要かつ適切な監督を行わなければならない。
3. 個人情報管理責任者は、事務取扱担当者に対して個人情報の保護および適正な取扱いに関する誓約書の提出を命じることができる。

(事務取扱担当者の責務)

第6条 事務取扱担当者は、当法人の個人データの取扱いまたは委託処理等、個人データを取り扱う業務に従事する際、法令等、本規程およびその他の規程ならびに個人情報管理責任者の指示した事項に従い、個人データの保護に十分な注意を払ってその業務を行うものとする。

2. 事務取扱担当者は、個人情報の漏えい等、法令等、本規程またはその他の規程に違反している事実または兆候を把握した場合、速やかに各園の個人情報管理者(園責任者)または個人情報管理責任者に報告するものとする。各園の事務取扱担当者から、当該報告を受けた個人情報管理者(園責任者)は速やかに個人情報管理責任者に報告するものとする。

(本規程にもとづく運用状況の記録)

第7条 事務取扱担当者は、本規程にもとづく運用状況を確認するため、以下の項目については、必要に応じて、運用結果を記録するものとする。

- ① 個人データの取得および個人情報データベース等ファイルへの入力状況
- ② 個人情報データベース等の利用・出力状況の記録
- ③ 個人データが記載または記録された書類・媒体等の搬出等の状況
- ④ 個人情報データベース等の削除・廃棄記録
- ⑤ 削除・廃棄を委託した場合、これを証明する記録等

- ⑥ 個人情報データベース等を情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況(ログイン実績、アクセスログ等)

(取扱状況の確認手段)

第8条 事務取扱担当者は、個人情報データベース等の取扱状況を確認するための手段として、「個人情報管理台帳」に以下の事項を記録するものとする。

- ① 業務の名称
- ② 情報資産名(個人情報の名称)
- ③ 個人情報の内容
- ④ 利用目的
- ⑤ 取得方法または経路
- ⑥ 開示・非開示の区分
- ⑦ アクセス権者
- ⑧ 保管方法・保管場所・保管期限
- ⑨ 提供・委託先
- ⑩ 廃棄方法
- ⑪ アクセス権者

(情報漏えい等事案への対応)

第9条 個人データの漏えい、滅失またはき損(以下「漏えい等」という。)の事案の発生または兆候を把握した場合は、以下に定める手順により対応する。

<緊急事態の特定及び対応手順>

- (1) 個人情報が漏えい、滅失又はき損した場合、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とする手順
- (2) 個人情報の漏えい、滅失又はき損が発生した場合は、①～③の中で必要な処置を講じる。
 - ① 当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人の容易に知り得る状態に置く。
 - ② 二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表する。
 - ③ 事実関係、発生原因及び対応策を関係機関に直ちに報告する。
- (3) 緊急事態の特定 (実行開始条件)
 - ① 当法人に所属する全職員は、下記に示された緊急事態やそれに類似する緊急事態が発生した場合、又は発生の可能性が高いと判断した場合に、速やかに個人情報管理責任者に報告を行うものとする。
 - ② 個人情報管理責任者は、報告内容を判断したうえで、本手順の発動を決定する。
 - ③ 個人データの漏洩等についての情報は、外部からもたらされる場合もあるため、関連する業務に従事する要員の認識を確実にしておく。

(ア) 個人情報に直接関係する緊急事態の例

- ・ 個人情報漏洩事故。この場合、発見された場所は園内外を問わない
- ・ 個人情報の不正持ち出し
- ・ 個人情報の盗難
- ・ 配送中など外部での個人情報の滅失・き損
- ・ 大規模な個人情報の紛失・損傷

(イ) 情報システムに関する緊急事態の例

- ・ ウィルスの侵入によるシステムダウン
- ・ ハッキング／クラッキング行為によるシステムの乗っ取り
- ・ スパイウェア、フィッシング、ファーミング等不正な行為の存在発覚
- ・ 社内外の不適切な者による管理者権限の取得
- ・ ID／パスワードなどの流出
- ・ ネットワーク上の個人情報の破壊および改ざん行為
- ・ ノートPCの紛失または盗難

- ④ 次の(ア)から(エ)までに掲げる事態(以下、「報告対象事態」という。)を知ったときは、個人情報保護委員会に報告を要する事案として判断する。

(ア)要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態(規則第6条の2第1号関係)

(イ)不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態(規則第6条の2第2号関係)

(ウ)不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態(規則第6条の2第3号関係)

(エ)個人データに係る本人の数が1,000人を超える漏えい等が発生し、又は発生したおそれがある事態(規則第6条の2第4号関係)

(4)緊急事態の対応手順 (緊急対応責任者)

緊急事態が発生した場合、個人情報管理責任者が緊急対応責任者として指揮をとる。個人情報管理責任者が対応できない場合については、個人情報管理責任者は緊急対応責任者を任命することができる。この場合、緊急対応責任者が複数となって指揮命令系統の混乱を招かぬよう留意する。

(5)緊急事態の対応手順 (事実関係の把握)

- ① 緊急対応責任者は、冷静・沈着に情報を収集、分析し、事件の事実関係や問題の大きさ、影響範囲などをできる限り特定する。同時に個人情報管理責任者に適切に問題点を連絡し、必要に応じて個人情報管理責任者の判断を仰ぐ。
- ② 収集に必要な情報は以下のとおり。
 - ・個人情報の名称、内容、件数
 - ・個人情報の機微度合い
 - ・個人情報が漏洩・滅失又はき損した時期と経緯
 - ・当時の管理状況

- ・情報主体が被った被害状況、又は影響を及ぼす可能性のある内容
- ・通報の場合、通報者の連絡先などの確認。
- ・情報の信憑性
- ・外部委託先での発生の可能性
- ・故意、過失の区分 など

(6)緊急事態の対応手順（緊急対応策の決定と実施）

- ① 緊急対応責任者は、収集、分析した情報を元に、想定される経済的な不利益及び社会的な信用の失墜などの恐れを考慮し、以下の内容に関する緊急対策を検討し、決定する。必要に応じて委託元や各関係部署と協議上、緊急対策を決定する。
 - ② 緊急対策は、定常的な業務の遂行に優先して実施する。
- ・被害の拡大の防止
 - ・情報システムの問題で、外部への二次的被害をもたらす可能性がある場合には、システムの一部切り離しまたは停止措置によって、強制的に被害の拡大を防止する。
 - ・被害が利用者など外部の者に広範囲に及ぶ場合、“緊急対策会議”を招集する。この会議には理事長をはじめ、必要と判断した者であれば、部門、階層を問わず参加を指示する。
 - ・マスメディア等によって当法人の信用に影響が出る懸念がある場合には、理事長と協議し、対策を講じる
 - ・理事長は、必要に応じて、影響をうける可能性のある本人、利用者、監督官庁、所属団体等への連絡に関する立案および指示を行う。

(7)緊急事態の対応手順（緊急事態による影響を受ける可能性のある本人、及びその他への情報提供体制の整備）

- ① 緊急対応責任者は、緊急事態による影響を受ける可能性のある本人及びその他に対して行う情報提供の実施責任者を任命する。
- ② 実施責任者は当該漏洩、滅失又はき損が発生した個人情報の内容などを、次の手段のいずれか又は組み合わせにより、本人に速やかに通知し、又は本人が容易に知り得る状態に置く。
記者会見／新聞広告／ホームページ／書面（郵送、FAX、メール）／電話
- ③ 実施責任者は二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、次の手段のいずれか又は組み合わせにより遅滞なく公表する。
記者会見／新聞広告／ホームページ
- ④ 緊急対応責任者は、以下の関連組織に、事実関係、発生原因及び対応策などの報告が行われることを確実にするため、次の手順を運用する。
 - (ア)報告時期:いずれかの部署が当該事態を知った時点を基準として、速報としては速やかに(概ね 3～5 日以内)、その後の確報としては 30 日以内(規則第 6 条の 2 第 3 号の事態においては 60 日以内。同号の事態に加え、同条第 1 号、第 2 号又は第 4 号の事態にも該当する場合も 60 日以内)に対応する。
 - (イ)報告事項:個人情報保護委員会への漏えい等報告については、次の 1)から 9)までに掲げる事項を原則と

して、個人情報保護委員会のホームページの報告フォーム

(<https://www.ppc.go.jp/personalinfo/legal/leakAction/>)に入力する方法により行う。速報時点での報告内容は、報告をしようとする時点で把握している内容を、確報では全ての事項について報告する。ただし、速報の時点で全ての事項を報告できる場合には、1回の報告で速報と確報を兼ねることができる。

1) 「概要」

当該事態の概要について、発生日、発覚日、発生事案、発見者、規則第6条の2各号該当性、委託元及び委託先の有無、事実経過等を報告する。

2) 「漏えい等が発生し、又は発生したおそれがある個人データの項目」

漏えい等が発生し、又は発生したおそれがある個人データの項目について、媒体や種類(利用者情報、職員情報の別等)とともに報告する。

3) 「漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数」

漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数について報告する。

4) 「原因」

当該事態が発生した原因について、当該事態が発生した主体(報告者又は委託先)とともに報告する。

5) 「二次被害又はそのおそれの有無及びその内容」

当該事態に起因して発生する被害又はそのおそれの有無及びその内容について報告する。

6) 「本人への対応の実施状況」

当該事態を知った後、本人に対して行った措置(通知を含む。)の実施状況について報告する。

7) 「公表の実施状況」

当該事態に関する公表の実施状況について報告する。

8) 「再発防止のための措置」

漏えい等事案が再発することを防止するために講ずる措置について、実施済みの措置と今後実施予定の措置に分けて報告する。

9) 「その他参考となる事項」

上記の①から⑧までの事項を補完するため、個人情報保護委員会が当該事態を把握する上で参考となる事項を報告する。

(報告先)

- ・主務官庁(経済産業省・厚生労働省他)
- ・九州経済産業局【092-482-5405】
- ・宗像市役所【0940-36-1121】
- ・個人情報保護委員会 ※マイナンバー総合ダイヤル【0120-95-0178】

※事故報告サイト:<https://www.ppc.go.jp/personalinfo/legal/leakAction/>

⑤ なお、公表する情報については、以下の事項を含めることを配慮する

- ・事件の事実関係
- ・事件を発生させたことに対する謝罪の意
- ・事件の発生時期、発生経緯
- ・個人情報の内容や件数

- ・漏洩時に講じていた安全管理策
- ・本人への影響
- ・発生原因、今後の対応策（下記参照）

（正式決定された再発防止策の公表が遅れる場合は、その理由、公表の予定時期）

- ・影響を及ぼした個人情報に対する利用停止、変更手続
- ・本人への補償内容
- ・緊急問合せ窓口の通知

（本人に負担をかけさせないように、フリーダイアルの採用も考慮する。）

⑥ 本人や外部との対応においては、以下の事項に配慮する。

（ア）被害を被った本人の立場にたった気持ちで、真摯に対応する。

（言葉使い、迅速な対応などの心がけ、相手の言い分をしっかりと聞く 等）

（イ）推測、感想、意見等は述べない。

（ウ）問合せ、取材の対応窓口は一本化し、個別対応しない。

（エ）本人からの問合せや対応を記録する場合は、個人情報として管理する。

（オ）本人からの問合せに回答できない場合には、その理由または、折り返し連絡する際の“時期”、“担当者”、“連絡方法”を伝達する。

（カ）ホームページに公表する場合、トップページから1回程度の操作で到達できる場所への掲載を行う。

(8)原因の究明、再発防止策の策定と実施

- ① 緊急対応責任者は、速やかに緊急事態の発生原因の特定を行う。この発生原因の特定は根本となる原因にいきつくまで行う。また同時に、被害状況を正確に把握するため情報を収集する。
- ② 各園は緊急対応責任者の指示に従い、定常的な業務の遂行に優先して指示事項を実施する。
- ③ 緊急対応責任者は、特定された発生原因を基に再発防止対策の必要性を検討する。恒久対策を行わない限り被害の拡大を停止できない場合、緊急対応責任者は緊急対策会議を招集し、緊急対策会議にて恒久対策を検討する。
- ④ 既に上記(7)の対応により被害が拡大しない状況になっている(沈静化している)場合には、緊急対応責任者が発生原因と被害状況を元に、恒久対策の可否を判断し、必要となった場合には恒久対策を検討する。
- ⑤ 策定された恒久対策を実施する。

(9)対策の有効性の確認と記録の作成

- ① 個人情報管理責任者は、緊急対応のみで終了した緊急事態に対しては緊急対応の有効性を、恒久対策を実施した緊急事態に対しては、恒久対策の有効性の確認を実施する。
- ② 実施時期は、個人情報管理責任者が適切と判断した時期に実施する。
- ③ 個人情報管理責任者または緊急対応責任者は、緊急事態(不適合)内容、原因、是正処置、是正処置の効果について「是正処置報告書」として記録する。

(10)緊急事態からの学習

- ① 個人情報管理責任者は、発生した緊急事態に対して取り得る緊急対応の完了時点、または恒久対策の完了時点のいずれかにおいて、当法人内で情報を共有化する必要性の有無を判断する。
- ② 情報共有化が必要であると判断した場合、緊急に全員を招集し、緊急事態の内容・状況および対応によって学んだ点を職員に伝える。
- ③ 是正処置の結果、文書化された手順があれば、是正処置が有効かつ確実に継続されるように教育・訓練の計画に組み込む等の措置をとる。

(11)記録

管理策に関する運用記録は、記録として各拠点にて「個人情報管理台帳」に定める期間、保管する。

(取扱状況の把握および安全管理措置の見直し)

第10条 各部の個人情報管理者(園責任者)は、定期的または必要に応じて臨時に第7条に規定する個人データの運用状況の記録および第8条に規定する個人情報データベース等の取扱状況の確認を実施しなければならない。

2. 各部の個人情報管理者(園責任者)は、前項の確認の結果および次条の監査の結果にもとづき、安全管理措置の評価、見直しおよび改善に取り組むものとする。

(監査)

第11条 当法人の監事は、監査チェックシートにもとづき、当法人の個人データの適正な取扱いその他法令および本規程の遵守状況について検証し、その改善を個人情報管理責任者および各部の個人情報管理者(園責任者)に促す。

2. 当法人の監事は、当法人の個人データの適正な取扱いその他法令および本規程の遵守状況について定期的に監査を実施する。

第2節 人的安全管理措置

(教育・研修)

第12条 個人情報管理責任者は、職員に本規程を理解し、遵守させるための教育訓練を企画・運営する責任を負う。

2. 職員は、個人情報管理責任者が主催する本規程を遵守させるための教育を受けなければならない。研修の内容およびスケジュールは、事業年度毎に個人情報管理責任者が定める。

第3節 物理的安全管理措置

(個人データを取り扱う区域の管理)

第13条 当法人は管理区域および取扱区域を明確にし、それぞれの区域に対し、次の各号に従い以下の措置を講じる。(ゾーニング)

(1) 管理区域

管理区域は、個人情報・マイナンバー等を金庫に保管している事務室、園長室として、許可された者以外の入退室を制限する。

(2) 取扱区域

取扱区域はマイナンバー以外の個人情報を取り扱う職員室とする。キャビネットの施錠や間仕切り等の設置、座席の配置の工夫などにより、可能な限り権限を有しない者による個人データの閲覧等を防止する。

●入退室管理

・情報処理施設を含む領域を保護するために、下記のセキュリティ境界を設ける。

1) 施設

- ① 正面玄関 ② 園長室 ③ 職員室 ④ 医務室・事務室 ⑤保健室 ⑥給食室

上記セキュリティエリアは、入退室の管理及び鍵の管理を実施するものとし、保育室はフリースペースとする。

- 2) 必要に応じ施設のセキュリティ境界に関する、『配置図』を作成し、区画を明確にする。

・執務室への立入制限について

1) 来訪者(外来者)入口の制限、及び記録

- ① 来訪者には、1F 玄関にて担当職員が対応し、「訪問記録簿」へ訪問時間、訪問者の所属する組織名及び氏名、訪問の目的及び訪問相手を記入する。
- ② 個人情報管理責任者は、毎月「訪問記録簿」を確認し、不適切なアクセス有無のチェックを行う。不備・記載 漏れ等が発見された場合は、対応者に確認の上、運用を徹底させる。必要な場合は、是正処置を講ずる。

2) 職員入口の制限及び記録

- ① 正面玄関での出入については、来訪者の出入管理に支障をきたさないように、配慮する。
- ② 第三者が内部を観察できないように、また容易に進入できないように開放しない。

3) 窓

- ① 常時施錠する。
- ② 換気等が必要な場合で職員の監視が行われている間のみ開放できる。

・セキュリティカード及び鍵の管理

- 1) 施設出入口のセキュリティカード及び鍵管理は、個人情報管理責任者及び個人情報管理責任者が選任した責任者が行う。赤間保育においてセキュリティカードは個人情報管理責任者が任命した職員に付与する。

(機器および電子媒体等の盗難等の防止)

第14条 当法人は管理区域および取扱区域における個人データを取り扱う機器、電子媒体および書類等の盗難または紛失等を防止するため、次の各号に掲げる措置を講じる。

(1) 個人データを取り扱う機器、電子媒体または書籍等を、施錠可能なキャビネット・書庫等に保管する。

(2) 個人データを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定する。

●情報処理装置のセキュリティ対策

・セキュリティ対策として以下の事項を遵守する。

- 1) CD-R・USB メモリ等による情報の盗難を防止するため、使用する媒体は、施設支給(パスワード付 USB メモリ)に限定し、施設の敷地外における記憶媒体の使用は原則禁止とする。
- 2) 施設支給の媒体については、個人情報管理責任者が USB 等記憶媒体の管理台帳で管理する。
- 3) 帰宅時及び不在時(一時的離席は除く)は、携帯可能な情報処理装置(ノート PC 等)・記憶媒体を所定の保管場所(鍵付きの机の中等)にしまい、“盗難”から保護する。
- 4) 私物パソコン及び外部記憶媒体の持ち込みは禁止する。

・電源対策として以下の事項を実施する。

- 1) 装置は、停電、その他の電源異常から下記のように保護する。

① ノートパソコン等の電源を搭載する情報処理設備

停電、電圧変動等の影響を受けないが、搭載している電源が十分に機能することを定期的を確認し、電源の機能が低下している場合には正常なものと交換する。

② 電源を搭載しない情報処理設備

サーバに無停電電源装置(UPS)を装備する。

(ア) UPS に接続する機器の消費電力合計は UPS の容量を超過しないように設定する。

(イ) UPS の容量は、接続している機器が安全に停止できるに十分な時間バックアップできるように設定する。

(ウ) 運用している UPS は個人情報管理責任者が状態確認を行う。異常を発見した場合には速やかに処置する。

(エ) UPS に接続された機器には、停電時に UPS による電源供給が開始されると共に停止処理が開始されるようなソフトウェアを搭載するようにし、そうでない場合には定期的に停電時の訓練を行う。

③ 委託先に運用、保守、管理を委託している情報処理設備

(ア) 赤間保育園「ルクミー」、第二赤間保育園「コドモン」(保育園専用業務ソフト)

(イ) メールサーバ

●携帯電話、モバイル機器の使用、セキュリティ

・保護者へのアクセス(連絡)は、原則、固定電話から行うものとする。

- 1) データの盗難、持出防止のため、園が支給した USB メモリ以外の USB ケーブルによる PC 等への接続は禁止する。日常点検時に、接続を発見した場合は、不適合事項とし、個人情報管理責任者に報告し、是正対策を講じる。

(電子媒体等を持ち運ぶ場合の漏えい等の防止)

第15条 個人データが記録された電子媒体または書類等の搬出を行う場合には、所定様式に記録するとともに、以下の安全策を講じるものとする。

- (1) 個人データが記録された電子媒体を安全に持ち運ぶ方法

- ① 搬出データの暗号化
 - ② 搬出データのパスワードによる保護
 - ③ 施錠できる搬送容器の使用
- (2) 個人データが記載された書類等を安全に持ち運ぶ方法
- ① 封緘、目隠しシールの貼付(各部署の事務取扱担当者から他の部署の事務取扱担当者に個人データが記載された書類等を移送する場合を含む。)

(個人データの削除および機器、電子媒体等の廃棄)

第16条 個人データの廃棄・削除段階における記録媒体等の管理は次のとおりとする。

- ① 事務取扱担当者は、個人データが記録された書類等を廃棄する場合、シュレッダー等による記載内容が復元不能までの裁断、自社または外部の焼却場での焼却・溶解等の復元不可能な手段を用いるものとする。
 - ② 事務取扱担当者は、個人データが記録された機器および電子媒体等を廃棄する場合、専用データ削除ソフトウェアの利用または物理的な破壊等により、復元不可能な手段を用いるものとする。
 - ③ 事務取扱担当者は、個人情報データベース等中の個人データを削除する場合、容易に復元できない手段を用いるものとする。
 - ④ 個人情報に記載された書類等については、当該関連する書類等について当法人が別途定める保存期間経過後の毎年度末に廃棄をするものとする。
2. 事務取扱担当者は、個人データもしくは個人情報データベース等を削除した場合、または電子媒体等を廃棄した場合には、所定様式に記録するものとする。
3. 削除・廃棄の記録としては、個人情報データベース等の種類・名称、責任者・取扱部署、削除・廃棄状況を記録するものとし、当該個人データ自体は含めないものとする。

第4節 技術的安全管理措置

(アクセス制御)

第17条 個人データへのアクセス制御は以下のとおりとする。

- ① 個人情報データベース等を取り扱うことができる情報システムを限定する。
- ② 個人データと紐付けてアクセスできる情報の範囲をアクセス制御により限定する。
- ③ ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる者を事務取扱担当者に限定する。

(アクセス者の識別と認証)

第18条 個人データを取り扱う情報システムは、ユーザーID、パスワード、磁気・ICカード等の識別方法により、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果にもとづき認証するものとする。

(外部からの不正アクセス等の防止)

第19条 当法人は、以下の各方法その他の適切な方法により、情報システムを外部からの不正アクセスまたは不正ソフトウェアから保護するものとする。

- ① 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する方法
- ② 情報システムおよび機器にセキュリティ対策ソフトウェア等(ウイルス対策ソフトウェア等)を導入する方法
- ③ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする方法
- ④ ログ等の分析を定期的に行い、不正アクセス等を検知する方法

●コンピュータウイルス管理

・コンピュータ利用に関する制限事項

- 1) 職員は、その使用するコンピュータに対し、有償・無償を問わず個人情報管理責任者の許可無くソフトウェアをインストール、又は使用してはならない。
- 2) 職員は、その使用するコンピュータに対して、業務に必要な範囲外でインターネット及び電子メールを使用してはならない。
- 3) 個人情報管理責任者は、上記の利用状況について適宜確認を行うことがある。

・外部から入手されるファイル及びソフトウェアの処置

- 1) インターネットから、又はインターネット経由で、若しくは、他の媒体により入手された、ファイル及びソフトウェアは、ウイルス検知用ソフトでウイルスが存在しないかどうかを使用前にチェックする。
- 2) 電子メールで送信されてくるデータのうち、疑わしき場合は(送り主や用件に覚えがない、文字化けしている等)、メールを開封せずにウイルスが存在しないかどうかを使用前にチェックする。

・セキュリティパッチの適用

- 1) 個人情報管理責任者は、インターネット等を通じて、オペレーティングシステムやソフトウェア等に対する脆弱性に関する修正プログラムが公開されているかを確認し、該当する場合は、セキュリティパッチを適用する。
- 2) オペレーティングシステムに自動更新プログラムが組み込まれている場合は、最新の状態が保たれるように設定する。

・ウイルス対策ソフトの運用

- 1) ウィルス対策ソフトの導入
利用される全てのコンピュータにはウイルス対策ソフトがインストールされ、マシンの起動と共に常駐されているようにしておく。
- 2) ウィルス定義パターンの更新
 - ① ウィルス対策ソフトのウィルス定義パターンは常に最新のものとなるように、マシンの起動時にアップデートされるようにしておく。
 - ② オフラインで使用されることの多いマシンについては最低でも使用する者によって週一回、ウィルス定義パターンの更新を行う。

・ウイルス感染が判明した場合の処置

1) 隔離

感染の判明したコンピュータは速やかにネットワークより切り離し、個人情報管理責任者に報告する。個人情報管理責任者は、ウイルス感染によって影響を受ける関係者(データの提供先等)に適宜連絡を行う。

2) ウイルスの駆除(治療)

感染したコンピュータは“ウイルス対策ソフト”によって処置を行う。ウイルスを除去できない場合には個人情報管理責任者の指示に従って、システムの復旧または媒体の破棄を行う。取られた処置は記録する。

3) 被害状況の把握と原因の調査

ウイルス除去の完了後、個人情報管理責任者は被害状況を把握するとともに、原因について調査を行う。

4) 是正処置

個人情報管理責任者は是正処置の必要性を検討し、必要な場合は是正処置を立案、実施する。

●電子メール上のセキュリティ

1) メールアカウントの設定は個人情報管理責任者に申請し、個別アカウントを設定する。

2) 私有のメールアカウント及び WEB メールを業務で使用しない。

3) メールの形式はウイルス感染の脆弱性のある HTML 形式でなく、テキスト形式とする。

4) 電子メールからのウイルス感染を予防するために、ウイルス対策ソフトは常時電子メールの監視状態にしておく。

5) 電子メールの添付ファイル若しくはダウンロードファイルについては、不正ソフトウェアでないかどうかを使用者が使用前にチェックする。

6) 機密情報を添付ファイルとして送信する場合には、パスワードが無いと内容確認ができないようにして送信する。

7) 宛先が不正確であったり、間違っていたりなどのエラーを防止するために、一度登録し、送付試験を完了したアドレスを用いて送付する。

8) 施設の信用を傷つけないための職員の責任として以下を注意する。

a. 誹謗・中傷的な内容の電子メールを送信しない。

b. 相手を困らせるための使用はしない。

c. 購入等で認可を必要とされている行為を、許可無しで行うための電子メール使用をしない。

●電話、ファックス時のセキュリティ

1) 電話時のセキュリティ

① 通話をする場合(特に携帯電話)にはすぐ近くにいる人々及び、電話の相手先にいる人々によって盗み聴きされたりしないように配慮する。

② 必要な場合、伝達しようとしている相手が適切であるか確認し、疑義のある場合には伝達をしない。本人若しくは関係者に“なりすまし”で情報を入力される場合もある。

③ 先方から電話を掛けてきた場合で必要な場合は、こちらから掛け直して、先方の所在が信用のおけるものであるか確認する。

- ④ 公共の場所または囲われていないオフィス、また、壁が薄い会場場所で機密の会話をしないように注意する。
- ⑤ 留守番電話にメッセージを残しておく、認可されていない者によって再生されるかもしれないし、共同システムに保存されたり、またダイヤル間違いの結果として間違っ保存されたりすることがあるので、メッセージを残しておかないようにする。

2) ファックス時のセキュリティ

- ① ファックスに出力された情報に認可されていないアクセスが行われる可能性があるため、場合によっては適切な要員に出力を確認させる。
- ② ダイヤル間違い又は間違っ記憶された番号によって、情報が間違っ送付先にファックス送信されてしまうので、送信者とは別の職員が目視にて十分に確認する。
- ③ ファックス受領時、紛失を防ぐために確実に手渡しする。不在時は、専用ファイルに入れる。

●離席時のセキュリティ

職員は、休憩時や業務途中で離席する場合は、データの盗難や盗み見等のリスクを予防する処置を講じる。

1) クリアデスク

業務上重要な機密情報を扱う場合は、その情報が他人に知られないように、該当箇所を隠すか(ファイルの場合は閉じる)、保管場所(机の中等)に格納してから離席する。

2) クリアスクリーン

パソコン等を用いて、業務上重要な機密情報を扱う場合は、その情報が他人に知られないように、ファイル画面を一旦閉じるか、データにパスワードを設定する。

他に知られてはいけない重要情報をデスクトップ上に保存することは禁止とする。

担当者不在時は、ログオフ又は、スクリーンセーバを設定する。なお、スクリーンセーバの起動時間は30分で設定する。

情報共有の必要性から、スクリーンセーバにはパスワード設定を行わず、担当者が問合せ時に確認可能な状態を維持する。

●バックアップ

機密情報及びソフトウェアについては、下記手順に従ってバックアップを定期的取得し、かつ検査する。

- 1) 個人情報管理責任者は、バックアップ対象を特定し、バックアップの必要な業務情報及びソフトウェアを明確にし、実施責任者、バックアップ先、バックアップの保存期間、バックアップ媒体の保存場所、バックアップ復元試験の実施頻度について明確にする。
- 2) バックアップの対象が障害を被るような事態がバックアップ媒体に影響しないように、バックアップ媒体の保存場所(離れた場所にある鍵つきの耐火金庫等)を考慮する。(バックアップ媒体が新たな脅威を引き起こすことがあることに留意する。)
- 3) バックアップ情報はバックアップの対象と同程度の保護を行う。
- 4) 取得したバックアップデータについては、随時、必要に応じ“復元試験”を行う。これにより、回復の手順が有効で、求められる時間内に完了でき、バックアップ媒体が問題無く機能するかを検証し、結果を記録する。

●削除又は媒体の処分

個人情報の消去、または媒体が不要となった場合は、安全、かつ、確実に処分するため、次の点に注意して行う。

- 1) 確実な処分を必要とする媒体として可能性のあるものは次のとおりである。
紙に印刷された文書、録音、録画、ビデオテープ、カーボン紙、出力レポート、使い捨てプリンタリボン、磁気テープ、フロッピーディスク、カセット(TEL 含む)、光学式記録媒体、プログラムリスト、試験データ、システム文書
- 2) 個人情報が含まれた媒体の処分に当たっては事前に申請し、各拠点責任者の承認を得る。各拠点責任者は、個人情報管理責任に報告し、承認を得る。
- 3) 個人情報が含まれる“紙媒体”は、シュレッダー等による物理的破断処理を行ない、中身が容易に分かる状態でゴミ箱へ廃棄することを禁止する。
- 4) 個人情報が含まれる磁気媒体(情報処理装置の記憶媒体、バックアップ媒体を含む)は、標準の削除機能を用いるよりも“データ消去ツール”による再読不可能処理、もしくは“物理的破断処理”、もしくは“確実に上書き”を行う。

(情報システムの使用に伴う漏えい等の防止)

第20条 当法人は、以下の各方法その他の適切な方法により、情報システムの使用に伴う個人データの漏えい等を防止するために必要となる措置を講じるものとする。

- ① 情報システムの設計時に安全性を確保し、継続的に見直す(情報システムの脆弱性を突いた攻撃への対策を講じることも含む。)
- ② 個人データを含む通信の経路または内容を暗号化する。
- ③ 移送する個人データについて、パスワード等による保護を行う。

●ネットワークのアクセス制御

ネットワークを介したサービスの保護を、以下の事項により確実にする。

4) 指定された接続経路

利用者端末からコンピュータサービスまでの経路を下記のとおり管理する。

- ① 施設内のシステムにファイア・ウォールを設け、不正アクセスが出来ない設定とする。
- ② 外部から施設内LANへの無許可のアクセスは不可とする。
- ③ 外部と接続する機器は、十分なアクセス制御機能を有したものを利用する。
- ④ 長期間利用しない機器は、電源を落としておくか、ネットワークに接続しない。

2) 遠隔診断用サポートの保護

- ① 当法人のシステム開発、保守管理は、株式会社 FT コミュニケーションへ委託している。サーバのメンテナンスについては、委託契約の中で定めた担当者が実施する。
- ② リモートメンテナンスは、行わない。必要に応じ、リモートメンテナンスを依頼する場合は、作業終了後、速やかにログインパスワード等を変更する。

第5節 外的環境の把握

(外的環境の把握)

第21条 当法人は、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じる。現状において当該データの取扱いは存在しない。

第3章 個人情報の管理

第1節 個人情報の取得および保有等

(利用目的の特定)

第22条 当法人は、個人情報を取り扱うにあたっては、業務を遂行するため必要な場合に限り、かつ、その利用の目的(以下「利用目的」という。)をできる限り特定しなければならない。

2. 当法人は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

(利用目的による制限)

第23条 当法人は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない。

2. 当法人は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3. 前二項の規定は、次に掲げる場合については、適用しない。

(1) 法令にもとづく場合

(2) 人の生命、身体または財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

(3) 公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

(4) 国の機関もしくは地方公共団体またはその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(5) 学術研究機関等に個人データを提供する場合であって、当該学術研究機関等が当該個人データを学術研究目的で取り扱う必要があるとき(当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。)

(利用目的の通知等)

第24条 当法人は、個人情報を取得する場合は、あらかじめその利用目的を公表している場合を除き、同時にまたは取得後速やかに、その利用目的を、本人に通知し、または公表するものとする。公表は施設内やホームページへの掲載により行うことができる。

2. 前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面(電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。)に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示するものとする。ただし、人の生命、身体または財産の保護のために緊急に必要がある場合は、この限りでない。
3. 当法人は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、または公表しなければならない。
4. 前三項の規定は、次に掲げる場合については、適用しない。
 - (1) 利用目的を本人に通知し、または公表することにより本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
 - (2) 利用目的を本人に通知し、または公表することにより当法人の権利または正当な利益を害するおそれがある場合
 - (3) 国の機関または地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、または公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
 - (4) 取得の状況からみて利用目的が明らかであると認められる場合

(不適正な利用の禁止)

第25条 当法人は、違法または不当な行為を助長し、または誘発するおそれがある方法により個人情報を利用してはならない。

(適正な取得)

第26条 当法人は、偽りその他不正な手段により個人情報を取得してはならない。

2. 当法人は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。
 - (1) 法令にもとづく場合
 - (2) 人の生命、身体または財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 国の機関もしくは地方公共団体またはその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
 - (5) 学術研究機関等から当該要配慮個人情報を取得する場合であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき(当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人

の権利利益を不当に侵害するおそれがある場合を除く。)(当法人と当該学術研究機関等が共同して学術研究を行う場合に限る。)

- (6) 当該要配慮個人情報、本人、国の機関、地方公共団体、学術研究機関等、個人情報保護法第 57 条第1項各号に掲げる者、外国政府、外国の政府機関、外国の地方公共団体または国際機関、外国における学術研究機関等に相当する者、外国における個人情報保護法第 57 条第1項各号に掲げる者に相当する者により公開されている場合
- (7) 本人を目視し、または撮影することにより、その外形上明らかな要配慮個人情報を取得する場合
- (8) 個人情報保護法第 27 条第5項各号において、個人データである要配慮個人情報の提供を受けるとき。

(データ内容の正確性の確保等)

第27条 当法人は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

第2節 監督

(職員の監督)

第28条 個人情報管理責任者は、職員が個人データを取り扱うにあたり、必要かつ適切な監督を行わなければならない。

- 2. 個人情報管理者(園責任者)は、自らの園に属する職員に対し、個人データの取扱いに関して必要かつ適切な監督を行わなければならない。
- 3. 個人情報管理責任者は、職員に対して個人情報の保護および適正な取扱いに関する誓約書の提出を命じることができる。

(委託先の監督)

第29条 個人情報管理者(園責任者)は、個人データの取扱いの全部または一部を委託する場合(労働者派遣契約または業務委託等契約により派遣労働者を受け入れる場合を含む。)は、その取扱いを委託した個人データの安全管理が図られるよう、委託先に対する必要かつ適切な監督を行わなければならない。

2. 前項の委託を行う個人情報管理者(園責任者)は、委託先に対して以下の各号の事項を実施しなければならない。

- (1) 委託先における個人情報の保護体制が十分であることを確認した上で委託先を選定すること
- (2) 委託先との間で次の事項を含む契約を締結すること
 - ① 個人情報の適法かつ適切な取扱い(個人データに対する組織的、人的、物理的、技術的な安全管理措置を委託先が講じることを含む。)
 - ② 個人情報に関する秘密保持
 - ③ 委託した業務以外の個人情報の利用禁止
 - ④ 個人情報を取り扱う上での安全対策

- ⑤ 再委託に関する事項(再委託は原則として禁止し、再委託がやむを得ない場合は事前に書面による当法人の同意を要する。)
 - ⑥ 契約内容が遵守されていることの確認および報告
 - ⑦ 個人情報に関する事故が生じた際の責任
 - ⑧ 契約終了時の個人情報の返却および抹消
- (3) 個人情報の取得を委託する場合は、当法人が取得の主体であることならびに当法人の指定する利用目的を明示するよう義務付けること

第3節 第三者提供の制限

(第三者提供の制限)

第30条 当法人は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

- (1) 法令にもとづく場合
 - (2) 人の生命、身体または財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 国の機関もしくは地方公共団体またはその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
 - (5) 当該第三者が学術研究機関等である場合であって、当該第三者が当該個人データを学術研究目的で取り扱う必要があるとき(当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。)
2. 当法人は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、または本人が容易に知り得る状態におくとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。ただし、第三者に提供される個人データが要配慮個人情報または偽りその他不正の手段により取得されたものもしくは他の個人情報取扱事業者からこの項本文の規定により提供されたもの(その全部または一部を複製し、または加工したものを含む。)である場合は、この限りではない。
- (1) 当法人の名称および住所ならびに代表者の氏名
 - (2) 第三者への提供を利用目的とすること。
 - (3) 第三者に提供される個人データの項目
 - (4) 第三者に提供される個人データの取得の方法
 - (5) 第三者への提供の方法
 - (6) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
 - (7) 本人の求めを受け付ける方法

(8) 第三者に提供される個人データの更新の方法、当該届出に係る個人データの第三者への提供を開始する予定日

3. 当法人は、前項第1号に掲げる事項に変更があったときまたは同項の規定による個人データの提供をやめたときは遅滞なく、同項第3号から第5号まで、第7号または第8号に掲げる事項を変更しようとするときはあらかじめ、その旨について、本人に通知し、または本人が容易に知り得る状態におくとともに、個人情報保護委員会に届け出なければならない。
4. 第2項および前項における「通知し、または本人が容易に知り得る状態におく」とは、規則において定められる以下のいずれかの措置を講ずることをいう。
 - (1) 第三者に提供される個人データによって識別される本人が当該提供の停止を求めるのに必要な期間をおくこと。
 - (2) 本人が第三者に提供される個人データの項目等の第2項各号の事項を確実に認識できる適切かつ合理的な方法によること。
5. 当法人は、第2項および第3項による個人情報保護委員会に対する届出事項が同委員会により公表された後、速やかに、インターネットの利用その他の適切な方法により、第三者に提供される第2項各号の事項(変更があったときは、変更後の事項)を公表するものとする。
6. 次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。
 - (1) 当法人が利用目的の達成に必要な範囲内において個人データの取扱いの全部または一部を委託することに伴って当該個人データが提供される場合
 - (2) 合併その他の事由による事業の承継に伴って個人データが提供される場合
 - (3) 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨ならびに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的ならびに当該個人データの管理について責任を有する者の氏名または名称および住所ならびに法人にあってはその代表者の氏名について、あらかじめ、本人に通知し、または本人が容易に知り得る状態にしているとき。
7. 当法人は、前項第3号に規定する個人データの管理について責任を有する者の氏名、名称もしくは住所または法人にあっては、その代表者の氏名に変更があったときは遅滞なく、同号に規定する利用する者の利用目的または当該責任を有する者を変更しようとするときはあらかじめ、その旨について、本人に通知し、または本人が容易に知り得る状態に置かなければならない。

(外国にある第三者への提供の制限)

- 第31条 当法人は、外国(本邦の域外にある国または地域をいう。以下同じ。)にある第三者(個人情報取扱事業者に該当する者を除く。)に個人データを提供する場合には、前条第1項各号に掲げる場合を除き、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。ただし、外国にある事業者が個人情報保護委員会の規則で定める基準に適合する体制を整備している者である場合は、前条を適用する。
2. 当法人は、前項の規定により本人の同意を得ようとする場合には、電磁的記録の提供による方法、書面の交付による方法その他の適切な方法により、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供する。

3. 当法人は、個人データを外国にある第三者に提供した場合には、個人情報保護委員会が規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供する。

(第三者提供をする際の記録)

第32条 当法人は、個人データを第三者(国の機関、地方公共団体、独立行政法人等、地方独立行政法人を除く。)に提供したときは、第三者提供にかかる記録を書面または電磁的記録により作成しなければならない。ただし、当該個人データの提供が第30条第1項各号に該当する場合または同条第6項各号のいずれか(前条第1項の規定による個人データの提供にあつては第30条第1項各号のいずれか)に該当する場合は、この限りでない。

2. 前項の記録は、次項または第4項に該当する場合を除き、第三者に個人データの提供をした都度、速やかに作成しなければならない。
3. 第1項の記録は、当該第三者に継続的にもしくは反復して個人データの提供(第30条第2項の方法により個人データを提供する場合を除く。)をしたとき、または当該第三者に継続的にもしくは反復して個人データを提供することが確実であると見込まれるときの記録は、一括して作成することができる。
4. 第1項の記録は、本人に対する物品または役務の提供に関連して当該本人にかかる個人データを第三者に提供した場合において、当該提供に関して作成された契約書その他の書面に記録すべき事項が記載されているときは、当該書面をもって第三者に個人データを提供したときの記録に代えることができる。
5. 第30条第2項にもとづき個人データを第三者に提供した場合は所定様式に以下の事項を記録するものとする。
 - (1) 当該個人データを提供した年月日
 - (2) 当該第三者の氏名または名称および住所ならびに法人にあつては、その代表者(法人でない団体で代表者または管理人の定めのあるものにあつては、その代表者または管理人)の氏名(不特定かつ多数の者に対して提供したときは、その旨)
 - (3) 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
 - (4) 当該個人データの項目
6. 第30条第1項または前条第1項にもとづく本人の同意を得て個人データを第三者に提供した場合は所定様式に以下の事項を記録するものとする。
 - (1) 本人の同意を得ている旨
 - (2) 当該第三者の氏名または名称および住所ならびに法人にあつては、その代表者(法人でない団体で代表者または管理人の定めのあるものにあつては、その代表者または管理人)の氏名(不特定かつ多数の者に対して提供したときは、その旨)
 - (3) 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
 - (4) 当該個人データの項目
7. 第5項および前項の記載事項のうち、第1項から第4項までの方法により作成した記録(保存している場合に限る。)に記録されている事項と内容が同一であるものについては、当該事項の記録を省略することができる。
8. 当法人は、第5項から前項までの規定により作成した記録を、以下の場合に応じて、当該記録を作成した日から所定の期間保存するものとする。

場合	保存期間
① 本人を当事者とする契約書等 にもとづく個人データの提供の 場合	最後に当該記録にかかる個人データの提供を行 った日から起算して1年を経過する日までの間
② 個人データを継続的にもしくは 反復して提供する場合	最後に当該記録にかかる個人データの提供を行 った日から起算して3年を経過する日までの間
③ 上記①または②以外の場合	当該記録を作成した日から3年間

(第三者提供を受ける際の確認および記録)

第33条 当法人は、第三者から個人データの提供を受けるに際しては、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第30条第1項各号に該当する場合または同条第6項各号のいずれかに該当する場合は、この限りでない。

(1) 当該第三者の氏名または名称および住所ならびに法人にあっては、その代表者(法人でない団体で代表者または管理人の定めのあるもの)にあっては、その代表者または管理人の氏名

(2) 当該第三者による当該個人データの取得の経緯

2. 当法人は、第三者から個人データの提供を受ける際の確認を行う方法は、確認を行う事項の区分に応じて、それぞれ次のとおりとする。

場合	方法
① 前項第1号に該当する事項	個人データを提供する第三者から申告を受ける 方法その他の適切な方法
② 前項第2号に該当する事項	個人データを提供する第三者から当該第三者に よる当該個人データの取得の経緯を示す契約書 その他の書面の提示を受ける方法その他の適切 な方法

3. 前項にかかわらず、第三者から他の個人データの提供を受けるに際して前項の方法による確認(当該確認について記録の作成および保存をしている場合におけるものに限る。)を行っている事項の確認を行う場合は、当該事項の内容と当該提供にかかる確認事項の内容が同一であることの確認を行う方法によるものとする。

4. 当法人は、前三項にもとづく確認を行ったときは、以下の区分に応じて以下の事項を記録しなければならない。

(1) 第30条第2項の方法により個人データの提供を受けた場合

① 個人データの提供を受けた年月日

② 当該第三者の氏名または名称

③ 当該第三者の住所

④ 当該第三者が法人である場合は、その代表者(法人でない団体で代表者または管理人の定めのあるもの)にあっては、その代表者または管理人の氏名

⑤ 当該第三者による当該個人データの取得の経緯

- ⑥ 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
 - ⑦ 当該個人データの項目
 - ⑧ 個人情報保護法第 27 条第4項にもとづき個人情報保護委員会による公表がされている旨
- (2) 第 30 条第1項または第 31 条第1項にもとづく本人の同意を得て第三者から提供を受けた場合
- ① 本人の同意を得ている旨
 - ② 当該第三者の氏名または名称
 - ③ 当該第三者の住所
 - ④ 当該第三者が法人である場合は、その代表者(法人でない団体で代表者または管理人の定めのあるものにあつては、その代表者または管理人)の氏名
 - ⑤ 当該第三者による当該個人データの取得の経緯
 - ⑥ 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
 - ⑦ 当該個人データの項目
- (3) 個人関連情報取扱事業者から個人関連情報の提供を受けて個人データとして取得した場合
- ① 本人の同意が得られている旨および外国にある個人情報取扱事業者にあつては、本人に参考となるべき情報の提供が行われている旨
 - ② 当該第三者の氏名または名称
 - ③ 当該第三者の住所
 - ④ 当該第三者が法人である場合は、その代表者(法人でない団体で代表者または管理人の定めのあるものにあつては、その代表者または管理人)の氏名
 - ⑤ 当該第三者による当該個人データの取得の経緯
 - ⑥ 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
 - ⑦ 当該個人関連情報の項目
- (4) 個人情報取扱事業者ではない第三者から提供を受けた場合
- ① 当該第三者の氏名または名称
 - ② 当該第三者の住所
 - ③ 当該第三者が法人である場合は、その代表者(法人でない団体で代表者または管理人の定めのあるものにあつては、その代表者または管理人)の氏名
 - ④ 当該第三者による当該個人データの取得の経緯
 - ⑤ 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
 - ⑥ 当該個人データの項目
5. 前項各号の記載事項のうち、既に作成した記録(保存している場合に限る。)に記録されている事項と内容が同一であるものについては、当該事項の記録を省略することができる。
6. 第4項の記録は、次項または第8項に該当する場合を除き、第三者から個人データの提供を受けた都度、速やかに作成しなければならない。
7. 第4項の記録は、当該第三者から継続的にもしくは反復して個人データの提供(第 30 条第2項の方法により個人データの提供を受けた場合を除く。)を受けたとき、または当該第三者から継続的にもしくは反復して個人データの提供を受けることが確実であると見込まれるときの記録は、一括して作成することができる。

8. 第4項の記録は、本人に対する物品または役務の提供に関連して第三者から当該本人にかかる個人データの提供を受けた場合において、当該提供に関して作成された契約書その他の書面に記録すべき事項が記載されているときは、当該書面をもって第三者から個人データの提供を受けたときの記録に代えることができる。
9. 当法人は、第4項または第5項により作成した記録を、以下の場合に依じて、当該記録を作成した日から所定の期間保存するものとする。

場合	保存期間
① 本人を当事者とする契約書等にもとづく個人データの提供の場合	最後に当該記録にかかる個人データの提供を受けた日から起算して1年を経過する日までの間
② 個人データを継続的にもしくは反復して提供する場合	最後に当該記録にかかる個人データの提供を受けた日から起算して3年を経過する日までの間
③ 上記①または②以外の場合	当該記録を作成した日から3年間

(個人関連情報の第三者提供の制限等)

第34条 当法人は、第三者が個人関連情報(個人関連情報データベース等を構成するものに限る。以下同じ。)を個人データとして取得することが想定されるときは、第30条第1項各号に掲げる場合を除くほか、次に掲げる事項について、あらかじめ個人情報保護委員会が規則で定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。

- (1) 当該第三者が当法人から個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の当該本人の同意が得られていること。
 - (2) 外国にある第三者への提供にあつては、前号の本人の同意を得ようとする場合において、電磁的記録の提供による方法、書面の交付による方法その他の適切な方法により、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報が当該本人に提供されていること。
2. 当法人は、個人データを外国にある第三者に提供した場合には、個人情報保護委員会が規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講じる。
3. 当法人は、第1項にもとづく確認を行ったときは、以下の事項を記録しなければならない。
- (1) 本人の同意が得られていることを確認した旨および外国にある第三者への提供にあつては、本人に参考となるべき情報の提供が行われていることを確認した旨
 - (2) 個人関連情報を提供した年月日(第6項により記録を一括して作成する場合にあつては、当該提供の期間の初日および末日)
 - (3) 当該第三者の氏名または名称
 - (4) 当該第三者の住所
 - (5) 当該第三者が法人である場合は、その代表者(法人でない団体の代表者または管理人の定めのあるものにあつては、その代表者または管理人)の氏名
 - (6) 当該個人関連情報の項目

4. 前項の記載事項のうち、既に作成した記録(記録を保存している場合に限る。)に記録された事項と内容が同一であるものについては、当該事項の記録を省略することができる。
5. 第3項の記録は、次項または第7項に該当する場合を除き、第三者に個人関連情報の提供をした都度、速やかに作成しなければならない。
6. 第3項の記録は、当該第三者に継続的にもしくは反復して個人関連情報の提供をしたとき、または当該第三者から継続的にもしくは反復して個人関連情報の提供をすることが確実であると見込まれるときの記録は、一括して作成することができる。
7. 第3項の記録は、本人に対する物品または役務の提供に関連して第三者に当該本人に係る個人関連情報の提供をした場合において、当該提供に関して作成された契約書その他の書面に記録すべき事項が記載されているときは、当該書面をもって第三者への個人関連情報の提供の記録に代えることができる。
8. 当法人は、第3項または第4項により作成した記録を、以下の場合に依じて、当該記録を作成した日から所定の期間保存するものとする。

場合	保存期間
本人を当事者とする契約書等にもとづく個人関連情報の提供の場合	最後に当該記録に係る個人関連情報の提供を行った日から起算して1年を経過する日までの間
個人関連情報を継続的にもしくは反復して提供する場合	最後に当該記録に係る個人関連情報の提供を行った日から起算して3年を経過する日までの間
上記①または②以外の場合	当該記録を作成した日から3年

第4節 保有個人データに関する事項の公表等

(保有個人データに関する事項の公表等)

第35条 当法人は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置かなければならない。

- (1) 当法人の名称および住所ならびにその代表者の氏名
 - (2) 全ての保有個人データの利用目的(第24条第4項第1号から第3号までに該当する場合を除く。)
 - (3) 次項の規定による求めまたは第36条第1項もしくは第37条第1項の規定による請求に応じる手続
 - (4) 保有個人データの安全管理のために講じた措置(本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)におくことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。)および苦情の申出先
2. 当法人は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、次の各号のいずれかに該当する場合は、この限りでない。
 - (1) 前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合
 - (2) 第24条第4項第1号から第3号までに該当する場合
 3. 当法人は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

第4章 保有個人データの開示等の請求等および苦情対応

(開示)

第36条 当法人は、本人から、当該本人が識別される保有個人データの開示を求められたときは、本人が請求した方法(当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法)により、遅滞なく当該保有データを開示する。ただし、開示することにより次のいずれかに該当する場合は、その全部または一部を開示しないことができる。

- (1) 本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- (2) 当法人の事業の適正な実施に著しい支障を及ぼすおそれがある場合
- (3) 他の法令に違反することとなる場合

2. 当法人は、前項の規定にもとづき求められた保有個人データの全部もしくは一部について開示しない旨の決定をしたとき、請求にかかる保有個人データが存在しないときまたは本人が請求した方法による開示が困難であるときは、本人に対し遅滞なく、書面により通知するものとする。この場合、その理由を説明するよう努めなければならない。
3. 他の法令により、本人に対し当該本人が識別される保有個人データを開示することとされている場合には、第1項は適用しない。
4. 第1項または第2項については、第32条第1項または第33条第4項の記録について準用する。
5. 第1項または前項の開示の請求の手續の方法に関しては、個人情報保護法に従い対応する。

(訂正等)

第37条 当法人は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって、当該保有個人データの訂正、追加または削除(以下「訂正等」という。)を求められたときは、その内容の訂正等に関して他の法令の規定により特別の手續が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果にもとづき、当該保有個人データの内容の訂正等を行うものとする。ただし、次のいずれかに該当する場合は、訂正等の求めに応じないことができる。

- (1) 利用目的の達成に必要な範囲を超えている場合
- (2) 他の法令の規定により、特別の手續が定められている場合

2. 前項により、保有個人データの訂正等を行ったとき、または訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なくその旨(訂正等を行ったときはその内容を含む。)を通知するものとする。
3. 第1項ただし書により訂正等の求めに応じない場合は、その理由を説明するよう努めなければならない。

(利用停止等)

第38条 当法人は、本人から、当該本人が識別される保有個人データが、第23条(利用目的による制限)、第25条(不適正な利用の禁止)または第26条(適正な取得)に違反しているという理由によって、当該保有個人データの利用の停止または消去(以下「利用停止等」という。)が求められた場合、または、第30条(第三者提供の制限)または第31条(外国にある第三者への提供の制限)に違反しているという理由によって、当該保有個人データの第三者提供の停止が求められた場合で、当該請求に理由があることが判明したときは、違反を是正するために必要

な限度で、遅滞なく、当該保有個人データの利用停止等または第三者への提供の停止を行わなければならない。ただし、当該保有個人データの利用停止等または第三者への提供の停止に多額の費用を要する場合その他の利用停止等または第三者への提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

2. 当法人は、本人より当該本人が識別される保有個人データを当法人が利用する必要がなくなった場合、当該本人が識別される保有個人データに係る報告等が必要な漏えい等が生じた場合その他当該本人が識別される保有個人データの取扱いにより当該本人の権利または正当な利益が害されるおそれがあるという理由によって、当該保有個人データの利用停止等または第三者への提供の停止が求められた場合で、その請求に理由があることが判明したときは、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等または第三者への提供の停止を行わなければならない。ただし、当該保有個人データの利用停止等または第三者への提供の停止に多額の費用を要する場合その他の利用停止等または第三者への提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。
3. 第1項または前項により、保有個人データの利用停止等または第三者提供の停止の措置を講じない旨の決定をしたときは、本人に対し、遅滞なくその旨を通知するものとする。
4. 第1項または第2項ただし書により利用停止等または第三者提供の停止の求めに応じない場合は、その理由を説明するよう努めなければならない。

(苦情への対応)

第39条 当法人は、保有個人データの取扱いに関する苦情について必要な体制の整備を行い、苦情があったときは適切かつ迅速な処理に努めるものとする。

第5章 雑則

(細則)

第40条 本規程を運用するために必要な細則、マニュアルなどは、理事長の承認を得て別途定める。

(所管部署)

第41条 本規程の所管は、当法人とする。

(規程の改廃)

第42条 本規程の改正、廃止については理事会の決議による。

(個人情報保護に関する基本方針宣言)

第43条 当法人は本規程の目的を達成する手段の一つとして、個人情報保護に対する基本方針を別途定める。

2. 前項の基本方針はポスター、ホームページなどの方法により当法人の内外で随時第三者の目に触れ、閲覧できるような措置をとる。

3. 基本方針は別紙のとおりとし、必要に応じて改定し、理事長が承認する。

第6章 罰則

(罰則等)

第44条 本規程および個人情報保護法に違反した役職員等は、就業規則にもとづき解雇を含む懲戒の対象となる。

2. 前項により懲戒の対象となった役職員等は当事者および当法人に対する損害賠償の責めに任ずる。

附則

(施行期日)

第1条 本規程は、平成17年10月1日より施行する。

第2条 本規程は、令和4年9月1日より施行し、旧規程は全文を廃止する。