別添

データ保護・管理要領

１　目的

本件委託業務において取り扱う各種データについて、適正なデータ保護・管理方策、情報システムのセキュリティ方策及びデータの漏えい、亡失、改ざん、消去等（以下、「データ漏えい等」という。）発生時に実施すべき事項・手順等について明確にすることを目的とする。

２　適用範囲

本契約を履行するに当たり、出版、報道等による公知の情報を除き、主管担当が交付、若しくは使用を許可し、又は受託者が作成若しくは出力したものであって印刷された情報を含む全ての情報（以下「電子データ等」という。）を対象とする。

３　対象とする脅威

本要領において対象とする脅威は、次に掲げる情報セキュリティが害された又はその恐れがある場合（本契約履行に当たって受託者環境で発生した場合を含む。）とする。

（１）不正プログラムへの感染
（２）サービス不能攻撃によるシステムの停止
（３）情報システムへの不正アクセス
（４）書面又は外部記録媒体の盗難又は紛失
（５）主管担当が受託者に提供した又は受託者にアクセスを認めた電子データ等の目的外利用又は漏えい若しくは改ざん
（６）主管担当がアクセスを許可していない電子データ等への受注者によるアクセス
（７）主管担当又は受託者が意図しない不正な変更等
（８）異常処理等、予期せぬ長時間のシステム停止

４　本件委託業務を受託する者が遵守すべき事項

受託者は、本契約の履行に関して、以下の項目をすべて遵守すること。

（１）委託作業開始前の遵守事項

ア　データ管理計画書の提出

受託者は、下記イからクの各項に定める事項を取りまとめた「データ管理計画書」を作成し、委託業務開始前までに主管担当に提出して、主管担当の承認を受けること。

イ　データ取扱者等の指定

受託者は、上記「２ 適用範囲」に定める電子データ等を取り扱う者（以下「データ取扱者」という。）及び、データ取扱者を統括する者（以下「データ取扱責任者」という。）を指定し、その所属、役職及び氏名等を記入した「データ取扱者等名簿」を作成

すること。
　なお、データ取扱者及びデータ取扱責任者（以下「データ取扱者等」という。）は、秘密情報を含めた、電子データ等の取扱いに関する社内教育、並びに定期的な情報セキュリティに関する教育、又はこれに準ずる講習等を受講した者とし、その受講実績も併せて「データ取扱者等名簿」に記入すること。

ウ　データ取扱者等への教育・周知

　受託者は、本件委託業務で取り扱う電子データ等について、その取扱いや漏えい防止等に係る「教育・周知計画書」を作成し、本データ保護・管理要領の内容に関して、データ取扱者等に対する教育及び周知を行うこと。

エ　データの取扱いに関する計画策定

　受託者は、本件委託業務における電子データ等の取扱いに関し、保存、運搬、複製及び破棄、並びに電子データ等の保管場所を変更する場合において実施する措置を記載した「データ取扱計画書」を作成すること。

オ　日本郵政株式会社が準備する場所・機器利用時におけるセキュリティ確保

　受託者が、日本郵政株式会社が用意する場所や機器を利用して、本契約を遂行する場合は、主管担当が指示するセキュリティ対策を遵守すること。

カ　受託者の作業場所等のセキュリティ確保

　受託者は、日本郵政株式会社及び日本郵政株式会社が指定する場所以外の受託者が管理する作業場所において、本件委託業務を行う場合は、電子データ等及び電子データ等を処理するシステムに係るセキュリティ確保のため講じ得る措置について、「作業場所等に係るセキュリティ措置計画書」を作成すること。

(ｱ) 作業場所のセキュリティ確保

　作業場所のセキュリティ確保のための措置を講じること。

　例：データエントリールーム、データ保管室、電子計算機室等に対する施錠設備、
　　ＩＤカードやパスワードを用いた入退室管理機能等

(ｲ) 作業で使用する機器等のセキュリティ確保

ⅰ　電子データ等を取り扱うサーバ（クラウド環境を含む。）、パソコン、モバイル端末等の機器について、盗難、紛失、表示画面ののぞき見等による漏えいを防ぐための措置を講ずること。

ⅱ　それらの機器について、アクセス制御、USB 等の外部記録媒体への接続制御、及び脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。

ⅲ　それらの措置を講じていない機器による作業は、制限すること。

ⅳ　データ取扱者やデータ取扱責任者の指定を受けているものであっても、電子データ等に対して私用機器からのアクセスは、禁止すること。

　例：管理台帳による機器管理、システムログインパスワード、データ操作に対する
　　専用のＩＤ（アカウント）、受託作業範囲（データ取扱者/担当者・データ取扱

責任者/管理者・保守・運用等）に応じたアクセス権限の設定、ＩＤ（アカウント）の発行数管理や定期的な使用者確認・棚卸、受託業務で使用するシステム（データベースやフォルダを含む）等のアクセス記録（ログ）や監視状況の管理・確認（監査）、機器へのウィルスチェックソフトの導入、機器へのセキュリティパッチの適用、媒体の施錠保管、各種鍵類の管理等

(ｳ) 作業を行う上で使用する情報システムが接続するネットワークのセキュリティ確保電子データ等を取扱う情報システムに対し、外部のネットワークからの侵入や改ざんを防御する措置を行うこと。

例：外部接続箇所に、ファイヤーウォールを設置し、不要な通信の遮断
外部接続箇所に侵入検知システムを設置し、ネットワークへの不正侵入の遮断
外部接続箇所で、不正な通信を検出した場合、主管担当へ通報

キ　データ漏えい等発生時の対応手順作成

受託者は、本件委託業務で取り扱う電子データ等の漏えい等が発生した場合を想定し、その「対応手順書」を作成すること。手順書には、次の内容を記載すること。

- 受託者内の情報漏えい時の連絡体制（２４時間３６５日、データ取扱者等の間で相互連絡が可能な体制とすること。）
- 主管担当への連絡方法

ク　情報機器等の持込み

受託者は、本件委託業務で使用する情報機器を日本郵政株式会社又は日本郵政株式会社が指定する場所に持ち込む場合は、使用条件を明記した「情報機器等持込み機器使用計画書」を作成すること。

（２） 委託作業中における遵守事項

ア　データ管理簿の作成

受託者は、上記２で適用範囲とした電子データ等について、授受方法、保管場所、保管方法、使用場所、使用目的等取扱方法を明確にするため「データ管理簿」を作成すること。

イ　作業場所の監査

受託者は、日本郵政株式会社及び日本郵政株式会社が指定する場所以外の作業場所において本件委託業務を行っている場合に、主管担当がその施設及び設備に関し、上記（１）カで受託者が作成した「作業場所等に係るセキュリティ措置計画書」に則ったセキュリティ確保が図られているか監査する旨申し出た時は、定期・不定期にかかわらず、これを受け入れること。

ウ　データの取扱い

受託者は、本件委託業務において取り扱う電子データ等に関し、データ取扱責任者に以下の作業を行わせること。

(ｱ) データ取扱責任者は、データ取扱者の作業に立ち会う等適切な管理を行うこと。

(ｲ) データ取扱責任者は、データ取扱者を作業に従事させる前に、データ取扱者ごとに使用するユーザーＩＤ及びパスワード等、主管担当が事前に指定する事項について報告を行い、主管担当の承認を受けること。
　なお、報告する時期等は主管担当の指示に従うこと。また、報告した内容に変更が生じる場合も、事前に主管担当の承認を受けること。

(ｳ) データ取扱責任者は、作業に従事する予定のデータ取扱者について、事前に氏名、作業時間、作業内容及び取扱データを記入した「作業予定表」を提出し、主管担当の承認を受けること。

(ｴ) データ取扱責任者は、作業に従事したデータ取扱者が作業を終了し、作業場所を離れる際は、データの持ち出しの有無を厳重に検査すること。

(ｵ) データ取扱責任者は、作業終了後、作業に従事したデータ取扱者の氏名、作業時間、作業内容、取扱データ及びデータの持ち出しの有無等を記入した「作業結果報告書」を主管担当へ提出すること。その際、当初予定していた作業時間を越えている場合は、その理由も併せて記入すること。
　なお、作業結果表の提出時期については、主管担当の指示によること。

(ｶ) 記録媒体には中身が特定できるようなラベルを添付し、定期又は不定期に在庫を確認すること。

(ｷ) 各種管理簿はフルネームで記入されているか、また、改ざんに対する措置を講じている場合、遵守されているか確認すること。

(ｸ) 本件委託業務に関するすべてのメールについて、送受信履歴を確認すること。

(ｹ) 作業場所にＦＡＸがある場合、送信記録を確認すること。

(ｺ) 電子データ等へアクセスする機器を、故障等による交換又は修理のために外部へ持ち出しする場合は、当該機器上に、電子データ等が保存されていないかを確認し、当該機器の記憶装置からデータ消去の措置を講ずること。

エ　作業場所等のセキュリティ確保状況

(ｱ) 作業場所のセキュリティ確保のために講じた措置について、遵守され、セキュリティ対策状況に応じて見直しされていること。

(ｲ) 作業で使用する機器のセキュリティ確保のために講じた措置について、遵守され、セキュリティ対策状況に応じて見直しされていること。

(ｳ) 作業を行う上で使用する情報システムが接続するネットワークのセキュリティ確保のために講じた措置について、遵守され、セキュリティ対策状況に応じて見直しされていること。

(ｴ) 受託者外設備を使用する場合のセキュリティ確保のために講じた措置について、遵守され、セキュリティ対策状況に応じて見直しされていること。

(ｵ) 電子データ等の消失に備えた措置（データのバックアップ等）を講じている場合、遵守されているか確認すること。

オ　計画書等の変更・提出

(ｱ) 上記４(1)アの「データ取扱計画書」は、変更等が生じる都度作成し、主管担当へ提出すること。

(ｲ) 上記４(1)イの「データ取扱者等名簿」に変更が生じる場合は、変更の都度、主管担当に提出すること。

(ｳ) 上記４(2)アの「データ管理簿」は、適用範囲とした電子データ等の授受が発生の都度、記載すること。

（３） 委託業務完了時の遵守事項

ア　データ返却等処理

受託者は、委託業務完了時に上記４（２）アで作成した「データ管理簿」に記載されている、すべてのデータについて、返却、消去、廃棄等の措置を行うこと。

なお、その処理の方法、日時、場所、立会者、作業責任者等の事項を網羅した「データ返却等計画書」を事前に主管担当あて提出し、承認を得た上で、処理を実施すること。

イ　作業後の報告

受託者は、上記アに基づき返却等の処理終了後、その結果を記載した「作業完了報告書」を主管担当あて提出すること。

（４） 上記以外の遵守事項

ア　データ漏えい等発生時の対応

受託者は、本件委託業務に関し、データ漏えい等が発生した場合は、以下により、直ちに対応を図ること。

(ｱ) 発生状況報告

委託業務中に、データの漏えい等が発生した場合は、その事由が発生した日時、場所、事由、その時のデータ取扱者を明らかにし、直ちに主管担当に報告すること。また、「データ漏えい等発生報告書」を主管担当あて報告すること。

対応措置受託者は、主管担当の指示に基づき、対応措置を実施すること。

(ｲ) 報告書の提出

受託者は、主管担当が指定する期日までに、発生した事態の具体的内容、原因、実施した対処措置等を内容とする「データ漏えい等対応報告書」を作成の上、提出すること。

（ｳ）再発防止策の策定・提出

受託者は、データ漏えい等が発生した場合、その処理後に再発を防止するための措置内容を策定し主管担当の承認を得た後、直ちにデータ漏えい等再発防止策を実施すること。

イ　不正な侵入、盗難、不正アクセス等発生時の対応

受託者は、本件委託業務に関し、作業場所への不正侵入、作業機器等の盗難、ネットワークへの不正アクセス等が発生した場合は、上記アの対応に準じ、主管担当へ発生状況報告及び再発防止策の策定・提出を行うこと。

５　サイバーセキュリティに関する遵守事項

（１）適用範囲

本件委託業務において、当社の機密情報等の取り扱いが含まれる場合は、上記４の遵守事項に加え、本件委託業務を実施する環境（メール環境、インターネット環境を含む）を対象として、サイバーセキュリティに関する取り組み、不審メールの検知・遮断、外部ネットワークからの不正アクセス防止等の対策について、確認する。

受託者は、本契約の履行に関して、委託作業開始前及び委託作業中に、以下（２）～（４）の項目を遵守し、主管担当の指示に基づき報告し、主管担当の承認を受けること。

（２）　共通事項

ア　体制

サイバーセキュリティについての各部署ごとの役割（主管担当への報告体制を含む）・責任が明確化されていること。

イ　経営陣の関与

サイバーセキュリティについて経営陣が積極的に関与した上で、サイバー攻撃への対策措置に取り組んでいること。

ウ　監査

サイバーセキュリティに関する内部監査または外部監査を実施していること。
なお、契約締結時に未実施の場合は、履行開始前までに実施すること。

エ　リスクの認識

サイバーセキュリティの観点からリスクが認識されていること。

オ　情報の収集

サイバーセキュリティに関する脅威や脆弱性等の情報を収集し、速やかに対応する体制があること。

カ　教育・周知

従業者に対し、サイバーセキュリティについての教育・周知を行っていること。
なお、契約締結時に未実施の場合は、履行開始前までに実施すること。

キ　報告

サイバー攻撃を含む情報セキュリティ事故等が発生した場合やその恐れがある場合、直ちに主管担当に連絡し、事案が収束するまで定期的に報告すること。併せて被害拡大防止策を講じること。

（３） 社外からのメールが受信できる端末を使用する場合

主管担当が委託する当社の機密情報等を保有するシステムにアクセス可能なメール利用端末も含めること。

ア　不審なメールの検知・遮断

通信を監視し、不審なメール等を検知・遮断する機能が整備されていること。

イ　被害発生時の対処

標的型攻撃メールによる被害発生時の対処フローが整備されていること。

ウ　電子メールの運用方針

電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針が明確にされていること。

エ　電子メール送受信、Web ページ（ホームページ）閲覧等の不正使用防止

業務目的以外の電子メールの送受信、Web ページ（ホームページ）の閲覧等に対処するため、不正使用防止対策が講じられていること。

（４） インターネットに接続するシステムを使用する場合

ア　不審な通信の検知・遮断

通信を監視し、不審な通信の検知・遮断する機器等が整備されていること。

イ　セキュリティ診断

新たなシステムによるサービス開始前にセキュリティ診断が実施されていること。
既存システムについては定期的にセキュリティ診断が実施されていること。
なお、契約締結時に未実施の場合は、履行開始前までに実施すること。

ウ　被害発生時の対処

不正アクセス等による被害発生時の対処フローが整備されていること。

エ　リソース共有時の攻撃影響

クラウドサービス契約のように、他社とリソースを共有する場合、他社のシステムへのサイバー攻撃が、当該システムに与えるリスクを認識していること。

オ　外部ネットワークからの不正アクセス防止

不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、不必要な機器を接続していないこと。

参　考

外注管理に関する様式例

別紙１　「データ管理計画書」
別紙２　「データ取扱者等名簿」
別紙３　「教育・周知計画書」
別紙４　「データ取扱い計画書」
別紙５　「作業場所等に係るセキュリティ措置計画書」
別紙６　「データ漏えい等発生時対応手順書」
別紙７　「データ管理簿」、「データ返却等計画書」、「作業予定表」
別紙８　「作業結果報告書」
別紙９　「作業完了報告書」
別紙１０　「情報機器等持込み使用計画書」

別紙１

データ管理計画書

委託業務名
　〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇の委託

納入期限
　〇〇〇〇年〇〇月〇〇日

受託者
　〇〇株式会社
　代表取締役　〇〇　〇〇

別紙２

データ取扱者等名簿

委託業務名

〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇の委託

本件委託業務を実施するに当たり、各種データを取り扱う者を下記のとおり報告いたします。

担　当	氏　名	所　　属	役　職	備　　考
データ取扱責任者	〇〇　〇〇	××事業部	課長	△△訓練修了
データ取扱者	□□　□□	××グループ	ＳＥ	××資格保持

別紙３

教育・周知計画書

委託業務名
〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇の委託

本件委託業務を実施するに当たり、各種データを取り扱う者に対し、データ保護に関する教育及び周知を下記のとおり実施いたします。

記

１　実施時期
〇〇〇〇年〇〇月〇〇日～〇〇〇〇年〇〇月〇〇日

２　実施内容
仕様書添付の「データ保護・管理要領」の内容周知

３　対象者
データ取扱者名簿記載者

４　その他
一人当たり２時間程度

別紙４

データ取扱い計画書

データについて、下記のとおり異動事由が発生いたしましたので、承認願います。

記

１　データ名称
　　〇〇〇〇データ

２　異動事由
　　保管場所の変更
　　本社コンピュータセンターから、工場への変更

３　異動の目的
　　運用試験実施に伴う、試験場への保管場所移動

４　異動時期
　　〇〇〇〇年〇〇月〇〇日

別紙５

作業場所等に係るセキュリティ措置計画書

本件、「〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇の委託」事務を受託するに当たり、作業場所のセキュリティ措置を下記のとおり実施いたします。

記

１　作業場所
東京都〇〇区〇〇　　〇〇ビル〇階
〇〇株式会社　コンピュータセンター

２　セキュリティ措置
（１）作業施設
・　入退室について、ＩＤカードによる本人認証の設備を設置済み。
・　データ保管庫についても、同様の設備を設置済み。
（２）作業設備
作業端末は本件委託事務専用とし、データ取扱者個別にログインＩＤ及びパスワードを交付します。

別紙６

データ漏えい等発生時対応手順書

データ漏えい等発生時の手順については、下記のとおりといたします。

記

１　受託者内の情報漏えい時の連絡体制

フロー図のようなものを作成

２　データ取扱者

作業を中断し、発生時の状況を記録し、データ取扱責任者へ直ちに報告する。

３　データ取扱責任者

（１）　データ取扱者からの報告を受け、事実関係を確認し主管担当へ直ちに報告し、主管担当からの指示を待つ。

（２）　データ管理簿上のすべてのデータについて、現在の状況を確認する。

（３）　作業場所への入退室状況を確認し、主管担当からの指示があるまで入退室を制限する。

別紙７

データ管理簿

項番	データ名	記録 媒体	交付者	交付日	受領者	授受 方法	保管 場所	保管 方法	使用 場所	使用 目的
1										
2										
3										

データ返却等計画書

下記データの返却等の取扱いについて、承認願います

記

データ名	方法	日時	場所	立会者	作業責任者

作業予定表

下記作業を行いますので、承認願います。

作業 ID	対象データ	作業者氏名	作業時間	作業内容	実作業時間	作業場所	備考

別紙８

作業結果報告書

下記のとおり作業が完了したので、報告いたします。

記

１　作業ＩＤ
　〇〇〇〇

２　作業内容
（１）　作業結果
　　正常
（２）　作業従事者
　　〇〇〇
（３）　作業時間
　　〇〇〇〇年〇〇月〇〇日
　　〇〇時〇〇分～〇〇時〇〇分
（４）作業内容
　　〇〇テスト
（５）取扱いデータ
　　〇〇データ
（６）データ持ち出しの有無
　　無し
（７）確認者
　　〇〇〇〇（データ取扱責任者）

別紙９

作業完了報告書

先に承認された「データ返却等計画書」の作業が終了いたしましたので、
報告いたします。

１　作業結果
良

２　作業責任者及び立会者
作業責任者　〇〇　〇〇
作業立会者　〇〇　〇〇

別紙１０

情報機器等持込み機器使用計画書

（持込み使用許可申請書兼承認書）

年　　月　　日

情報セキュリティ責任者

〇〇　〇〇　様

申請者

会社名

氏　名

以下のとおり、情報機器等を日本郵政株式会社（〇〇部）へ持ち込んで利用したいので申請いたします。

【申請者記入欄】

持込み機器名・機種 （ﾒｰｶｰ･型番）	
持ち込み理由 （具体的な理由を記入）	
持込み期間	年　月　日　～　年　月　日（１年以内）
カメラ機能の有無	有　・　無
備　考	

※　持込み期間は１年以内とする。

【注】当社内において承認等処理を行う際に、電子申請、メール申請を使用しない（紙で申請処理を実施）場合は、以下に自筆署名。

	年　月　日		氏　名（自署）
情報セキュリティ管理者	確　認	年　月　日	
情報セキュリティ責任者	□承　認 □非承認	年　月　日	