個人情報・特定個人情報安全管理細則

株式会社エントライズ

第１章 総 則

（目 的）

第１条　本細則は、「個人情報・特定個人情報保護規程」（以下「保護規程」という。）に基づき、当社における個人データ及び個人番号その他の特定個人情報の適切な管理のためにとるべき具体的事項を定めることを目的とする。

第２章 組織的安全管理措置

（従業者の役割と責任）

第２条　個人データ及び特定個人情報の取得、利用、保存、提供及び削除・廃棄等の作業は、個人情報保護管理者（保護規程第４条）又は個人情報取扱責任者（保護規程第６条。以下「取扱責任者」という。）が責任者となり、その監督のもとで実施する。

２．個人データの取得、利用、保存、提供及び削除・廃棄等の作業を担当する従業者は、必要な範囲の人員に限定し、みだりに他の従業者に当該作業を行わせてはならない。

３．個人番号事務取扱担当者（保護規程第５条。以下「事務取扱担当者」という。）以外の従業者は、当社の個人番号関係事務に従事することができない。

４．事務取扱担当者は、当社の個人番号関係事務を処理するために必要な限度で、個人番号及び特定個人情報（以下「特定個人情報等」という。）の取得、利用、保存、提供及び削除・廃棄等の作業に従事することができる。

５．当社が個人データの取扱い又は個人番号関係事務（保護規程第２条第(14)号）を外部に委託する場合の委託先に関する監督は、個人情報保護管理者又は取扱責任者が責任者となり、その監督のもとで実施する。

（特定個人情報の取得）

第３条　特定個人情報等の取得作業を担当する事務取扱担当者は、当社が保護規程第24条及び第25条により他人から個人番号の提供を受ける場合に、紛失による情報漏えい等を防止するため、下記各号を遵守して個人番号その他の特定個人情報を取得する。

(1) 本人等から個人番号が記載された書類等（個人番号カードのICチップを読み取る等による電子的方式を含む。）の提出を受けるときは、原則として、事務取扱担当者が直接受け取るものとする。

(2) 本人等から個人番号が記載された書類等の提出を受けるときは、当該書類等を封筒に入れた状態で直接受領する等、他人が特定個人情報等を容易に確認できない状態で提出を受けるものとする。

(3) 本人等から個人番号が記載された書類等の提出を受けて取りまとめる作業のみを担当する事務取扱担当者を定めることができる。この事務取扱担当者は、書類の不備がない

かの確認等の必要な事務を行った後は、速やかに入力等を担当する事務取扱担当者に受け渡しを行い、自分の手元に特定個人情報等を残してはならない。

(4) 個人番号が記載された書類等の提出を受けて取得し、入力等の作業を行う部署に当該書類を移動する際は、専用の封筒又は書類入れに入れる等、他人が特定個人情報等を容易に確認できず、紛失等も防止できる方策を講ずるものとする。

(5) 事務取扱担当者以外の従業者は、個人番号が記載された書類等又はその可能性のある書類等を受け取った場合は、速やかに事務取扱担当者に受け渡さなければならない。

(6) 事務取扱担当者は、従事している個人番号関係事務の処理以外の目的で、取得した個人番号を含むメモ、複写、印刷物、データのコピーその他の控えを作成してはならない。

（個人データ・特定個人情報の入力）

第４条　取得した個人データを情報システムに入力する作業を担当する従業者は、情報漏えい等を防止するため、下記各号を遵守して作業を実施する。

(1) 物理的安全管理措置（本規程第３章）及び技術的安全管理措置（本規程第４章）が施された場所及び機器で、入力作業を実施する。

(2) 取扱責任者が承認した場合を除き、入力を行う端末に、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続してはならない。

(3) 入力したデータを暗号化又はパスワードにより保護した場合の暗号鍵・パスワードは、入力作業中は入力を担当する者が管理し、定期的に取扱責任者が管理の状況を点検する。

(4) 入力作業のほか、個人データの移送・送信、利用・加工、保存又は削除・廃棄等、あらかじめ権限を付与されている作業以外の作業を行ってはならず、権限外の作業を行う場合は、取扱責任者又は上長の承認を得なければならない。

２．取得した特定個人情報等を情報システムに入力する作業を担当する事務取扱担当者は、情報漏えいや個人番号の不正利用等を防止するため、下記各号を遵守して作業を実施する。

(1) 物理的安全管理措置（本規程第３章）及び技術的安全管理措置（本規程第４章）が施された場所及び機器で、入力作業を実施する。

(2) 取扱責任者が承認した場合を除き、入力を行う端末に、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続してはならない。

(3) 入力したデータを暗号化又はパスワードにより保護した場合の暗号鍵・パスワードは、入力作業中は入力を担当する者が管理し、定期的に取扱責任者が管理の状況を点検する。

(4) 入力作業のほか、特定個人情報等の移送・送信、利用・加工、保存、削除・廃棄等、あらかじめ権限を付与されている作業以外の作業を行ってはならず、権限外の個人番号関係事務処理を行う場合は、取扱責任者の承認を得なければならない。

(5) 従事している個人番号関係事務の処理以外の目的で、個人番号を含むメモ、複写、印刷物、データのコピーその他の控えを作成してはならない。

(6) 従事している個人番号関係事務の処理以外の目的で、特定個人情報ファイル（保護規程第２条第(8)号）を複製し、加工し、又は新たに特定個人情報ファイルを作成してはならない。

（個人データ・特定個人情報の利用等）

第５条　個人データの利用・加工、保存等（以下「利用等」という。）の作業を担当する従業者は、情報漏えい等を防止するため、下記各号を遵守して作業を実施する。

(1) 物理的安全管理措置（本規程第３章）及び技術的安全管理措置（本規程第４章）が施された場所及び機器で、利用等の作業を実施する。

(2) 取扱責任者が承認した場合を除き、利用等の作業を行う端末に、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続してはならない。

(3) 利用等の対象となるデータ及びそのバックアップデータを暗号化又はパスワードにより保護した場合の暗号鍵・パスワードは、利用等を担当する者が管理し、定期的に取扱責任者が管理の状況を点検する。

(4) 利用等の作業のほか、あらかじめ権限を付与されている作業以外の作業を行ってはならず、権限外の作業を行う場合は、取扱責任者又は上長の承認を得なければならない。

２．特定個人情報等の利用・保存等の作業を担当する事務取扱担当者は、情報漏えい等を防止するため、下記各号を遵守して作業を実施する。

(1) 物理的安全管理措置（本規程第３章）及び技術的安全管理措置（本規程第４章）が施された場所及び機器で、利用等の作業を実施する。

(2) 取扱責任者が承認した場合を除き、利用等の作業を行う端末に、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続してはならない。

(3) 利用等の対象となるデータ及びそのバックアップデータを暗号化又はパスワードにより保護した場合の暗号鍵・パスワードは、利用等を担当する者が管理し、定期的に取扱責任者が管理の状況を点検する。

(4) 利用等の作業のほか、あらかじめ権限を付与されている作業以外の作業を行ってはならず、権限外の個人番号関係事務処理を行う場合は、取扱責任者の承認を得なければならない。

(5) 従事している個人番号関係事務の処理以外の目的で、個人番号を含むメモ、複写、印刷物、データのコピーその他の控えを作成してはならない。

(6) 従事している個人番号関係事務の処理以外の目的で、特定個人情報ファイル（保護規程第２条第(8)号）を複製し、加工し、又は新たに特定個人情報ファイルを作成してはならない。

(7) 特定個人情報等を管理するシステムの複製データ、特定個人情報等の利用等の作業のために作成した電子データ及び行政機関へ提出する書類を作成するために出力したチェックリスト等は、利用等の必要がなくなり次第すみやかに削除し、必要のない複製データ等が存在しないようにしなければならない。

（個人データ・特定個人情報の提供等）

第 6 条　個人データの移送・送信、提供等の作業を担当する従業者は、個人データの性質及び量等に応じて、紛失・盗難による情報漏えい等を防止するため、下記各号を参照し、適宜の保護措置を講じて作業を実施する。

(1) 個人データが記載された書類を交付する方法により提供する場合は、封筒への封緘、目隠しシールの貼付等により、他人が個人データを容易に確認できない状態で行う。

(2) 郵送等により個人データを提供する場合には、あて先を複数回確認のうえ送付する。

(3) ＦＡＸ送信により個人データを提供する場合は、あて先番号を確認の上、あらかじめ電話によりあて先に送信する旨を伝え、送信後に受領確認を行う。個人データが記載された書類等は確実に回収し、ＦＡＸ機等に放置してはならない。

(4) 個人データが記載された書類を取扱区域外に持ち出す場合は、封筒への封入、専用の書類入れの利用又は目隠しシール貼付等をした上で、施錠できる鞄や搬送容器で搬送する等、紛失・盗難等を防ぐための方策を講ずる。

(5) 個人データが記録された機器・電子媒体等を取扱区域外に持ち出す場合は、持ち出すデータを暗号化又はパスワードにより保護し、施錠できる搬送容器を利用する等、紛失・盗難等を防ぐための方策を講ずる。

(6) 個人データが記録されたデータをインターネット・メール等により外部に送信する場合は、取扱責任者又は上長の承認を得た上で、第 12 条第 3 項による技術的安全管理措置を講じ、送信先のメールアドレスに間違いないかを複数回確認のうえ送信し、受信確認を行う。

２．特定個人情報等の移送・送信、提供等の作業を担当する事務取扱担当者は、紛失・盗難による情報漏えい等を防止するため、下記各号その他の適宜の保護措置を講じて作業を実施する。

(1) 特定個人情報等が記載された書類を本人に返却・交付する場合や行政機関等の個人番号利用事務実施者に提出する場合は、封筒への封緘、目隠しシールの貼付等により、他人が特定個人情報等を容易に確認できない状態で交付・提出する。ただし、個人番号利用事務実施者（保護規程第 2 条第(16)号）に提出する場合は、当該個人番号利用事務実施者の指定する提出方法に従う。

(2) 郵送等の方法により特定個人情報等を提供する場合には、あて先を複数回確認のうえ送付し、受領確認を行う。ただし、個人番号利用事務実施者に提出する場合は、当該個人番号利用事務実施者の指定する提出方法に従う。

(3) 特定個人情報等が記載された書類を取扱区域外に持ち出す場合は、封筒への封入、専用の書類入れの利用又は目隠しシール貼付等をした上で、施錠できる鞄や搬送容器で搬送する等、紛失・盗難を防ぐための方策を講ずる。

(4) 特定個人情報等が記録された機器・電子媒体等を取扱区域外に持ち出す場合は、持ち出すデータを暗号化又はパスワードにより保護し、施錠できる搬送容器を利用する等、紛失・盗難を防ぐための方策を講ずる。

(5) 特定個人情報等が記録されたデータをインターネット・メール等により外部に送信する場合は、取扱責任者の承認を得た上で、第 12 条第 3 項による技術的安全管理措置を講じ、送信先のメールアドレス等に間違いないかを複数回確認のうえ送信し、受信確認を行

う。ただし、個人番号利用事務実施者にデータを提出する場合は、当該個人番号利用事務実施者の指定する提出方法に従う。

（個人データ・特定個人情報の削除・廃棄）

第７条　個人データの削除又は廃棄の作業を担当する従業者は、個人データを確実に削除・廃棄するために、下記各号を参照し、適宜の方法で作業を実施する。

(1) 個人データが記載された書類等を、焼却、溶解、復元不可能な程度に裁断可能なシュレッダーによる裁断等の復元不可能な手段で廃棄する。

(2) 個人データが記載された書類又は電子媒体等の中の個人データを、容易に復元できない手段で削除する。

(3) 個人データが記録されたデータのバックアップ内の個人データも削除する。

(4) 個人データが記録された機器及び電子媒体等を廃棄する場合は、専用のデータ削除ソフトウェアの利用等によりデータを完全消去し、又は物理的な破壊等によりデータを復元不可能にして廃棄する。

(5) 個人データが記録された機器及び電子媒体等をリース会社等に返却する場合は、専用のデータ削除ソフトウェアの利用等によりデータを完全消去する。

(6) 削除・廃棄の担当者が個人情報保護管理者又は取扱責任者に削除・廃棄の完了を報告し、個人情報保護管理者又は取扱責任者が確認する。

(7) 個人データの削除又は廃棄を実施した記録（削除・廃棄の日、削除・廃棄の方法、作業担当者）を保存する。

(8) 削除・廃棄の作業を委託する場合は、委託先が確実に削除・廃棄を実施したことについて証明書等により確認し、前号の記録に削除・廃棄の証明書等を添付する。

２．個人番号の削除又は廃棄の作業を担当する事務取扱担当者は、個人番号を確実に削除・廃棄するために、下記各号を遵守して作業を実施する。

(1) 特定個人情報等が記載された書類等を、焼却、溶解、復元不可能な程度に裁断可能なシュレッダーによる裁断等の復元不可能な手段で廃棄する。

(2) 特定個人情報等が記載された書類等の個人番号部分を復元不可能な程度にマスキングする。

(3) 特定個人情報等が記載された書類又は電子媒体等の中の個人番号を、容易に復元できない手段で削除する。

(4) 特定個人情報等が記録されたデータのバックアップ内の個人番号も削除する。

(5) 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合は、専用のデータ削除ソフトウェアの利用等によりデータを完全消去し、又は物理的な破壊等によりデータを復元不可能にして廃棄する。

(6) 特定個人情報等が記録された機器及び電子媒体等をリース会社等に返却する場合は、専用のデータ削除ソフトウェアの利用等によりデータを完全消去する。

(7) 削除又は廃棄の担当者が個人情報保護管理者又は取扱責任者に削除又は廃棄の完了を報告し、個人情報保護管理者又は取扱責任者が確認する。

(8) 個人番号若しくは特定個人情報ファイルを削除し、又はこれらのものが記録された電子媒体を廃棄した場合は、削除又は廃棄した記録を保存する。

(9) 削除又は廃棄等の作業を委託する場合は、委託先が確実に削除又は廃棄を実施したことについて証明書等により確認し、前号の廃棄の記録に証明書等を添付する。

（特定個人情報の取扱状況の記録）

第８条　特定個人情報等の取得、利用、保存、提供及び削除・廃棄等の作業による取扱状況については、後に確認できるように、適宜の方法で、次に掲げる事項を含むシステムログ・取扱実績等の記録を保存するものとする。当該取扱状況の記録には、個人番号を記載してはならない。

(1) 特定個人情報ファイルの利用・出力状況の記録

① 特定個人情報等の入手（入手日、事務取扱担当者、入手媒体の種別（紙・電子媒体等））

② 源泉徴収票等、特定個人情報等が記載された書類等の作成（作成日、事務取扱担当者）

(2) 書類・媒体等の持ち出しの記録

① 特定個人情報等が記載された書類等の本人への交付（交付日、事務取扱担当者）

② 特定個人情報等が記載された書類等の個人番号利用事務実施者への提出（提出日、事務取扱担当者）

③ 特定個人情報等が記載・記録された書類及び機器・電子媒体等の取扱区域外への持ち出し（持ち出し及び持ち帰りの日時、持ち帰ったデータの消去等の記録、事務取扱担当者）

④ 特定個人情報等のインターネット等による外部への送信（送信日、送信方法、事務取扱担当者）

(3) 前条に定める特定個人情報等の削除・廃棄の記録（削除・廃棄の証明書等を含む）

(4) 特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者による情報システムの利用状況（ログイン実績、アクセスログ等）

２．特定個人情報等の取扱状況は、取扱責任者が定期的に点検する。

第３章 物理的安全管理措置

（入退館等の管理）

第９条　事務所の入退館は、不審者の立入を予防して情報漏えい等を防止するとともに、後に入退館状況の確認ができるように、下記各号を参照し、適宜の方法で管理するものとする。

(1) 従業者は、業務終了後は速やかに退社し、業務終了後に事務所にみだりに立ち入ってはならない。

(2) 事務所を最後に退館した記録（従業者名・退館時刻等）を残す。

(3) 当社の休日等、事務所が閉鎖されている間に入館する場合は、上長の承認を得なければならない。

(4) 訪問者を事務所に入館させる場合は、取扱責任者が承認した場合を除き、次条に定める情報取扱区域に訪問者が近づくことのないように注意しなければならない。

(5) 特定個人情報保護管理者は、入退館の状況を定期的に確認する。

（情報取扱区域の管理）

第 10 条　個人データ又は特定個人情報ファイルを取り扱う情報システム（以下「情報システム」という。）を管理する区域及び特定個人情報を取り扱う事務を実施する区域（以下「情報取扱区域」という。）は、情報漏えい等を防止するために、下記各号を参照し、適宜の方法で管理するものとする。

(1) ＩＣカード、ナンバーキー等による入退室管理システムを設置する。

(2) 外部からは容易に入室できない室内とする。

(3) 壁又は間仕切り等の設置や作業を覗き見されにくい座席配置などの保護措置を講じた区域とする。

(4) 情報取扱区域は取扱責任者が管理する。

(5) 情報取扱区域には、取扱責任者が承認した場合を除き、情報システムで個人データを取り扱う担当者及び事務取扱担当者以外の者が立ち入ってはならない。

(6) 情報取扱区域は、取扱責任者が承認した場合を除き、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器の持込及び持出を禁止し、取扱責任者は、必要に応じて当該機器の持込・持出の検査を実施できる。

(7) 取扱責任者は、情報取扱区域の状況を定期的に点検する。

（情報取扱区域における機器等の管理）

第 11 条　情報取扱区域において個人データ及び特定個人情報等を取り扱う機器・電子媒体等は、紛失又は窃盗による情報漏えい等を防止するため、下記各号を参照し、適宜の方法で管理するものとする。

(1) 個人データ又は特定個人情報等を取り扱う機器は、離席時にロックするとともに、10 分程度でパスワード付きのスクリーンセーバー等が起動するように設定する。

(2) 個人データ又は特定個人情報等を取り扱う機器は、施錠できるキャビネット又は金庫での保管、セキュリティワイヤー等で固定する等の方法により、容易に外部に持ち出すことができない措置を講じる。

(3) 個人データ又は特定個人情報等を取り扱う機器は、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続できない措置を講じ、又は取扱責任者の承認を得ずに接続することを禁ずる。

(4) 個人データ又は特定個人情報等が記載された書類及び個人データ又は特定個人情報等が記録された電子媒体は、施錠できる保管場所に保管し、机上等に放置してはならない。

(5) 個人データ又は特定個人情報等を取り扱う機器を情報取扱区域外に持ち出す場合は、取扱責任者の承認を得なければならない。

(6) 当社が管理すべき個人データ又は特定個人情報等は、従業者の私物パソコン等で取り扱ってはならない。

(7) 個人データ又は特定個人情報等を取り扱う情報システムの操作マニュアルは、机上等に放置してはならない。

第４章 技術的安全管理措置

（情報システムへのアクセス管理）

第 12 条　個人データ又は特定個人情報ファイルを情報システムで取り扱う場合は、個人データ又は特定個人情報等を取り扱う情報システム（以下「情報システム」という。）及び個人データ・特定個人情報ファイルへのアクセス制御、アクセス者の識別・認証は、情報漏えい等を防止するため、下記各号を参照し、適宜の安全管理措置を講ずるものとする。

(1) 情報システム及び個人データにアクセスできる権限を有する従業者を限定する。

(2) 情報システム及び特定個人情報ファイルにアクセスできる権限を有する事務取扱担当者を限定する。

(3) ＩＤとパスワードにより、第(1)号及び第(2)号により限定した正当なアクセス権限を有する者であることの識別と認証を実施する。

(4) ＩＤ・パスワードの発行、変更及び廃止・削除は、取扱責任者が行う。

(5) ＩＤ・パスワードは付与される者ごとに異なるものとし、パスワードの最低文字数・有効期限等は取扱責任者が定める。

(6) パスワードは、氏名、社員番号、生年月日等、他人に推測されやすいものを使用してはならない。

(7) 磁気カード・ＩＣカードにより、第(1)号及び第(2)号により限定した正当なアクセス権限を有するものであることの識別と認証を実施する。

(8) ＩＤ・パスワード又は磁気カード・ＩＣカードを複数人で共同利用してはならない。

(9) パスワードは、メモを机上等に放置するなど他人が容易に認識可能な状態で管理してはならない。

(10) 退職・配転等により不要となったＩＤは速やかに削除・停止し、再利用してはならない。

(11) 退職・配転等により不要となった磁気カード・ＩＣカードは速やかに停止・回収し、再利用してはならない。

(12) 情報システム及び個人データ・特定個人情報ファイルへのアクセスは、業務時間内に限って行うものとする。

２．情報システム及び個人データ・特定個人情報ファイルへの不正アクセス等を防止するため、下記各号を参照し、適宜の安全管理措置を講ずるものとする。

(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て、不正アクセスを遮断する。

(2) 情報システム及びパソコン等の機器にセキュリティ対策ソフトウェア等を導入して適切な設定をする。

(3) 導入したセキュリティ対策ソフトウェア等により、出入力データにおける不正ソフトウェアの有無を確認する。

(4) 情報システム及びパソコン等の機器のオペレーティングシステム、ソフトウェア等を常に最新の状態に更新する。

(5) 端末には取扱責任者が認めるソフトウェアのみをインストールできることとする。

(6) 情報システム及び個人データ・特定個人情報ファイルへのアクセスや操作の成功と失

敗の記録及び不正が疑われる異常な記録の存否について定期的に確認し、不正アクセス等を検知する。

3．個人データ・特定個人情報等を外部に送信する場合に、通信経路における情報漏えいを防止するために、下記各号を参照し、適宜の技術的安全管理措置を講ずるものとする。

(1) 通信経路を暗号化する。

(2) 送信するデータを暗号化する。

(3) 送信するデータにパスワードによる保護をかける。

第５章 委託先の監督

（委託先の選定及び委託契約の締結）

第13条　当社が個人データの取扱い又は個人番号関係事務を外部に委託する場合は、個人情報保護管理者又は取扱責任者の監督下で、委託先に対して次の各号の事項を実施するものとする。

(1) 委託先の選定にあたり、個人データ又は特定個人情報等に関して当社が実施する安全管理措置と同等の安全管理措置が委託先においても講じられているかを確認する。

(2) 委託先との間で次の事項を含む契約を締結する。

① 委託した個人データ及び特定個人情報等に関する秘密保持義務

② 委託した個人データ又は特定個人情報等の事業所内からの持ち出しの禁止

③ 委託した業務以外の目的で個人データ又は特定個人情報等を利用することの禁止

④ 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、書面による当社の許諾を得て再委託するものとし、委託先が再委託先と連帯して責任を負うことの確認

⑤ 再委託先が更に再委託する場合も、書面による当社の許諾を得て再委託するとともに、再々委託先が再委託先及び委託先と連帯して責任を負うことを要し、更に再委託が繰り返される場合も同様である旨の確認

⑥ 委託先の従業者に対する監督・教育を実施すること

⑦ 契約内容の遵守状況についての報告

⑧ 委託した個人データ又は特定個人情報等に関する漏えい事故等が生じた際の委託先の責任

⑨ 委託契約終了時の個人データ及び特定個人情報等の返却、抹消及び廃棄

（委託先の監査）

第 14 条　当社は、個人情報保護管理者又は取扱責任者の監督のもとで、委託先に対し、適宜、契約内容が順守されていることの報告を求めるなどして、委託先における個人データ及び特定個人情報等の取扱状況を調査し、必要に応じて委託の内容等を見直すものとする。

（附 則）

第１ 条 本規程は、平成２７年１１月２５日より実施する。