栃木県那須塩原市

外部委託における情報セキュリティ遵守事項

制定（改正）年月日	改正の概要及び理由
2024 年（令和6年）10 月 22 日	制定初版

1. 用語の定義

（1）重要情報以上の情報

本書における「重要情報以上の情報」とは、重要度区分における最重要情報及び重要情報をいう。那須塩原市（以下、「市」という。）の情報セキュリティポリシーでは、以下のとおり市の情報資産を重要度による区分を行っている。

区分	情報資産（例）	詳細
最重要情報	●個人情報 ・住民、職員の個人情報 ・特定個人情報（マイナンバー） ●個人情報以外 ・認証情報（パスワードや生体情報等） ・施設設計情報 ・入札予定価格	原則市民向けに公開されない情報 情報が漏えいした場合に、プレスリリースが必要になり得る情報
重要情報	・政策検討に関する情報 ・公にすることを前提としていないものの、最重要情報には該当しない情報	市ホームページ等で市民向けに公開される前の情報
一般情報	・一般公開された情報 ・公にすることを前提とした個人情報	市ホームページ等で市民向けに公開されている情報

※特定個人情報…番号法第2条第8項に規定する特定個人情報（特定個人情報も最重要情報の一部である）

※個人情報…個人情報の保護に関する法律第2条に規定する個人情報（個人情報も最重要情報の一部である）

2. 秘密保持義務

（1）受託期間中に知り得た重要情報以上の情報については、本業務の従事者以外に提供してはならない。受託期間終了後（この契約が解除された後）においても同様とする。

（2）受託期間中に知り得た重要情報以上の情報は、従事者の退職後についても有効な秘密保持義務を課さなければならない。

（3）機器の修理、廃棄又はリース返却等において機器に内蔵する電磁的記録媒体における情報を取り扱う場合は、秘密保持契約を締結するほか、情報の消去等に関する証明書を提出しなければならない。

3. 目的外利用、受託者以外への提供禁止

（1）特定個人情報（マイナンバー）について、目的外の利用を禁止する。

（2）受託期間中に知り得た重要情報以上の情報について、受託業務以外に利用してはならない。

4. 受託事業実施中に作成又は収集した資料の返還義務

特に市が指定しない限り、受託事業実施中に作成又は収集若しくは市から提供された紙資料（以下、「資料」という。）は市に返還しなければならない。市から廃棄を依頼された場合には、復元不可能な状態にし、廃棄しなければならない。

※契約期間中の廃棄が難しい場合には、廃棄をするまでの保管方法を市と取り決め、廃棄時には受託者から市へ廃棄証明書の発行を行うこと。

※マイナンバーが記載された資料については、受託者が廃棄する場合は市職員の立ち会いが必要。

5. 受託事業実施中に作成又は収集したデータの廃棄義務

特に市が指定しない限り、受託事業実施中に作成又は収集若しくは市から提供されたデータ（以下、「データ」という。）は復元不可能な状態にし、廃棄しなければならない。

※契約期間中の廃棄が難しい場合には、廃棄をするまでの保管方法を市と取り決め、廃棄時には受託者から市へ廃棄証明書の発行が必要。

6. 体制の整備

（1）受託者は、受託業務の責任者、受託内容、作業者及び作業場所について市に報告すること。

（2）全ての業務従事者は、市の事務スペース等に入室する際には受託事業者である旨を証する表示を行うこと。

（3）全ての業務従事者は、市が指定した作業場所にて作業をすること。

（4）電算室に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

（5）電算室の機器等の搬入出について、市職員の立ち会いの下で行わなければならない。

（6）特権を付与されたID及びパスワードを変更を勝手に行ってはならない。

（7）クラウドサービスにおいて特権を付与されたIDを使用する場合、多要素認証を用いて認証しなければならない。

（8）システムの重要な設定変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。

7. 従事者への教育の義務

受託業務の実施前に、受託業務にかかわる全ての従事者（再委託先を含む。）に対して、本書に定める遵守事項を十分に周知させ、実行できるよう措置をとること。

8. 報告義務

情報セキュリティインシデントが発生したとき又は発生のおそれがある場合は、速やかに市に報告しなければならない。

9. 定期報告

受託者は、本書に定める遵守事項の実施状況（監督・教育、契約内容の遵守状況）について、定期的に市に報告すること。

10. 情報資産の適切な管理

受託者が、市から情報資産の提供を受けた場合は、市の指定する情報資産の分類に応じて以下の扱いをすること。重要情報以上の情報と一般情報が混在する場合等は、最も重要度区分の高い情報の取扱いによること。また、特定個人情報とその他の情報が混在する場合は、特定個人情報の取扱いによること。

（1）情報資産へのアクセス制限

重要情報以上の情報へのアクセスを業務上必要な従事者に限定すること。

（2）情報資産の利用

① 番号法に規定された業務以外に利用してはならない 。

② 市が指定した業務以外に利用してはならない。

③ 市が承認した区域内のみで利用すること。

④ 市が承認した利用者だけが利用すること。

⑤ 利用者の指定は最小限とすること。

⑥ 利用後は市があらかじめ指定した場所に収納すること。

⑦ 利用の際は利用者氏名・利用日時を記録し適切な期間保存すること。

（3）情報資産の保管

① 個人所有の機器（パソコン、スマートフォン、タブレット等）や電磁的記録媒体等へ情報資産を保存してはならない。

② 重要情報以上の情報が第三者に使用又は閲覧されることがないよう適正な措置を講じること。

③ 最重要情報が含まれる帳票に関して、使用時以外はロッカー、キャビネット等で常時施錠保管すること。

④ 特定個人情報（マイナンバー）は、施錠可能な指定された場所に保管し、市から保管場所の承認を得ること。また、市マイナンバー利用事務系の領域又は同等のアクセス制限等のセキュリティ対策が講じられた場所へ格納することとし、オンラインストレージや電磁的記録媒体（可搬記録媒体）への格納は禁止とする。

⑤ 受託業務に関する情報について、電磁的記録媒体等を使用時以外はロッカー、キャビネット等で施錠保管すること。

⑥ 受託業務に関する情報について、保存される必要がなくなった時点で速やかに記録した情報を消去すること。

⑦ 情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じること。

⑧ 利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、安全な場所に保管すること。

（4）情報資産の印刷、複製及び複写

① 最重要情報の印刷、複製（電子データのコピー等）及び複写（紙のコピー等）は原則禁止とする。ただし、業務上やむを得ない場合は事前に市の許可を得ること。

② 重要情報の印刷、複製及び複写は必要最低限とする。

（5）情報資産の電子メール送信

① 特定個人情報（マイナンバー）の外部へのメール送信は禁止とする。

② 特定個人情報を除く最重要情報を外部にメール送信することは原則禁止とする。ただし、業務上やむを得ない場合は、市の許可の下、データの暗号化又はパスワード設定をした上で送信しなければならない。

③ 重要情報を外部にメール送信する場合は、市の許可の下、パスワードの設定等の必要な措置を講じること。

（6）情報資産のFAX送信

① 特定個人情報（マイナンバー）の外部へのFAX送信は禁止とする。

② 特定個人情報を除く最重要情報は、FAXでの送信を原則禁止とする。ただし、業務上やむを得ない場合は市の許可を得て送信すること。その場合、送信先の事前確認及び到着確認を行うこと。

（7）情報資産の郵送等

① 特定個人情報（マイナンバー）の郵送等による送付は禁止とする。

② 特定個人情報を除く最重要情報を含む帳票及び電磁的記録媒体は、郵送等を原則禁止とする。ただし、業務上やむを得ない場合は市の許可を得て送付すること。その場合、特定記録郵便等の追跡可能な送付方法を講じた上で親展表示などのセキュリティ対策を実施しなければならない。また電磁的記録媒体に関しては、データの暗号化又はパスワード設定をした上で送付しなければならない。

③ 重要情報を含む帳票及び電磁的記録媒体を郵便等で送付する場合には、書留相当で送付すること。また電磁的記録媒体に関しては、データの暗号化又はパスワード設定をした上で送付すること。

（8）オンラインストレージサービスを利用した情報資産の送信

① 特定個人情報（マイナンバー）のオンラインストレージサービスによる送信は禁止とする。

② 特定個人情報を除く最重要情報をオンラインストレージサービス経由で送信することは原則禁止とする。ただし、業務上やむを得ない場合は市の許可の下、原則としてデジタル推進課が管理するオンラインストレージサービスにより、データの暗号化又はアクセス制限等のセキュリティ対策を講じた上で送信しなければならない。

③ 重要情報をオンラインストレージサービス経由で送信する場合は、セキュリティ管理者の判断の下、パスワード設定等の必要な措置を講じた上で送信すること。

（9）情報資産の運搬

① 特定個人情報（マイナンバー）の運搬・持ち出しは原則禁止とする。ただし、業務上やむを得ない場合は市の許可を得て運搬・持ち出しすること。

② 特定個人情報を除く重要情報以上の情報に該当する情報資産を運搬する場合には、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じ、事前に市の許可を得ること。

（10）情報資産の廃棄

① 情報資産の廃棄やリース返却等を行う場合には、市の許可を得て、記録されている情報の機密性に応じ、記載内容が判読できない状態で廃棄すること。

② 廃棄する帳票・電磁的記録媒体等を集積する場合は、施錠できる場所に保管すること。

③ 情報資産の廃棄やリース返却等を行う場合は、行った処理について、日時、担当者及び処理内容を記録すること。

④ クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了に際して、クラウドサービスで扱う情報を適切に移行及び削除すること。

11. 情報システムの開発時の対応

開発データ、開発環境	・テスト環境とシステム運用環境を分離すること ・原則として開発時にはダミーデータを利用し、重要情報以上の情報をテストデータに利用してはならない。ただし、業務上やむを得ない場合は、市と事前に協議すること。
検査及びテストの実施	・運用テストを行う場合、あらかじめテスト環境による操作確認を行うこと。 ・システムの受入テストを行う場合、導入する組織と受け入れる組織がそれぞれ独立したテストを行うこと。
開発環境の報告	以下のうち必要な項目について作業開始前に市に報告し、承認を得ること。 ・保存されるサーバ、クライアントの設置場所の指定、アクセス制御の内容 ・媒体の利用の有無、保存、搬送方法 ・利用されるネットワーク環境 ・業務従事者体制届出書の提出 ・従事者に対する教育状況の提出 ・障害時の対応手順 ・不正プログラム（コンピュータウィルス等）対策の適用状況

12. 再委託の制限

（1）受託者が業務の一部を再委託する必要がある場合は市の承認を得ること。

（2）受託者は、再委託を行う場合には本契約に基づく一切の義務を再委託先に遵守させると共に、再委託先に対して全ての監督責任を負うものとする。

13. 立ち入り調査への協力

（1）受託者は、市の情報資産に関しての立ち入り調査に応じなければならない。

（2）受託者は、再委託を行う場合には再委託先に対する市の情報資産に関しての立ち入り調査に応じなければならない。

14. 遵守不履行の際の対応（損害賠償）

（1）告発等

本書に定める遵守事項を履行しなかったことにより、市は、罰則の適用及び告発、その他必要な措置をとるものとする。

（2）契約の解除等

本書に定める遵守事項が履行されなかった場合、市は契約の解除、損害賠償の請求等を行うことができるものとする。

15.　その他

受託者は、遵守事項の解釈について疑義が生じたとき、または遵守事項に定めのない事項については、市と協議の上、定めるものとする。