個人データの安全管理に係る取扱規程

個人情報管理規則

1. 目的

(1)　本規則は、当社における個人情報の適正な取扱いの確保を目的とする。

(2)　個人情報の管理に関してこの規則に定めのない事項については、個人情報保護法その他の法令等の定めるところによる。

2. 定義

本規則において、各用語の定義は次の通りとする。

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

① 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ものを含む）

「個人に関する情報」とは、氏名、性別、生年月日、住所、年齢、職業、続柄等の事実に関する情報に限られず、個人の身体、財産、職種、肩書等の属性に関する判断や評価を表すすべての情報を指し、公刊物等によって公にされている情報や、映像、音声による情報も含まれる。これら「個人に関する情報」が、氏名等と相まって「特定の個人を識別することができる」ことになれば、それが「個人情報」となる。なお、生存しない個人に関する情報が、同時に、遺族等の生存する個人に関する情報に当たる場合には、当該生存する個人に関する情報となる。また、企業名等、法人その他の団体に関する情報は、基本的に「個人情報」には該当しないが、役員の氏名等の個人に関する情報が含まれる場合には、その部分については、「個人情報」に該当する。さらに、「個人」には外国人も当然に含まれる。

② 個人識別符号が含まれるもの

個人識別符号とは、個人情報の保護に関する法律施行令等で定める文字、番号、記号その他の符号をいう。例えば、顔の画像、指紋、声紋、旅券番号、基礎年金番号、免許証番号、住民票コード、個人番号が該当する。

(2)　個人情報データベース等とは、個人情報を含む情報の集合物であって、特定の個人情報をコンピュータ等を用いて検索できるように体系的に構成したもの、又はコンピュータ等を用いていない場合であっても、五十音順に索引を付して並べられた顧客カード等、個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるよう体系的に構成したものであって、目次、索引、符号等により一般的に容易に検索可能な状態に置かれているものをいう。

(3)　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。なお、個人情報データベース等から電子記録媒体へダウンロードされたもの及び紙面に出力されたもの（そのコピーを含む）も含まれる。

(4)　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。

(5)　保有個人データとは、当社が、本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして次に掲げるもの以外のもの及び６ヶ月以内に消去すること（更新することを除く）となるもの以外のものをいう。

① 存否が明らかになることで、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

② 存否が明らかになることで、違法又は不当な行為を助長し、又は誘発するおそれがあるもの

③ 存否が明らかになることで、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若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 存否が明らかになることで、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

3. 個人情報の取扱い

3.1 利用目的の特定

(1)　個人情報の取扱いに当たっては、個人情報がどのような事業の用に供され、どのような目的で利用されるかを本人が合理的に予想できるようできる限り特定し、公表する。

(2)　利用目的を変更する場合には、変更後の利用目的が変更前の利用目的からみて、社会通念上本人が想定できる範囲を超えて行ってはならない。本人が想定できない変更を行う場合には、本人の同意を得なければならない。

3.2 利用目的による制限

あらかじめ本人の同意を得ずに、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

ただし、あらかじめ本人の同意を得るために個人情報を利用することは、当初特定した利用目的にない場合にも、目的外利用には当たらない。

3.3 センシティブ情報の取扱い

(1)　個人情報のうち、人種、信条、門地、本籍地、社会的身分、保健医療、労働組合への加盟、性生活、犯罪経歴、犯罪により害を被った事実、被疑者又は被告人としての刑事事件に関する手続が行われた事実、少年の保護事件に関する手続が行われた事実（以下「センシティブ情報」といいます）については、次の場合を除くほか、取得、利用又は第三者提供を行わない。

① 適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲でセンシティブ情報を取得する場合

② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を取得する場合

③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属又は加盟に関する従業員等のセンシティブ情報を取得する場合

④ 前各号のほか、金融分野における個人情報保護に関するガイドライン第５条第１項各号に掲げる場合

(2) センシティブ情報を、前項に掲げる場合に取得、利用、又は第三者提供する場合には、同項に掲げる事由を逸脱した取得、利用又は第三者提供を行うことのないよう、特に慎重に取り扱うこととする。なお、センシティブ情報を第三者へ提供するに当たっては、オプトアウトを用いてはならない。

3.4 クレジットカード情報の取扱い個人情報のうち、クレジットカード番号、クレジットカード有効期限、クレジットカード名義人氏名、セキュリティコード（以下、クレジットカード情報といいます）については、保険代理店業務を遂行するうえで、取り扱ってはならない

3.5 基礎年金番号の取扱い

個人情報のうち、年金加入記録を管理するため日本年金機構から払出される 10 桁の固有の番号（以下、基礎年金番号といいます）については、保険代理店業務を遂行するうえで、取り扱ってはならない。

3.6 個人番号（マイナンバー）の取扱い

個人情報のうち、「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（以下「番号法」という）」第 2 条 5 項が定める住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるもの（以下、個人番号といいます）については、保険代理店業務を遂行するうえで、取り扱ってはならない。

3.7 個人情報の取得

3.7.1 適正な取得

個人情報は、偽りその他不正の手段により取得してはならない。

第三者から個人情報を取得するに際しては、本人の利益の不当な侵害を行ってはならず、個人情報の不正取得等の不当な行為を行っている第三者から、当該情報が漏えいされた個人情報であること等を知った上で当該情報を取得してはならない。

3.7.2 取得に際しての利用目的の通知

(1) 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に記載された個人情報を取得する場合は、あらかじめ利用目的を明示する。ただし、次の事項に該当する場合はこの限りでない。

① 本人又は第三者の生命、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 当社の権利又は正当な利益を害するおそれがある場合
③ 国の機関又は地方公共団体が法令の定める事務の遂行に支障を及ぼすおそれがある場合
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

4. 個人データ管理

4.1 個人データの正確性の確保

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よう努める。

4.2 安全管理措置

取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規程等の整備及び安全管理措置に係る実施体制の整備等の必要かつ適切な措置を講じる。

4.2.1 個人データの安全管理に係る基本方針の整備

次の内容・方法に関する記載を含む「個人データの安全管理に係る基本方針（プライバシーポリシー)」を策定・公表し、必要に応じて、見直しを行う。

(1) プライバシーポリシーに盛り込む内容

① 代理店名

② 個人情報保護への取組方針の宣言

（個人データの安全管理に関する宣言、基本方針の継続的改善の宣言、関係法令等遵守の宣言、個人情報を目的外に利用しないこと、苦情処理に適切に取り組むこと等)

③ 諸手続きの説明

(利用目的の通知・公表等の手続き、開示等に関する手続き等の分かりやすい説明)

④ 個人情報の取扱いに関する質問及び苦情処理の窓口についての説明

(2) 公表方法

① インターネットのホームページ上での常時掲載

② 事務所の窓口等でのポスターの常時掲載

③ チラシ等の常時備付け

4.2.2 個人データの安全管理措置に係る実施体制の整備

4.2.2.1 実施体制の整備に関する組織的安全管理措置

4.2.2.1.1 個人データ管理責任者等の設置

(1) 次に掲げる役職者を設置する。

① 個人データの安全管理に係る業務遂行の総責任者である個人データ管理責任者

② 個人データを取り扱う各部署における個人データ管理者

(2) 個人データ取扱部署が単一である場合等、個人データ管理責任者による全体管理が可能な場合は個人データ管理責任者と個人データ管理者は兼務することができる。

(3) 個人データ管理責任者は取締役又は執行役等の業務執行に責任を有する者を任命する。

(4) 各役職者の役割は次の通りとする。

① 個人データ管理責任者

ａ．個人データ管理について定めた社内規則等及び委託先の選定基準の承認及び周知

ｂ．個人データ管理者及び個人データの利用者の識別・認証に関する機能の管理者の任命

ｃ．個人データ管理者からの報告徴収及び助言・指導
ｄ．個人データの安全管理に関する教育・研修の企画
ｅ．その他代理店全体における個人データの安全管理に関する業務

② 個人データ管理者
ａ．個人データの取扱者の指定及び変更等の管理
ｂ．個人データの利用申請の承認及び記録等の管理
ｃ．個人データを取り扱う保管媒体の設置場所の指定及び変更等
ｄ．個人データの管理区分及び権限についての設定及び変更の管理
ｅ．個人データの取扱状況の把握
ｆ．委託先における個人データの取扱状況等の監督
ｇ．個人データの安全管理に関する教育・研修の実施
ｈ．個人データ管理責任者に対する報告
ｉ．その他所管部署における個人データの安全管理に関する業務

4.2.2.1.2 就業規則等における安全管理措置の整備

次の事項を就業規則等に定めるとともに、従業者の採用時及び退職時に、個人データの非開示契約等の締結を行う。

(1) 個人データの取扱いに関する従業者の役割・責任
(2) 違反時の懲戒処分

4.2.2.1.3 個人データの安全管理に係る社内規則等に従った運用

個人データの安全管理に係る社内規則等に従った体制を整備し、当該社内規則等に従った運用を行うとともに、当該社内規則等に規定する事項の遵守状況の記録及び確認を行う。

4.2.2.1.4 個人データの取扱状況を確認できる手段の整備

(1) 次の事項を含む「個人データ管理台帳」を整備し、取扱状況を管理する。
① 取得項目
② 利用目的
③ 保管場所・保管方法・保管期限
④ 管理部署
⑤ アクセス制御の状況
(2) 個人データ管理台帳に記載されている個人データ等について、記載通りに管理されているか定期的（半年に 1 回以上）に点検（棚卸し）を実施し、その履歴を残す。

4.2.2.1.5 個人データの取扱状況の点検及び監査体制の整備と実施

(1)「個人データの取扱状況の点検・監査に関する規則」に基づき、次の事項を実施する。
① 個人データを取り扱う部署における点検体制の整備と定期的及び臨時の点検
② 上記部署以外の者による監査体制の整備と定期的及び臨時の監査

(2) 個人データ取扱部署が単一の場合は、点検により監査を代替することも認められる。
(3) 点検実施にあたっては、次の体制を整備する。
① 点検責任者・点検担当者の選任
② 点検計画の策定
③「-点検シート」等を作成・利用した自主点検体制の整備
(4) 個人データ取扱部署が単一の場合等において、点検責任者による全社の点検が可能な場合は点検責任者と点検担当者を同一とすることができる。
(5) 点検実施後、万一個人データ管理について定めた社内規則等の違反事項等を発見した場合は速やかに改善する。
(6) 監査実施にあたっては、次の体制を整備する。
① 監査責任者・監査担当者の選任（監査の対象となる個人データを取り扱う担当者・部署以外）
② 監査計画の策定
③ 監査体制の整備
(7) 監査責任者・担当者・部署が監査業務等により個人データを取り扱う場合には、当該監査責任者・担当者・部署における個人データの取扱いについて、個人データ管理責任者が特に任命する者がその監査を実施する。
(8) 監査対象被監査部署が少なく、一名のみで監査が完結することが可能な場合は、監査責任者と監査担当者は同一とすることができる。
(9) 個人データ取扱部署が単一の場合等において、点検により監査を代替することができる。
(10) 監査実施後において、個人データ管理について定めた社内規則等の違反事項等を把握した場合は、速やかに改善を行う。

4.2.2.1.6 漏えい事案等に対応する体制の整備

(1)「漏えい事案等」とは、個人情報が記載・収録された帳票や電子記録媒体（FD、CD-ROM等）の盗難又は紛失、郵便物の誤送付、電子メールやファックスの誤送信等の事故により、個人情報の漏えい、滅失又はき損が生じ、又は生じるおそれが高い場合をいう。
(2) 漏えい事案等の発生に備え、次の体制を整備する。
① 対応部署
② 漏えい事案等の影響・原因等に関する調査体制
③ 再発防止策・事後対策の検討体制
④ 自社内外への報告体制
(3) 漏えい事案等が発生した場合、次の事項を実施しなければならない。
① 監督当局等への報告
② 本人への通知等
③ 二次被害の防止・類似事案の発生回避等の観点からの漏えい事案等の事実関係及び再発防止策等の早急な公表
(4) 保険代理店業務に関連し、お客様の個人情報の漏えい事案等が発生した場合、又はその疑いがある場合には、直ちに保険会社へ連絡する。

4.2.2.2 実施体制の整備に関する人的安全管理措置

4.2.2.2.1 従業者との個人データの非開示契約等の締結

従業者による個人データの漏えい・紛失等を防止するため、次の事項を実施する。

① 採用時及び退職時における個人データの非開示契約等の締結
② 非開示契約等に違反した場合における懲戒処分の就業規則等への規定
③ 従業者が退職等をした場合、従業者が利用する機器・電子記録媒体等の回収又は、当該機器・電子記録媒体等に含まれる個人データの削除を行い、証跡を残す。

4.2.2.2.2 従業者の役割・責任等の明確化

個人データの取扱いにおける従業者の役割・責任等を明確にするため、次の事項を実施する。

① 各管理段階における個人データの取扱いに関する従業者の役割・責任の明確化
② 個人データの管理区分及びアクセス権限の設定
③ 違反時の懲戒処分を定めた就業規則等の整備
④ 必要に応じた規則等の見直し
⑤ 担当変更や代理店の組織変更等により、従業者の役割・責任等に変更が生じた場合における、新たな役割・責任等の速やかな決定

4.2.2.2.3 従業者への安全管理措置の周知徹底、教育及び訓練

従業者に対する安全管理措置を周知するため、次の事項を実施する。

① 採用時及び採用後の定期的（年 1 回以上）な個人データの安全管理措置に関する教育・訓練の実施
② 個人データ管理責任者及び個人データ管理者に対する教育・訓練
③ 個人データ管理について定めた社内規則等の違反行為等に対する就業規則等に基づく懲戒処分の周知
④ 従業者に対する教育・訓練の評価及び定期的な見直し

4.2.2.3 実施体制の整備に関する技術的安全管理措置

4.2.2.3.1 個人データの利用者の識別及び認証

(1)「個人データの利用者の識別及び認証」として、次の措置を講じる。
　① パスワードの設定
　② パスワードの定期的な変更
　③ パスワードが他人に知られないような厳重な管理
　④ ユーザーID の共有及び貸し借りの原則禁止

(2) やむを得ず、システムを所管する責任者の許諾を受けた上で、ユーザーID の共有、貸し借りをしている場合には、記録簿の作成等により、使用者を明確にする。

(3) 上記（1）（2）の対応は、システム管理者等特別な権限を有するユーザーにも適用する。

4.2.2.3.2 個人データの管理区分の設定及びアクセス制御

(1)「個人データの管理区分の設定及びアクセス制御」として、次の措置を講じる。

① 機器や電子記録媒体に保存した電子データ等には、アクセス権限に応じたパスワードを設定する。

② 業務上で利用する機器等には、ファイル共有・ファイル交換ソフトのインストールを禁止する。

③ 私的に利用している機器等、または社外から持ち込まれた機器等や電子記録媒体は、原則業務で使用しない。

ただし、管理者が業務上の必要性を認めた上で利用する場合は、不正アクセス等に対応するため、以下を実施する。

-利用する際は管理者の承認を得る

-パスワードの設定やファイル交換ソフトの導入等の技術的な安全管理措置を講じる

-業務の担当変更、退職等により従業者が保険代理店業務に従事しなくなった場合は、従業者が利用していた機器等の回収又は、当該機器等に含まれる個人データの削除を行い、証跡を残す

④ 社外インターネットに接続された機器等で個人データを取り扱う場合は、外部からの不正アクセスに対応するための措置を講じる。

（例）利用しているインターネットサービスプロバイダや、ウィルスソフトに備わっている不正アクセス遮断サービス（ファイアーウォール）又は機能を利用する。

4.2.2.3.3 個人データへのアクセス権限の管理

「個人データへのアクセス権限の管理」として、次の措置を講じる。

① 長期間使用しないユーザーIDを削除する。

② 従業者が異動、退職した際は直ちにユーザーIDの削除、又は権限の変更を行う。

③ ユーザーID及び従業者のアクセス権限の定期的な棚卸しを行う。

④ 従業者に付与するアクセス権限を最小限に限定する。

4.2.2.3.4 個人データの漏えい・き損等防止策

「個人データの漏えい・き損等防止策」として、次の個人データの保護策を講ずることとともに、障害発生時の技術的対応・復旧手続を整備する。

① ウィルス対策ソフトを導入し、最新の状態に保つ。

② メールを利用して個人データを伝送するときは、暗号化又はパスワード設定をする。

③ 電子記録媒体（USBメモリ、CD-R等）を利用するときは、個人データの暗号化又はパスワード設定をする。

④ 電子記録媒体（USBメモリ、CD-R等）使用後は、速やかに個人データの消去・廃棄を行う。

⑤ 事故発生時の責任者（対応部署）を定める。

4.2.2.3.5 個人データへのアクセス記録及び分析

(1)「 個人データへのアクセス記録及び分析」として、次の措置を講じる。

① 個人データの種類や形態等に応じて、送付・受領履歴、「個人データ管理台帳」等により、個人データへのアクセス状況及び操作内容を記録する。

② 必要に応じて、記録されたアクセス記録・操作記録を確認する。

③ 不正が疑われる異常な記録の存否を定期的に確認する。

4.2.2.3.6 個人データを取り扱う情報システムの稼動状況の記録及び分析

(1)「 個人データを取り扱う情報システムの稼働状況の記録及び分析」として、次の措置を講じる。

① 個人データを取り扱う情報システムを利用している場合、漏えい等につながる可能性のある機能、操作等を把握する。

② 漏えい等につながる可能性のある機能、操作等がある場合、個人データのダウンロード等情報システムの稼働・利用状況について記録し、必要に応じて、状況を確認する。

4.2.2.3.7 個人データを取り扱う情報システムの監視及び監査

(1)「個人データを取り扱う情報システムの利用状況、個人データへのアクセス状況及び情報システムへの外部からのアクセス状況を監視するとともに、当該監視状況について点検及び監査を行う。

4.3 従業者の監督

(1) 個人データの安全管理が図られるよう、適切な内部管理体制を構築し、その従業者に対する必要かつ適切な監督を行う。

(2) 従業者とは、組織内にあって直接又は間接に当社の指揮監督を受けて当社の業務に従事している者をいい、雇用関係にある従業者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、当社との間の雇用関係にない者（取締役、執行役、理事、監査役、監事、派遣社員等）も含まれる。

(3) 従業者に対し必要かつ適切な監督を行うため、「4.2.2.2 実施体制の整備に関する人的安全管理措置」に規定された体制整備等を行う。

4.4 委託先の監督

個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、附則「個人データの外部委託に関する規則」に定められた事項を遵守し、委託を受けた者に対する必要かつ適切な監督を行う。

4.5 第三者提供の制限

(1) 次の場合を除くほか、あらかじめ本人に同意を得ることなく、個人データを第三者に提供してはならない。

① 法令に基づく場合

② 人の生命、身体又は財産（法人の財産を含む）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場合

③ 公衆衛生の向上又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場合

④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務の遂行に支障を及ぼすおそれがある場合

(2) 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 個人情報取扱事業者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又は一部を委託する場合

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 個人データを特定の者との間で共同して利用する場合であって、その旨並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及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いている場合

5. 開示・訂正・利用停止等の請求の対応

5.1 開示

(1) 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、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法があるときは、当該方法）により、遅滞なく、保有個人データを開示する。ただし、次のいずれかに該当する場合には、その全部又は一部を開示しないことができる。

① 本人又は第三者の生命、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 当社の業務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) 求められた保有個人データの全部又は一部について開示しない旨の決定をしたとき又は開示等の求めの対象となっている保有個人データが存在しないときは、本人に対し、遅滞なく、その旨を通知する。また、その決定の理由について、根拠とした法の条文及び判断の基準となる事実を示して遅滞なく説明を行うこととする。なお、本人に対して通知するまでの期間は、開示等の求めに対し、その到達した日から 2 週間以内とする。

(3) 保険代理店業務に関連し、本人から、当該本人が識別される保険会社の保有個人データの開示を求められたときは、直ちに保険会社へ連絡し、その指示に従い対応を行う。

5.2 訂正等

(1) 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内容の訂正、追加又は削除（以下「訂正等」といいます）を求められた場合には、利用目的の達成に必要な範囲内において、遅滞なく、事実の確認等の必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行う。

(2) 訂正等を行った場合、又は訂正等を行わないこととした場合は、本人に対し、遅滞なくその旨（訂正等を行った場合は、その内容を含む）を通知する。なお、訂正等を行わない場合は、訂正等を行わない根拠及びその根拠となる事実を示し、その理由を説明することとする。なお、本人に対して通知するまでの期間は、開示等の求めに対し、その到達した日から 2 週間以内とする。

(3) 保険代理店業務に関連し、本人から、当該本人が識別される保険会社の保有個人データの訂正等を求められた場合には、直ちに保険会社へ連絡し、その指示に従い対応を行う。

5.3 利用停止等

(1) 本人から、当該本人が識別される保有個人データが個人情報保護法第 16 条の規定に違反して取り扱われているという理由又は個人情報保護法第 17 条の規定に違反して取得されたものであ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又は消去（以下「利用停止等」といいます）を求められた場合であって、その求め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を行う。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等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) 本人から、当該本人が識別される保有個人データが個人情報保護法第 23 条第 1 項の規定に違反して第三者に提供され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への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止する。ただし、当該保有個人データの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第三者への提供を停止する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) 保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき又は保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止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（本人から求められた措置と異なる措置を行う場合には、その措置内容を含む）を通知する。なお、本人に対して通知するまでの期間は、開示等の求めに対し、その到達した日から 2 週間以内とする。

(4) 保険代理店業務に関連し、本人から、当該本人が識別される保険会社の保有個人データの利用停止等又は第三者への提供の停止を求められた場合には、直ちに保険会社へ連絡し、その指示に従い対応を行う。

6. 苦情処理

6.1 苦情の処理

(1) 個人情報の取扱いに関する苦情を受けたときは、その内容について調査し、合理的な期間内に、適切かつ迅速に処理する。

(2) 苦情処理手順の策定、苦情受付窓口の設置、苦情処理に当たる従業者への十分な教育・研修等、苦情処理を適切かつ迅速に行うために必要な体制を整備する。

(3) 保険代理店業務に関連し、個人情報の取扱いに関する苦情を受けたときは、直ちに保険会社へ連絡し、保険会社の指示に従い対応を行う。

取得・入力段階取扱規則

第1条（目的）

本規則は、当社における個人データの安全管理措置のうち、個人データの「取得・入力」段階の取扱いについて定めたものである。

第2条（定義）

1．「取得」とは、本人又は第三者から個人データを物理的又は電子的手段により取得すること等をいう（社内の他部署からの取得は含まない）。
2．「入力」とは、取得した個人データをデータベース等の情報システムに物理的及び電子的に入力すること等をいう。

第3条（取得・入力に関する取扱者の役割・責任及び取扱者の限定）

1． 個人データ管理責任者は、個人データの取得・入力に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2． 個人データ管理者は、各部署において業務上必要な者に限り個人データの取得・入力が行われるよう取扱者を限定しなければならない。

第4条（センシティブ情報の取得・入力に関する取扱者の限定）

個人データ管理者は、個人情報のうち、人種、信条、門地、本籍地、社会的身分、保健医療、労働組合への加盟、性生活、犯罪経歴、犯罪により害を被った事実、被疑者又は被告人としての刑事事件に関する手続が行われた事実、少年の保護事件に関する手続が行われた事実（以下「センシティブ情報」といいます）の取得・入力の取扱者を必要最小限に限定しなければならない。

第5条（取得・入力の対象となる個人データの限定）

個人データ管理者は、取得・入力する個人データを業務上必要な範囲内のものに限定しなければならない。

第6条（取得・入力時の照合及び確認手続き）

1． 個人データの取扱者は、個人データを取得するときには、情報提供者の本人確認及び権限等の確認を行わなければならない。
2． 個人データの取扱者は、個人データを入力するときには、入力データが正確であることを確認しなければならない。

第 7 条（取得・入力の規則外作業に関する申請及び承認手続き）

個人データの取扱者は、本規則に定める以外の方法で個人データを取得・入力する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第 8 条（機器・電子記録媒体等の管理手続き）

１． 個人データ管理者は、取得・入力した個人データが保存された機器・電子記録媒体等の設置場所の指定ならびに管理区分及び権限の設定をし、必要に応じて、変更しなければならない。
２． 個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・電子記録媒体等を適切に保管･保存しなければならない。

第 9 条（個人データへのアクセス制御）

個人データ管理者は、取得・入力した個人データへのアクセスを制御するために、個人データが記載された文書や個人データが保存された機器・電子記録媒体等に関して次の措置を講じなければならない。
① 個人データが記載された文書及び個人データが保存された機器・電子記録媒体等を施錠管理する、又は保管するスペースへの部外者の立ち入りを制限する。
② 機器や電子記録媒体等に保存した個人データには、パスワードを設定する。
③ 郵便物や FAX 等により取得した個人データについても適切な管理を行う。

第 10 条（取得・入力状況の記録及び分析）

１． 個人データの取扱者は、個人データを取得・入力する場合、情報の種類や形態等に応じて、受領履歴、「個人データ管理台帳」等により、適切に取得・入力状況について記録を行わなければならない。
２． 個人データ管理者は、個人データの漏えい等の防止のため、必要に応じて、記録された状況を確認する。

第 11 条（センシティブ情報の取得の制限）

個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、取得してはならない。
① 適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲でセンシティブ情報を取得する場合
② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を取得する場合
③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属又は加盟に関する従業員等のセンシティブ情報を取得する場合
④ 前各号のほか、金融分野における個人情報保護に関するガイドライン第 5 条第１項各号に掲げる場合

第 12 条（センシティブ情報の取得に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項）

１．　個人データの取扱者は、前条第１号に基づきセンシティブ情報を取得する場合には、当該センシティブ情報を保険業の適切な業務運営を確保する必要性から、本人の同意（原則として書面による）に基づき業務遂行上必要な範囲で取得しなければならない。

２．　個人データの取扱者は、前項において本人の同意に基づかない場合には、当該センシティブ情報を取得してはならない。

３．　個人データの取扱者は、郵送等により取得した個人データが含まれる文書等にセンシティブ情報が含まれている場合は、原則として、本人の指定した方法により、当該情報を速やかに本人に返却又は廃棄する。

ただし、当該文書等に記載された他の情報が業務遂行上必要な場合、個人データの取扱者は、直ちに当該センシティブ情報の記載部分を判読不能な状態にして取得するものとする。

利用・加工段階取扱規則

第1条（目的）

本規則は、当社における個人データの安全管理措置のうち、個人データの「利用・加工」段階の取扱いについて定めたものである。

第2条（定義）

1．「利用」とは、個人データを利用目的の範囲内で取り扱うこと等をいう。
2．「加工」とは、個人データの更新を行うこと、又は個人データを利用し、新たなデータベースを作成すること等をいう。
3．「管理区域」とは、事業者の敷地内をいう。

第3条（利用・加工に関する取扱者の役割・責任及び取扱者の限定）

1． 個人データ管理責任者は、個人データの利用・加工に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2． 個人データ管理者は、各部署において、業務上必要な者に限り個人データの利用・加工が行われるよう取扱者を限定しなければならない。

第4条　センシティブ情報の利用・加工に関する取扱者の限定

個人データ管理者は、個人情報のうち、人種、信条、門地、本籍地、社会的身分、保健医療、労働組合への加盟、性生活、犯罪経歴、犯罪により害を被った事実、被疑者又は被告人としての刑事事件に関する手続が行われた事実、少年の保護事件に関する手続が行われた事実（以下「センシティブ情報」といいます）の利用・加工の取扱者を必要最小限に限定しなければならない。

第5条　利用・加工の対象となる個人データの限定

個人データ管理者は、利用・加工する個人データを業務上必要な範囲内のものに限定しなければならない。

第6条　利用・加工時の照合及び確認手続き

1． 個人データの取扱者は、利用する個人データが対象データとして正しいかについて確認しなければならない。
2． 個人データの取扱者は、利用する個人データが正しく加工されたかについて元データと照合する等の措置を講じなければならない。

第 7 条　利用・加工の規則外作業に関する申請及び承認手続き

個人データの取扱者は、本規則に定める以外の方法で個人データを利用・加工する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第 8 条　機器・電子記録媒体等の管理手続き

1．個人データ管理者は、利用・加工する個人データが保存された機器・電子記録媒体等の設置場所の指定ならびに管理区分及び権限の設定をし、必要に応じて、変更しなければならない。
2．個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・電子記録媒体等を適切に保管・保存しなければならない。

第 9 条　個人データへのアクセス制御

1．　個人データ管理者は、利用・加工する個人データへのアクセスを制御するために、個人データが記載された文書や個人データが保存された機器・電子記録媒体等に関して次の措置を講じなければならない。
　① 個人データが記載された文書及び個人データが保存された機器・電子記録媒体等を施錠管理する、又は保管するスペースへの部外者の立ち入りを制限する。
　② 機器や電子記録媒体等に保存した個人データには、パスワードを設定する。
2．　個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の利用・加工を認めた必要最小限の取扱者により利用・加工が行われるようユーザーID 及びパスワードを付与すると共に、ユーザーID 及びパスワードの管理を徹底しなければならない。

第 10 条　利用・加工状況の記録及び分析

1．個人データの取扱者は、個人データを利用・加工する場合、情報の種類や形態等に応じて、送付・受領履歴、「個人データ管理台帳」等により、適切に利用・加工状況について記録を行わなければならない。
2．個人データ管理者は、個人データの漏えい等の防止のため、必要に応じて、記録された状況を確認する。

第 11 条　センシティブ情報の利用・加工の制限

個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、利用・加工してはならない。

① 保険業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲でセンシティブ情報を利用・加工する場合
② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を利用・加工する場合
③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属又は加盟に関する従業員等のセンシティブ情報を利用・加工する場合
④ 前各号のほか、金融分野における個人情報保護に関するガイドライン第 5 条第１項各号に掲げる場合

第 12 条　センシティブ情報の利用に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項

１．個人データの取扱者は、前条①に基づきセンシティブ情報を利用する場合には、当該センシティブ情報を保険業の適切な業務運営を確保する必要性から、本人の同意（原則として書面による）に基づき業務遂行上必要な範囲で利用しなければならない。
２．個人データの取扱者は、前項において本人の同意に基づかない場合には、当該センシティブ情報を利用してはならない。

第 13 条　個人データの管理区域外への持ち出しに関する措置

１．個人データ管理責任者は、個人データの管理区域外への持ち出しに関する取扱者の役割・責任を定め、組織内に周知しなければならない。
２．個人データ管理者は、個人データの管理区域外への持ち出しに関する取扱者を必要最小限に限定しなければならない。
３．個人データ管理者は、管理区域外に持ち出すことが可能な個人データを業務上必要最小限の範囲に限定しなければならない。
４．個人データ管理者は、個人データの管理区域外への持ち出しに際し、個人データを持ち出す者が第２項で限定された取扱者本人であることを確認しなければならない。
　又、個人データ管理者は、持ち出す個人データが第３項により持ち出すことを限定した個人データの範囲内であるか確認しなければならない。
５．個人データの取扱者は、個人データを管理区域外に持ち出す場合には、個人データ管理者に申請し、承認を得たうえで行わなければならない。
６．個人データの取扱者は、個人データを管理区域外に持ち出す場合には、必要最小限の件数等に限ると共に、持ち出した個人データを常時携行する等適切に管理しなければならない。
７．個人データの取扱者は、個人データを管理区域外に持ち出す場合には、データの種類や形態等に応じて、必要かつ適切に持ち出した個人データの状況について報告及び記録を行わなければならない。
　個人データ管理者は、個人データの漏えい等の防止のため、必要に応じて、報告及び記録された状況を確認する。

第 14 条　個人データの利用者の識別及び認証

個人データ管理者は、パスワードの設定等個人データを利用・加工する取扱者の識別及び認証機能を設けなければならない。

第 15 条　個人データの管理区分の設定及びアクセス制御

個人データ管理者は、個人データの利用・加工段階において、例えば次のような管理区分の設定及びアクセス制御に関する機能を設けなければならない。

① 個人データが記載された文書や個人データが保存された機器・電子記録媒体等について、施錠管理等により、事業者内部における権限外者のアクセスを制御する。

② 機器や電子記録媒体等に保存した個人データには、部署や役割毎にアクセス権限に応じたパスワードを設定する。

③ 個人データが記載された文書や個人データが保存された機器・電子記録媒体等を保管するスペースへの部外者の立ち入りを制限する。

２． 個人データ管理者は、前項のアクセス制御機能の設定にあたっては、センシティブ情報の利用・加工の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第 16 条　個人データへのアクセス権限の管理

１． 個人データ管理者は、利用・加工段階における個人データのアクセス権限管理として、例えば次のような措置を講じなければならない。

(1) ① 機器や電子記録媒体等に保存した個人データに対して、管理区分に応じた適切なパスワードを設定する。

② 機器や電子記録媒体等に保存した個人データに設定されたパスワードを知る従業者を必要最小限に限定する。

③ 機器や電子記録媒体等に保存した個人データに設定されたパスワードの見直し、及び開示者の見直しを行う。

２． 個人データ管理者は、前項のアクセス権限に関する機能の設定にあたっては、センシティブ情報の利用・加工の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第 17 条　個人データの漏えい・き損等防止策

個人データ管理者は、個人データの利用・加工段階における漏えい・き損等の防止策を講じなければならない。

第 18 条　個人データへのアクセス記録及び分析

１． 個人データ管理者は、個人データの種類や形態等に応じて、送付・受領履歴、「個人データ管理台帳」等により、個人データへのアクセス状況を記録する。

２． 個人データ管理者は、必要に応じて、前項に定める記録された状況を確認する。

第 19 条　個人データを取扱う情報システムの稼動状況の記録及び分析

１．個人データ管理者は、個人データを取り扱う情報システムを利用している場合、漏えい等につながる可能性のある機能、操作等を把握する。
２．個人データ管理者は、漏えい等につながる可能性のある機能、操作等がある場合、個人データのダウンロード等情報システムの稼働・利用状況について記録し、必要に応じて、状況を確認する。

保管・保存段階取扱規則

第1条　目的

本規則は、当社における個人データの安全管理措置のうち、個人データの「保管・保存」段階の取扱いについて定めたものである。

第2条　定義

1．「保管」とは、個人データを加工せず、オフィスフロア内に置き管理すること等をいう。
2．「保存」とは、個人データを加工せず、オフィスフロア外（書庫等）に置き廃棄に至るまで管理すること、及び機器や電子記録媒体等に電子データを格納し消去にいたるまで管理すること（個人データのバックアップを含む）等をいう。

第3条　保管・保存に関する取扱者の役割・責任及び取扱者の限定

1．　個人データ管理責任者は、個人データの保管・保存に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2．　個人データ管理者は、各部署において、業務上必要な者に限り個人データの保管・保存が行われるよう取扱者を限定しなければならない。

第4条　センシティブ情報の保管・保存に関する取扱者の限定

個人データ管理者は、個人情報のうち、人種、信条、門地、本籍地、社会的身分、保健医療、労働組合への加盟、性生活、犯罪経歴、犯罪により害を被った事実、被疑者又は被告人としての刑事事件に関する手続が行われた事実、少年の保護事件に関する手続が行われた事実（以下「センシティブ情報」といいます）の保管・保存の取扱者を必要最小限に限定して定めなければならない。

第5条　保管・保存の対象となる個人データの限定

　個人データ管理者は、保管・保存する個人データを業務上必要な範囲内のものに限定しなければならない。

第6条　保管・保存の規則外作業に関する申請及び承認手続き

個人データの取扱者は、本規則に定める以外の方法で個人データを保管・保存する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第 7 条　機器・電子記録媒体等の管理手続き

１．　個人データ管理者は、「個人データ管理台帳」を踏まえ、個人データが保存された機器・電子記録媒体等の保管場所等の指定ならびに管理区分及び権限の設定をし、必要に応じて、変更しなければならない。
２．　個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・電子記録媒体等を適切に保管しなければならない。

第 8 条　個人データへのアクセス制御

１．　個人データ管理者は、保管・保存した個人データへのアクセスを制御するために、個人データが記載された文書や個人データが保存された機器・電子記録媒体等に関して次の措置を講じなければならない。
　① 個人データが記載された文書及び個人データが保存された機器・電子記録媒体等を施錠管理する、又は保管するスペースへの部外者の立ち入りを制限する。
　② 機器や電子記録媒体等に保存した個人データには、パスワードを設定する。
２．　個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の保管・保存を認めた必要最小限の取扱者により保管･保存が行われるようユーザーID 及びパスワードを付与すると共に、ユーザーID 及びパスワードの管理を徹底しなければならない。

第 9 条　保管・保存状況の記録及び分析

１．　個人データの取扱者は、個人データを保管・保存する場合、データの種類や形態等に応じて、適切に保管・保存状況について記録を行わなければならない。
２．　個人データ管理者は、個人データの漏えい等の防止のため、必要に応じて、前項の記録状況を分析する。

第 10 条　個人データに関する障害発生時の対応・復旧手続き

１．　個人データ管理者は、保管・保存した個人データについて、障害が発生した際に本人に継続的なサービスの提供が行えない場合、取扱者に対し定期的にバックアップ等を行うよう徹底する。
２．　個人データ管理者は、保管・保存した個人データに障害が発生した際には、必要に応じて、復旧させなければならない。
３．　個人データの取扱者は、作成したバックアップデータ等を適切に管理しなければならない。

第 11 条　個人データの利用者の識別及び認証

　個人データ管理者は、個人データを保管・保存する取扱者の識別及び認証機能を設けなければならない。

第 12 条　個人データの管理区分の設定及びアクセス制御

１．　個人データ管理者は、個人データの保管・保存段階において、例えば次のような管理区分の設定及びアクセス制御に関する機能を設けなければならない。

① 個人データが記載された文書や個人データ保存された機器・電子記録媒体等について、施錠管理等により、事業者内部における権限外者のアクセスを制御する。

② 機器や電子記録媒体等に保存した個人データには、部署や役割毎にアクセス権限に応じたパスワードを設定する。

③ 個人データが記載された文書や個人データが保存された機器・電子記録媒体等を保管・保存するスペースへの部外者の立ち入りを制限する。

２．　個人データ管理者は、前項のアクセス制御機能の設定にあたっては、センシティブ情報の保管・保存の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第 13 条　個人データへのアクセス権限の管理

１．　個人データ管理者は、保管・保存段階における個人データのアクセス権限管理として、例えば次のような措置を講じなければならない。

(1)　① 機器や電子記録媒体等に保存した個人データに対して、管理区分に応じた適切なパスワードを設定する。

② 機器や電子記録媒体等に保存した個人データに設定されたパスワードを知る従業者を必要最小限に限定する。

③ 機器や電子記録媒体等に保存した個人データに設定されたパスワードの見直し、及び開示者の見直しを行う。

２．　個人データ管理者は、前項のアクセス権限に関する機能の設定にあたっては、センシティブ情報の保管・保存の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第 14 条　個人データの漏えい・き損等防止策

個人データ管理者は、個人データの保管・保存段階における漏えい・き損等の防止策を講じなければならない。

第 15 条　個人データへのアクセス記録及び分析

１．　個人データ管理者は、個人データの種類や形態等に応じて、送付・受領履歴、「個人データ管理台帳」等により、個人データへのアクセス状況を記録する。

２．　個人データ管理者は、必要に応じて、記録されたアクセス状況を確認する。

第 16 条　個人データを取扱う情報システムの稼動状況の記録及び分析

１．個人データ管理者は、個人データを取り扱う情報システムを利用している場合、漏えい等につながる可能性のある機能、操作等を把握する。
２．個人データ管理者は、漏えい等につながる可能性のある機能、操作等がある場合、個人データのダウンロード等情報システムの稼働・利用状況について記録し、必要に応じて、状況を確認する。

移送・送信段階取扱規則

第1条　目的

本規則は、当社における個人データの安全管理措置のうち、個人データの「移送・送信」段階の取扱いについて定めたものである。

第2条　定義

1．「移送」とは、物理的な手段により個人データを異なる場所や人に移すこと等をいう。
2．「送信」とは、電子的な手段により個人データを異なる場所や人に移すこと等をいう。

第3条　移送・送信に関する取扱者の役割・責任及び取扱者の限定

1．個人データ管理責任者は、個人データの移送・送信に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2．個人データ管理者は、各部署において業務上必要な者に限り個人データの移送・送信が行われるよう取扱者を限定しなければならない。

第4条　センシティブ情報の移送・送信に関する取扱者の限定

個人データ管理者は、個人データのうち、人種、信条、門地、本籍地、社会的身分、保健医療、労働組合への加盟、性生活、犯罪経歴、犯罪により害を被った事実、被疑者又は被告人としての刑事事件に関する手続が行われた事実、少年の保護事件に関する手続が行われた事実（以下「センシティブ情報」といいます）の移送・送信の取扱者を必要最小限に限定して定めなければならない。

第5条　移送・送信の対象となる個人データの限定

個人データ管理者は、移送・送信する個人データを業務上必要な範囲内のものに限定しなければならない。

第6条　移送・送信時の照合及び確認手続き

個人データの取扱者は、個人データを移送・送信するときには、移送・送信先及び移送・送信物に相違がないか照合及び確認を行わなければならない。

第7条　移送・送信の規則外作業に関する申請及び承認手続き

個人データの取扱者は、本規則に定める以外の方法で個人データを移送・送信する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第 8 条　個人データへのアクセス制御

1．個人データ管理者は、移送・送信する個人データへのアクセスを制御するために、個人データが記載された文書や個人データが保存された機器・電子記録媒体等に関して次の措置を講じなければならない。
   ① 個人データが記載された文書及び個人データが保存された機器・電子記録媒体等を施錠管理する、又は保管するスペースへの部外者の立ち入りを制限する。
   ② 機器や電子記録媒体等に保存した個人データには、パスワードを設定する。
2．個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の移送・送信を認めた必要最小限の取扱者により移送・送信が行われるようユーザーID 及びパスワードを付与すると共に、ユーザーID 及びパスワードの管理を徹底しなければならない。

第 9 条　移送・送信状況の記録及び分析

1．個人データの取扱者は、個人データを移送・送信する場合、データの種類や形態等に応じて、適切に移送・送信状況について記録を行わなければならない。
2．　個人データ管理者は、個人データの漏えい等の防止のため、必要に応じて、記録された状況を確認する。

第 10 条　センシティブ情報の移送・送信の制限

個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、移送・送信してはならない。
① 保険業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲でセンシティブ情報を移送・送信する場合
② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を移送・送信する場合
③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属又は加盟に関する従業員等のセンシティブ情報を移送・送信する場合
④ 前各号のほか、金融分野における個人情報保護に関するガイドライン第 5 条第 1 項各号に掲げる場合

第 11 条　個人データに関する障害発生時の対応・復旧手続き

1．　個人データ管理者は、移送・送信する個人データについて、障害が発生した際に本人に継続的なサービスの提供が行えない場合、取扱者に対し定期的にバックアップ等を行うよう徹底する。
2．　個人データ管理者は、移送・送信した個人データに障害が発生した際には、必要に応じて、復旧させなければならない。
3．　個人データの取扱者は、作成したバックアップデータ等を適切に管理しなければならない。

第 12 条　個人データの利用者の識別及び認証

個人データ管理者は、個人データを移送・送信する取扱者の識別及び認証機能を設けなければならない。

第 13 条　個人データの管理区分の設定及びアクセス制御

1．　個人データ管理者は、個人データの移送・送信段階において、例えば次のような管理区分の設定及びアクセス制御に関する機能を設けなければならない。
　① 個人データが記載された文書や個人データが保存された機器・電子記録媒体等について、施錠管理等により、事業者内部における権限外者のアクセスを制御する。
　② 機器や電子記録媒体等に保存した個人データには、部署や役割毎にアクセス権限に応じたパスワードを設定する。
　③ 個人データが記載された文書や個人データが保存された機器・電子記録媒体等を保管するスペースへの部外者の立ち入りを制限する。
2．　個人データ管理者は、前項のアクセス制御機能の設定にあたっては、センシティブ情報の移送・送信の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第 14 条　個人データへのアクセス権限の管理

1．　個人データ管理者は、個人データの移送・送信段階におけるアクセス権限管理として、例えば次のような措置を講じなければならない。
(1)　① 機器や電子記録媒体等に保存した個人データに対して、管理区分に応じた適切なパスワードを設定する。
　② 機器や電子記録媒体等に保存した個人データに設定されたパスワードを知る従業者を必要最小限に限定する。
　③ 機器や電子記録媒体等に保存した個人データに設定されたパスワードの見直し、及び開示者の見直しを行う。

2．　個人データ管理者は、前項のアクセス権限に関する機能の設定にあたっては、センシティブ情報の移送・送信の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第 15 条　個人データの漏えい・き損等防止策

個人データ管理者は、個人データの移送・送信段階における漏えい・き損等の防止策を講じなければならない。

第 16 条　個人データへのアクセス記録及び分析

個人データ管理者は、個人データの移送・送信段階におけるアクセス記録を取得し、必要な期間保管･保存するとともに、個人データの漏えい等の防止のため、必要に応じて、これを分析しなければならない。

消去・廃棄段階取扱規則

第1条　目的

本規則は、当社における個人データの安全管理措置のうち、個人データの「消去・廃棄」段階の取扱いについて定めたものである。

第2条　定義

1．「消去」とは、個人データが保存されている媒体の個人データを電子的な方法その他の方法により削除すること等をいう。
2．「廃棄」とは、個人データが保存されている媒体を物理的に廃棄すること等をいう。

第3条　消去・廃棄に関する取扱者の役割・責任及び取扱者の限定

1．個人データ管理責任者は、個人データの消去・廃棄に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2．個人データ管理者は、業務上必要な者に限り個人データの消去・廃棄が行われるよう取扱者を限定しなければならない。

第4条　センシティブ情報の消去・廃棄に関する取扱者の限定

個人データ管理者は、個人データのうち、人種、信条、門地、本籍地、社会的身分、保健医療、労働組合への加盟、性生活、犯罪経歴、犯罪により害を被った事実、被疑者又は被告人としての刑事事件に関する手続が行われた事実、少年の保護事件に関する手続が行われた事実（以下「センシティブ情報」といいます）の消去・廃棄の取扱者を必要最小限に限定して定めなければならない。

第5条　消去・廃棄時の照合及び確認手続き

1．個人データの取扱者は、個人データの消去・廃棄に際し、消去・廃棄する個人データについて、「個人データ管理台帳」等により保管･保存期間を照合又は消去・廃棄理由を確認のうえ、消去・廃棄しなければならない。
2．個人データの取扱者は、個人データを消去・廃棄する際には、当該データが保存されている機器・電子記録媒体等の性質に応じ適正な方法で消去・廃棄しなければならない。

第6条　消去・廃棄の規則外作業に関する申請及び承認手続き

個人データの取扱者は、本規則に定める以外の方法で個人データを消去・廃棄する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第 7 条　機器・電子記録媒体等の管理手続き

1．個人データ管理者は、消去・廃棄する個人データが保存された機器・電子記録媒体等の設置場所の指定ならびに管理区分及び権限の設定をし、必要に応じて、変更しなければならない。
2．個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・電子記録媒体等を適切に保管･保存しなければならない。

第 8 条　個人データへのアクセス制御

個人データ管理者は、消去・廃棄する個人データへのアクセスを制御するために、個人データが記載された文書や個人データが保存された機器・電子記録媒体等に関して次の措置を講じなければならない。

① 個人データが記載された文書及び個人データが保存された機器・電子記録媒体等を施錠管理する、又は保管するスペースへの部外者の立ち入りを制限する。
② 機器や電子記録媒体等に保存した個人データには、部署や役割毎にアクセス権限に応じたパスワードを設定する。

第 9 条　消去・廃棄状況の記録及び分析

1．個人データの取扱者は、個人データを消去・廃棄する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に消去・廃棄状況について記録を行わなければならない。
2．個人データ管理者は、個人データの漏えい等の防止のため、必要に応じて、記録された状況を確認する。

漏えい事案等対応規則

第１条　目的

本規則は、当社における個人データの安全管理措置のうち、個人情報の漏えい事案等への対応の段階における取扱いについて定めたものである。

第２条　定義

「漏えい事案等」とは、個人情報が記載・記録された文書や電子記録媒体（FD、CD-ROM 等）の盗難又は紛失、郵便物の誤送付、電子メールやファックスの誤送信等の事故により、個人情報の漏えい、滅失又はき損が生じ、又は生じるおそれが高い場合をいう。

第３条　漏えい事案等への対応に関する対応部署の役割・責任及び取扱者の限定

１．　個人データ管理責任者は、漏えい事案等への対応に関する対応部署（以下「対応部署」といいます）の役割・責任を定め、組織内に周知しなければならない。
２．　対応部署の個人データ管理者は、各部署において、業務上必要な者に限り漏えい事案等への対応が行われるよう取扱者を限定しなければならない。

第４条　漏えい事案等への対応の規則外作業に関する申請及び承認手続き

個人データの取扱者は、本規則に定める以外の方法で漏えい事案等に対応する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第５条　漏えい事案等の影響等に関する調査手続き

漏えい事案等が発生した部署の個人データ管理者は、個人データ管理責任者及び対応部署と連携のうえ漏えい等した個人情報の取扱状況の記録内容の分析を行い、漏えい等した個人情報の量、質、事故の原因、態様、被害の程度等の内容及び影響の調査を行うこととする。

第６条　再発防止策・事後対策の検討に関する手続き

漏えい事案等が発生した部署の個人データ管理者は、対応部署と協議のうえ、漏えい等した個人情報の取扱状況の記録内容の分析を踏まえた再発防止策・事後対策を策定し、個人データ管理責任者へ報告することとする。

第７条　報告に関する手続き

１．　漏えい事案等が発生した場合、発見者は、漏えい等した範囲の拡大防止等必要な措置をとると共に、直ちに対応部署に報告しなければならない。
２．　対応部署は、報告を受けた漏えい事案等について、直ちに保険会社に報告しなければならない。
３．　対応部署の個人データ管理者は保険会社の指示に従い、社外への報告等（警察への届出、本人への通知等、二次被害の防止・類似事案の発生回避の観点からの漏えい事案等の事実関係及び再発防止策の公表）の要否及びその方法について決定しなければならない。

第８条　漏えい事案等への対応記録及び分析

１．　対応部署の個人情報の取扱者は、漏えい事案等へ対応する場合、個人情報の種類や形態等に応じて、必要に応じ、かつ適切に漏えい事案等の状況について記録を行わなければならない。
２．　対応部署の個人データ管理者は、個人情報の漏えい等の防止のため、必要に応じて、記録された状況を確認する。

個人データの取扱状況の点検・監査に関する規則

第1条　目的

本規則は、当社における個人データの取扱状況に関する点検及び監査について定めたものである。

第2条　実施部署

1．　個人データ管理責任者は、個人データを取り扱う部署において個人データの点検に関する点検責任者及び点検担当者を選任し、当該部署が自ら点検を実施するよう指示しなければならない。
2．　点検責任者と点検担当者は兼務することができる。
3．　個人データ管理責任者は、監査を実施する部署を指定し、その部署から個人データの監査に関する監査責任者及び監査担当者を選任し、監査を実施するよう指示しなければならない。
　ただし、監査を実施する部署が個人データを取り扱うときには、個人データ管理責任者は、当該部署以外の部署から当該部署を監査する監査責任者及び監査担当者を選任しなければならない。

第3条　点検

1．　個人データ管理責任者は、個人データの取扱状況の点検に関する計画を立案し、点検責任者に対し、定期的及び臨時の点検を実施するよう指示しなければならない。
2．　点検担当者は、点検責任者の指示に基づいて確実に点検を実施しなければならない。
3．　点検担当者は、点検により個人データ管理について定めた社内規則等に違反する事項等を発見した場合には、点検責任者に報告しなければならない。
4．　点検責任者は、個人データ管理について定めた社内規則等に違反する事項について、個人データ管理責任者に報告すると共に個人データ管理責任者の指示を踏まえ、改善のための措置を講じなければならない。

第4条　監査

1．　監査責任者は、個人データの取扱状況の監査に関する計画を立案し、定期的及び臨時の監査を実施しなければならない。
2．　監査担当者は、監査責任者の指示に基づいて確実に監査を実施しなければならない。
3．　監査担当者は、監査により個人データ管理について定めた社内規則等に違反する事項等を発見した場合には、監査責任者に報告しなければならない。
4．　監査責任者は、個人データ管理について定めた社内規則等に違反する事項について、個人データ管理責任者に報告する。報告を受けた個人データ管理責任者は、個人データ管理者に対し、改善のための措置を講じるよう指示しなければならない。

個人データの外部委託に関する規則

第1条　目的

本規則は、当社による個人データの取扱いの委託について、個人データを適正に取扱っていると認められる者を選定すること、及び委託先における個人データに対する安全管理措置が図られることを確保するため定めたものである。

第2条　定義

1．「委託」とは、契約の形態や種類を問わず、当社が他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約の一切を含む。
2．「委託先」とは、当社が、個人データの取扱いの全部又は一部を第三者に委託する場合の当該第三者のことをいう。

第3条　委託にあたっての保険会社への申請及び承認

個人データ管理責任者は、個人データの委託にあたって、保険会社に申請し、承認を得なければならない。
ただし、保険会社が別に定める場合はこの限りではない。

第4条　取引の必要性・有用性の確認

個人データ管理者は、個人データの取扱いの委託を検討するにあたり、次の基準を基に事前に委託業務の必要性、取引の有用性・適否の確認を行う。

① 業務の必要性
　委託業務自体、会社として必要なものである
③　取引の有用性・適否の確認
　委託により得られる効果が、想定されるリスクやコストを十分に上回る見込みである

第5条　委託先選定の基準

1．個人データ管理者は、委託先を選定するにあたって、次の基準に基づき委託先を選定する。

① 確実に責務を履行しうる経営状態（財務状況）
　－ 資金繰りに不安な要素はない
　－ 株価の急落、格付けの引き下げ等の不安定な要素はない
　－ 万一損害等が発生した場合に、負担に耐え得る資力を有している
② 業務の履行・管理態勢
　－ 品質を確保したうえで、委託業務量、納期を遵守できる態勢である
　－ 過去に取引がある場合、業務の履行においてトラブルの発生がない

③ 情報取扱の管理態勢

(1) 委託先における個人データの安全管理に係る基本方針・取扱規程等の整備

－ 委託先における個人データの安全管理に係る基本方針が整備されている

－ 委託先における個人データの安全管理に係る取扱規程が整備されている

－ 委託先における個人データの取扱状況の点検及び監査に係る規程が整備されている

－ 委託先における外部委託に係る規程が整備されている

(2) 委託先における個人データの安全管理に係る実施体制の整備

－ 個人情報管理規則「6.1　実施体制の整備に関する組織的安全管理措置」、「6.2　実施体制の整備に関する人的安全管理措置」及び「6.3　実施体制の整備に関する技術的安全管理措置」に規定された事項が整備されており、委託先から再委託する場合の再委託先においても同様の整備がなされている

(3) 実績等に基づく委託先の個人データ安全管理上の信用度

－ 過去に個人情報の漏えい等の事故（当社個人情報だけでなく他社の個人情報含む）を発生させていない。漏えい等の事故が発生している場合は、再発防止策が適切にとられている

２．　個人データ管理責任者は、当該基準に準じた当社独自の基準を、必要に応じて、策定しなければならない。

３．　当社独自の基準を定めた場合には、個人データ管理責任者は定期的に基準の見直しを行わなければならない。

４．　個人データ管理責任者は基準を組織内に周知しなければならない。

第6条　委託契約

１．個人データ管理責任者は、選定した委託先との間で、次の安全管理に関する事項を盛り込んだ委託契約の締結等をしなければならない。

① 当社の委託先に対する監督及び監査報告徴収に関する権限

② 委託先における個人データの漏えい、盗用、改竄及び目的外利用の禁止

③ 再委託における条件

④ 漏えい等が発生した際の委託先の責任

⑤ 委託業務終了時における、委託した個人情報返却及び回収・廃棄

２．個人データ管理責任者は、委託契約に以下の内容を盛り込むよう努めるものとする。

①「再委託における条件」として、再委託の可否及び再委託を行うに当たっての委託元への文書による事前報告又は承認等

② 委託先において個人データを取り扱う者の氏名・役職又は部署名

３．個人データ管理責任者は、定期的に委託契約等に盛り込む安全管理に関する事項を見直さなければならない。

第７条　委託先における選定基準の遵守状況の確認

個人データ管理者は、委託契約締結後に委託先選定基準に定められた事項の委託先における遵守状況を定期的又は随時に確認するとともに、委託先が当該基準を満たしていない場合には、委託先に対して改善を求めなければならない。

第８条　委託先における委託契約上の安全管理措置の遵守状況の確認

個人データ管理者は、定期的又は随時に委託先における委託契約上の安全管理の遵守状況を確認するとともに、委託先が遵守していない場合には、委託先に対して改善を求めなければならない。

〈附則〉

２０２３年４月１日改定。