個人データ取扱規定(段階別)

1. 取得・入力段階

(目的)
第 1 条　本規程は、株式会社シスデイズ（以降「弊社」と表記する）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。

(定義)
第 2 条　「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をいう。「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をいう。

(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)
第 3 条　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。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。

(センシティブ情報の取得・入力に関する取扱者の限定)
第 4 条　個人データ管理者は、個人情報のうち、健康状態・病歴などのセンシティブ情報の取得・入力の取扱者を必要最小限に限定しなければならない。

(取得・入力の対象となる個人データの限定)
第 5 条　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。

(取得・入力時の照合および確認手続き)
第 6 条　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。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。

(取得・入力の規程外作業に関する申請および承認手続き)

第 7 条　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。

（機器・記録媒体等の管理手続き）
第 8 条　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。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。

（個人データへのアクセス制御）
第 9 条　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場所へ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。

（取得・入力状況の記録および分析）
第 10 条　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。個人データ管理者は、個人情報の漏洩等の防止のため、必要に応じ、記録された状況を確認する。

（センシティブ情報）
第 11 条　個人データの取扱者がセンシティブ情報を取得する場合には、本人の同意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。また、郵送等により取得した文書等にセンシティブ情報が含まれている場合は、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。

2. 利用・加工段階

（目的）
第 1 条　本規程は、弊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」段階の取り扱いについて定めたものである。

（定義）
第 2 条　「利用」とは、個人データを利用目的の範囲内で取扱うことをいう。「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。「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。

（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）
第 3 条　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。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。

（センシティブ情報の利用・加工に関する取扱者の限定）
第 4 条　個人データ管理者は、個人データのうち、健康状態・病歴などのセンシティブ情報の利用・加工の取扱者を必要最小限に限定しなければならない。

（利用・加工の対象となる個人データの限定）
第 5 条　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。

（利用・加工時の照合および確認手続き）
第 6 条　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。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。

（利用・加工の規程外作業に関する申請および承認手続き）
第 7 条　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。

（機器・記録媒体等の管理手続き）
第 8 条　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。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。

（個人データへのアクセス制御）
第 9 条　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。

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。

（利用・加工状況の記録および分析）
第 10 条　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、かつ適切に利用・加工状況について記録を行わなければならない。個人データ管理者は、個人データの漏洩等の防止のため、必要に応じ、記録された状況を確認する。

（センシティブ情報）
第 11 条　個人データの取扱者がセンシティブ情報を利用する場合には、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。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。また、郵送等により取得した文書等にセンシティブ情報が含まれている場合は、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。

（個人データの管理区域外への持ち出しに関する措置）
第 12 条　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。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、且つ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。

（個人データへのアクセス制御）
第 13 条　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。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。

（個人データの漏洩・毀損等防止策）
第 14 条　個人データの利用・加工段階における漏洩・毀損等の防止策を講じなければならない。

（個人データへのアクセス記録および分析）
第 15 条　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、個人データの漏洩等の防止のため、必要に応じてこれを分析しなければならない。

3. 保管・保存段階

（目的）
第 1 条　本規程は、弊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。

（定義）
第 2 条　「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。「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至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。

（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）
第 3 条　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。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。

（センシティブ情報の保管・保存に関する取扱者の限定）
第 4 条　個人データ管理者は、個人データのうち、健康状態・病歴などのセンシティブ情報の保管・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。

（保管・保存の対象となる個人データの限定）
第 5 条　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。

（保管・保存の規程外作業に関する申請および承認手続き）
第 6 条　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。

（機器・記録媒体等の管理手続き）
第 7 条　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。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。

（個人データへのアクセス制御）
第 8 条　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。

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。

（保管・保存状況の記録および分析）
第 9 条　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。個人データ管理者は、個人データの漏洩等の防止のため、必要に応じ、記録された状況を確認する。

（個人データに関する障害発生時の対応・復旧手続き）
第 10 条　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。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。

（個人データの管理区分の設定およびアクセス制御）
第 11 条　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。また、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。

（個人データへのアクセス権限の管理）
第 12 条　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。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。

（個人データの漏洩・毀損等防止策）
第 13 条　個人データの保管・保存段階における漏洩・毀損等の防止策を講じなければならない。

（個人データへのアクセス記録および分析）
第 14 条　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、個人データの漏洩等の防止のため、必要に応じてこれを分析しなければならない。

4. 移送・送信段階

（目的）
第 1 条　本規程は、弊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。

（定義）
第 2 条　「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。「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。

（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）
第 3 条　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。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。

（センシティブ情報の移送・送信に関する取扱者の限定）
第 4 条　個人データ管理者は、個人データのうち、健康状態・病歴などのセンシティブ情

報の移送・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。

（移送・送信の対象となる個人データの限定）
第 5 条　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。

（移送・送信時の照合および確認手続き）
第 6 条　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。

（移送・送信の規程外作業に関する申請および承認手続き）
第 7 条　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。

（個人データへのアクセス制御）
第 8 条　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。

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。

（移送・送信状況の記録および分析）
第 9 条　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、かつ適切に移送・送信状況について記録を行わなければならない。個人データ管理者は、個人データの漏洩等の防止のため、必要に応じ、記録された状況を確認する。

（個人データに関する障害発生時の対応・復旧手続き）
第 10 条　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。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。

（個人データの利用者の識別および認証）
第 11 条　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。

（個人データの管理区分の設定およびアクセス制御）
第 12 条　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。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。

（個人データへのアクセス権限の管理）
第 13 条　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。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。

（個人データの漏洩・毀損等防止策）
第 14 条　個人データの移送・送信段階における漏洩・毀損等の防止策を講じなければならない。

（個人データへのアクセス記録および分析）
第 15 条　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、個人データの漏洩等の防止のため、必要に応じてこれを分析しなければならない。

5.　消去・廃棄段階

（目的）
第 1 条　本規程は、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。

（定義）
第 2 条　「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。「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。

（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）
第 3 条　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。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。

（センシティブ情報の消去・廃棄に関する取扱者の限定）
第 4 条　個人データ管理者は、個人データのうち、健康状態・病歴などのセンシティブ情報の消去・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。

（消去・廃棄時の照合および確認手続き）
第 5 条　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。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。

（消去・廃棄の規程外作業に関する申請および承認手続き）
第 6 条　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。

（機器・記録媒体等の管理手続き）
第 7 条　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。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。

（個人データへのアクセス制御）
第 8 条　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。

（消去・廃棄状況の記録および分析）
第 9 条　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。個人データ管理者は、個人データの漏洩等の防止のため、必要に応じ、記録された状況を確認する。

6. 漏洩事案等への対応の段階

（目的）
第 1 条　本規程は、当社における個人データの安全管理措置のうち、個人データの漏洩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。

（定義）
第 2 条　「漏洩事案等」とは、個人情報が記載・収録された帳票や電子記録媒体（ＣＤ等）の盗難または紛失、郵便物の誤送付、電子メールやＦＡＸの誤送信等の事故により、個人情報の漏洩、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。

（漏洩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）
第 3 条　個人データ管理責任者は、漏洩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。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洩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。

（漏洩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）
第 4 条　個人データの取扱者は、本規程に定める以外の方法で漏洩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。

（漏洩事案等の影響等に関する調査手続き）
第 5 条　漏洩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洩した個人データの取扱状況の記録内容の分析を行い、漏洩した個人データの量、質、事故の原因、態様、被害の程度等漏洩事案等の内容および影響の調査を行うこととする。

（再発防止策・事後対策の検討に関する手続き）
第 6 条　漏洩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、漏洩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。

（報告に関する手続き）

第 7 条　漏洩事案等が発生した場合、発見者は、漏洩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。対応部署は、報告を受けた漏洩事案等について、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洩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。

（漏洩事案等への対応記録および分析）

第 8 条　対応部署の個人データの取扱者は、漏洩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、かつ適切に漏洩事案等への対応状況について記録を行わなければならない。対応部署の個人データ管理者は、個人データの漏洩等の防止のため、必要に応じ、記録された状況を確認する。

以上