個人データの取扱いに関する規程

代理店名	畑田　玲子

取得・入力段階取扱規程

第１条　目的

本規程は、当事務所における個人データの安全管理措置のうち、個人情報の「取得・入力」段階の取り扱いについて定めたものである。

第２条　定義

１.「取得」とは、本人または第三者から個人情報を物理的および電子的手段により取得することなどをいう（社内の他部門からの取得は含まない）。
２.「入力」とは、取得した個人情報をデータベース等の情報システムに物理的および電子的に入力することなどをいう。

第３条　取得・入力に関する取扱者の役割・責任および取扱者の限定

１．個人データ管理責任者は、個人情報の取得・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情報の取得・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、政治的見解、信教（宗教、思想および信条をいう。）、労働組合への加盟、人種および民族、門地および本籍地、保健医療および性生活、ならびに犯罪歴に関する情報（以下、「センシティブ情報」という。）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・入力する個人情報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・入力時の照合および確認手続き

１．個人データの取扱者は、個人情報を取得するときには、情報提供者の本人確認およ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、個人情報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・入力の規程外作業に関する申請および承認手続き

個人データの取扱者は、本規程に定める以外の方法で個人情報を取得・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・記録媒体等の管理手続き

１．個人データ管理者は、取得・入力した個人情報が保存された機器・記録媒体等の設置場所の指定ならびに管理区分および権限の設定をし、必要に応じ変更しなければならない。
２．個人データの取扱者は、前項の指定および設定に従い、個人情報が保存された機器・記録媒体等を適切に保管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・入力した個人情報へのアクセスを制御するために、取得・入力した個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

① 個人情報の入力に必要なＩＤおよびパスワードの管理を徹底する。
② 個人情報が保存された機器・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。
③ 受信した郵便物やＦＡＸ等の個人情報について適切な管理を行う。

第１０条　取得・入力状況の記録および分析

１．個人データの取扱者は、個人情報を取得・入力する場合、情報の種類や形態等に応じて、必要に応じ、かつ適切に取得・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、個人情報の漏えい等の防止のため、必要に応じ、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・宗教等の団体もしくは労働組合への所属もしく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、金融庁ガイドライン第６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およ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もしくは廃棄する。

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・加工段階取扱規程

第１条　目的

本規程は、当事務所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」段階の取り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扱うことなどをいう。
２.「加工」とは、個人データの更新を行うこと、また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などをいう。
３.「管理区域」とは、営業範囲を勘案して予め指定した区域をいう。

第３条　利用・加工に関する取扱者の役割・責任および取扱者の限定

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、個人データのうち、政治的見解、信教（宗教、思想および信条をいう。）、労働組合への加盟、人種および民族、門地および本籍地、保健医療および性生活、ならびに犯罪歴に関する情報（以下、「センシティブ情報」という。）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・加工時の照合および確認手続き

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しなければならない。

第７条　利用・加工の規程外作業に関する申請および承認手続き

個人データの取扱者は、本規程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・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・記録媒体等の設置場所の指定ならびに管理区分および権限の設定をし、必要に応じ変更しなければならない。
２．個人データの取扱者は、前項の指定および設定に従い、個人データが保存された機器・記録媒体等を適切に保管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、利用・加工する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。
　①　個人データの利用・加工に必要なＩＤおよびパスワードの管理を徹底する。
　②　個人データが保存された機器・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、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・加工を認められた必要最小限の取扱者に限り利用・加工が行われるようＩＤおよびパスワードを付与すると共に、ＩＤおよ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・加工状況の記録および分析

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、データの種類や形態等に応じて、必要に応じ、かつ適切に取得・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、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・宗教等の団体もしくは労働組合への所属もしく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、金融庁ガイドライン第６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およ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。
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もしくは廃棄する。

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。

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。

また、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、別に定める件数等に限ると共に、個人データが保存された機器・媒体等を常時携行するなど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およ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、報告およ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および認証

個人データ管理者は、個人データを利用・加工する取扱者の識別およ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およびアクセス制御

1．個人データ管理者は、個人データの利用・加工段階における管理区分の設定およびアクセス制御機能を設けなければならない。
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、個人データの利用・加工段階におけるアクセス権限に関する機能を設けなければならない。
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および分析

個人データ管理者は、個人データの利用・加工段階におけるアクセス記録を取得し、必要な期間保管するとともに、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。

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および分析

個人データ管理者は、個人データの利用・加工段階におけるシステムの稼動状況に関し記録を取得し、必要な期間保管するとともに、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。

保管・保存段階取扱規程

第1条　目的

本規程は、当事務所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などをいう。
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、およびパソコンや電子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。）などをいう。

第3条　保管・保存に関する取扱者の役割・責任および取扱者の限定

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、個人データのうち、政治的見解、信教（宗教、思想および信条をいう。）、労働組合への加盟、人種および民族、門地および本籍地、保健医療および性生活、並びに犯罪歴に関する情報（以下、「センシティブ情報」という。）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・保存の規程外作業に関する申請および承認手続き

個人データの取扱者は、本規程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・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・記録媒体等の保管場所等の指定ならびに管理区分および権限の設定をし、必要に応じ変更しなければならない。
2．個人データの取扱者は、前項の指定および設定に従い、個人データが保存された機器・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．個人データ管理責任者は、保管・保存する個人データへのアクセスを制御するために、保管・保存した個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。
　①　個人データの保管・保存に必要なＩＤおよびパスワードの管理を徹底する。
　②　個人データが保存された機器・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、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・保存を認められた必要最小限の取扱者に限り保管・保存が行われるようＩＤおよびパスワードを付与すると共に、ＩＤおよ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・保存状況の記録および分析

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、必要に応じ、かつ適切に保管・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、記録された状況を確認する。

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、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と共に、保管・保存した個人データに障害が発生した際にはバックアップデータ等により復旧させなければならない。
2．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および認証

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およ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およびアクセス制御

1．個人データ管理者は、個人データの保管・保存段階における管理区分の設定およびアクセス制御機能を設けなければならない。
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、個人データの保管・保存段階におけるアクセス権限に関する機能を設けなければならない。
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および分析

個人データ管理者は、個人データの保管・保存段階におけるアクセス記録を取得し、必要な期間保管するとともに、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。

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および分析

個人データ管理者は、個人データの保管・保存段階におけるシステムの稼動状況に関し記録を取得し、必要な期間保管するとともに、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。

移送・送信段階取扱規程

第1条　目的

本規程は、当事務所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などをいう。
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などをいう。

第3条　移送・送信に関する取扱者の役割・責任および取扱者の限定

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、政治的見解、信教（宗教、思想および信条をいう。）、労働組合への加盟、人種および民族、門地および本籍地、保健医療および性生活、ならびに犯罪歴に関する情報（以下、「センシティブ情報」という。）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・送信時の照合および確認手続き

個人データの取扱者は、個人データの移送・送信するときには、移送・送信先に相違がないか照合および確認を行わなければならない。

第７条　移送・送信の規程外作業に関する申請および承認手続き

個人データの取扱者は、本規程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、移送・送信する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

① 個人データの移送・送信に必要なＩＤおよびパスワードの管理を徹底する。

② 個人データが保存された機器・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、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・送信を認められた必要最小限の取扱者に限り移送・送信が行われるようＩＤおよびパスワードを付与すると共に、ＩＤおよ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・送信状況の記録および分析

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、必要に応じ、かつ適切に取得・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、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・宗教等の団体もしくは労働組合への所属もしく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、金融庁ガイドライン第６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、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と共に、移送・送信した個人データに障害が発生した際にはバックアップデータ等により復旧させなければならない。

2．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および認証

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およ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およびアクセス制御

1．個人データ管理者は、個人データの移送・送信段階における管理区分の設定およびアクセス制御機能を設けなければならない。

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に関する機能を設けなければならない。

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および分析

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・廃棄段階取扱規程

第１条　目的

本規程は、当事務所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などをいう。
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などをいう。

第３条　消去・廃棄に関する取扱者の役割・責任および取扱者の限定

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、政治的見解、信教（宗教、思想および信条をいう。）、労働組合への加盟、人種および民族、門地および本籍地、保健医療および性生活、ならびに犯罪歴に関する情報（以下、「センシティブ情報」という。）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・廃棄時の照合および確認手続き

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期間を照合または消去・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・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・廃棄の規程外作業に関する申請および承認手続き

個人データの取扱者は、本規程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・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・記録媒体等の設置場所の指定ならびに管理区分および権限の設定をし、必要に応じ変更しなければならない。

２．個人データの取扱者は、前項の指定および設定に従い、個人データが保存された機器・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

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、消去・廃棄する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

① 個人データの入力に必要なＩＤおよびパスワードの管理を徹底する。

② 個人データが保存された機器・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。

第９条　消去・廃棄状況の記録および分析

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、記録された状況を確認する。

漏えい事案等対応規程

第１条　目的

本規程は、当事務所における個人データの安全管理措置のうち、個人データの漏えい事案等への対応の段階における取り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・収録された帳票や電子記録媒体（FD、CD-ROM 等）の盗難または紛失、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、滅失または毀損が生じ、また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・責任および取扱者の限定

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」という。）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程外作業に関する申請および承認手続き

個人データの取扱者は、本規程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および対応部署と連携のうえ漏えいした個人データの取扱状況の記録内容の分析を行い、漏えいした個人データの量、質、事故の原因、態様、被害の程度等漏えい事案等の内容およ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、漏えいした個人データ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、直ちに取引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取引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および再発防止策の公表）の要否およ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および分析

１．対応部署の個人データの取扱者は、漏えい事案等へ対応する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に取得・入力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、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

点検・監査に関する規程

第１条　目的

本規程は、当事務所における個人データの取扱状況に関する点検およ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およ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およ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

る監査責任者およ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、定期的およ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の取り扱いに関する規程に違反する事項など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、規程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．個人データ管理責任者は、個人データの取扱状況の監査に関する計画を立案し、監査責任者に対し、定期的および臨時の監査を実施するよう指示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の取り扱いに関する規程に違反する事項など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、規程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に従い、改善のための措置を講じなければならない。

外部委託に関する規程

第１条　目的

本規程は、当事務所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、およ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、当事務所が他の者に個人データの取扱いの全部また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、当事務所が、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　委託にあたっての所属保険会社への申請および承認

個人データ管理責任者は、保険会社から取扱の委託を受けた個人データの委託にあたって、所属保険会社に申請し、承認を得なければならない。

ただし、所属保険会社が別に定める場合はこの限りではない。

第４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、「委託先選定チェックリスト」を別に定め、これに基づき委託先を選定するとともに、「委託先選定チェックリスト」を定期的に見直さなければならない。
２．個人データ管理者は、「委託先選定チェックリスト」の策定および見直しにあたっては個人データ管理責任者の承認を得なければならない。
３．個人データ管理責任者は、承認した「委託先選定チェックリスト」を組織内に周知しなければならない。

第５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、委託契約後に「委託先選定チェックリスト」に定められた事項の委託先における遵守状況を定期的また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、以下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 当事務所の委託先に対する監督およ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、改竄およ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
２．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、定期的また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。