由布市の保有する個人情報の安全管理のための措置に関する指針

（令和６年３月１２日制定）

第１　総論

（趣旨）

この指針は、個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）第６６条第１項の規定による市の機関（議会を除く。以下「市の機関」という。）の保有個人情報の安全管理のための措置として、保有個人情報の適切な管理について、必要な事項を定めるものとする。

第２　管理体制

（総括保護管理者）

１　市の機関に保有個人情報の管理に係る総括保護管理者を置くものとし、副市長をもって充てる。

総括保護管理者は、市の機関における保有個人情報の管理に関する事務を総括する任に当たる。

（保護管理者）

２　会計管理者及び課又は局長の職にある者をもって充てる。

保護管理者は、課又は局（以下「課等」という。）における保有個人情報の適切な管理を確保する任に当たる。ただし、保有個人情報を由布市行政情報セキュリティポリシー（平成１８年１０月１日）１－２－６に規定する情報システム（以下「情報システム」という。）で取り扱う場合には、保護管理者は、当該情報システムの情報セキュリティ管理者と連携して、その任に当たる。

保護管理者は、保有個人情報の取扱いに関し苦情の申し出があったときは、関係書類を調査し、関係者に報告を求め、事実関係を把握するものとする。

（保護担当者）

３　課等に当該課等の保護管理者が指定する保護担当者を１名置くものとし、取り扱う保有個人情報の性質及び量に応じ、適宜複数人置くことも可能とする。

保護担当者は、保護管理者を補佐し、課等における保有個人情報の管理に関する事務を担当するものとする。

なお、保護管理者は、保護担当者を指定したとき、変更したとき、又は解任したときは、保護担当者指定（変更・解任）通知書（別記様式）により総務課へ速やかに通知しなければならない。

（監査責任者）

４　本市に監査責任者を置くものとし、総務課長をもって充てる。
　監査責任者は、保有個人情報の管理の状況について監査する任に当たる。
（保有個人情報の適切な管理のための委員会）
５　総括保護管理者は、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるときは、関係職員を構成員とする委員会を設けることができる。

第３　教育研修
１　総括保護管理者及び保護管理者は、保有個人情報の取扱いに従事する職員（臨時職員、会計年度任用職員、再任用職員及び派遣労働者を含む。以下同じ。）に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。
２　総括保護管理者及び保護管理者は、保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に対し、保有個人情報の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。
３　総括保護管理者は、保護管理者及び保護担当者に対し、保有個人情報の適切な管理のための教育研修を定期的に実施する。
４　保護管理者は、課等の職員に対し、保有個人情報の適切な管理のために、総括保護管理者の実施する教育研修へ参加の機会を付与する等の必要な措置を講ずる。

第４　職員の責務
　職員は、法の趣旨に則り、関連する法令及び規定等の定め並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱わなければならない。

第５　保有個人情報の取扱い
（アクセス権限）
１　保護管理者は、保有個人情報の秘匿性等その内容（特定の個人の識別の容易性の程度、要配慮個人情報の有無、漏えい等が発生した場合に生じる被害の性質・程度等をいう。以下同じ。）に応じて、当該保有個人情報にアクセスする権限を有する職員の範囲と権限内容を、当該職員が業務を行う上で必要最小限の範囲に限る。
２　アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。
３　職員は、アクセス権限を有する場合であっても、業務上の目的以外で保有個

人情報にアクセスしてはならず、アクセスは業務上の目的内で必要最小限としなければならない。

（複製等の制限）

4　職員が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次の行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、職員は、保護管理者の指示に従い行う。

（１）　保有個人情報の複製

（２）　保有個人情報の送信

（３）　保有個人情報が記録されている媒体の外部への送付又は持ち出し

（４）　その他保有個人情報の適切な管理に支障を及ぼすおそれがある行為

（誤りの訂正等）

5　職員は、保有個人情報の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行う。

（媒体の管理等）

6　職員は、保護管理者の指示に従い保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫等への保管、施錠等を行う。また、保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、原則として、パスワード等による暗号化を行う等アクセス管理のための必要な措置を講ずる。

（誤送付の防止）

7　職員は、保有個人情報を含む電磁的記録又は媒体（文書の内容だけでなく、付加情報（ＰＤＦファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合も含む。）の誤送信、誤送付、誤交付又はウェブサイト等への誤掲載を防止するため、個別の事務・事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認、チェックリストの活用等の必要な措置を講ずる。

（廃棄等）

8　職員は、保有個人情報又は保有個人情報が記録されている媒体（端末及びサーバーに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。

特に保有個人情報の消去又は保有個人情報が記録されている媒体の廃棄を委託する場合（二以上の段階にわたる委託を含む。）には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取る等委託先において消去及び廃棄が確実に行われていることを確

認する。

（保有個人情報の取扱状況の記録）

９　保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録する。

（外的環境の把握）

１０　保護管理者は、保有個人情報が、外国において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全のために必要かつ適切な措置を講じなければならない。

第６　情報システムにおける安全の確保等

（アクセス制限）

１　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（１６を除く。）において同じ。）の秘匿性等その内容に応じて、認証機能を有する等のアクセス制限のために必要な措置を講ずる。

２　保護管理者は、上記１の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。

（アクセス記録）

３　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期的に分析するために必要な措置を講ずる。

４　保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。

（アクセス状況の監視）

５　保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含む又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。

（管理者権限の設定）

６　保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずる。

（外部から不正アクセスの防止）

７　保護管理者は、保有個人情報を取り扱う情報システムへの外部からの不正

アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずる。

（不正プログラムによる漏えい等の防止）

８　保護管理者は、不正プログラムによる保有個人情報の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等の必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。

（情報システムにおける保有個人情報の処理）

９　職員は、保有個人情報について、一時的に加工等の処理を行うための複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。

（暗号化）

１０　保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。職員は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。

（記録機能を有する機器・媒体の接続制限）

１１　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい等の防止のため、スマートフォン、ＵＳＢメモリ等の記録内容等を有する機器・媒体の情報システム端末等への接続制限（当該機器の更新への対応含む。）等の必要な措置を講ずる。

（端末の限定）

１２　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。

（端末の盗難防止）

１３　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。

１４　職員は、保護管理者が必要であると認めたときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

（第三者の閲覧防止）

１５　職員は、端末使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。

（入力情報の照合等）

１６　職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保

有個人情報との照合等を行う。

（バックアップ）

１７　保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散して保管するための必要な措置を講ずる。

（情報システム設計書等の管理）

１８　保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。

第７　管理区域の安全管理

（入退管理）

１　保護管理者は、保有個人情報を取り扱う基幹的なサーバー等の機器を設置する室その他の区域（由布市行政情報セキュリティポリシー２－５－１（１）に規定する管理区域をいう。以下「管理区域」という。）に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。また、保有個人情報を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。

２　保護管理者は、必要があると認めるときは、管理区域の出入り口の特定化による入退の管理の容易化、所在表示の制限等の措置を講ずる。

３　保護管理者は、管理区域及び保管施設の入退の管理について、必要があると認めるときは、立ち入りに係る認証機能を設定し、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）及びパスワード等の読取防止等を行うために必要な措置を講ずる。

（管理区域の管理）

４　保護管理者は、外部からの不正な侵入に備え、管理区域に施錠設備、警報装置及び監視設備の設置等の装置を講ずる。

５　保護管理者は、災害時に備え、管理区域に、耐震、防火、防塵、防水等の必要な措置を講ずるとともに、サーバー等の機器の予備電源の確保及び配線の損害防止の措置を講ずる。

第８　保有個人情報の提供

（保有個人情報の提供）

保護管理者は、法第６９条第１項又は第２項第１号、第３号若しくは第４号の規定により市の機関以外の者に保有個人情報を提供する場合には、法第７

０条の安全確保の措置を要求するものとする。なお、必要があると認めるときには、提供前又は随時に実地の調査等を行い、措置状況等を確認してその結果を記録するとともに、改善要求等の措置を講ずる。

第９　保有個人情報の取扱いの委託

（業務の委託等）

保有個人情報の取扱いに係る業務を外部に委託する場合には、由布市個人情報取扱業務委託基準（令和６年３月１２日制定）に従い、適切な措置を講ずるものとし、公の施設の管理を指定管理者（地方自治法（昭和２２年法律第６７号）法第２４４条の２第３項に規定する指定管理者をいう。）に行わせる場合においては、指定管理者が管理を行う公の施設に係る個人情報取扱基準（令和６年３月１２日制定）に定める措置を講ずるものとする。

第１０　サイバーセキュリティの確保

（サイバーセキュリティに関する対策の基準等）

保有個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法（平成２６年法律第１０４号）第２６条第１項第２号に掲げられたサイバーセキュリティに関する対策の基準等を参考として、取り扱う保有個人情報の性質等に照らして適正なサイバーセキュリティの水準を確保する。

第１１　安全確保上の問題への対応

（事案の報告及び再発防止措置）

１　保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報を管理する保護管理者に報告する。

２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずる。ただし、外部からの不正アクセス又は不正プログラムの感染が疑われる当該端末のＬＡＮケーブルを抜く等、被害拡大防止のための直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。

３　保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。

４　総括保護管理者は、上記３の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を市の機関の長及び市長に速やかに報告する。

５　総括保護管理者及び保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。

（法に基づく報告及び通知）

６　漏えい等が生じた場合であって法第６８条第１項の規定により個人情報保護委員会（以下「委員会」という。）への報告及び同条第２項の規定による本人への通知を要するときは、上記１から５までと並行して、速やかに所定の手続きを行うとともに、委員会による事案の把握等に協力する。

（公表等）

７　法第６８条第１項の規定による委員会への報告及び同条第２項の規定による本人への通知を要しない場合であっても、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への連絡等の措置を講ずる。この場合において、市民へ不安を招きかねない事案（例えば公表を行う漏えい等が発生したとき、個人情報保護に係る内部規程に対する違反があったとき、又は委託先において保有個人情報の適切な管理に関する契約条項等に違反があったとき等）については、当該事案の内容、経緯及び被害状況等について、速やかに委員会へ情報提供を行うものとする。

第１２　監査及び点検の実施

（監査）

１　監査責任者は、保有個人情報の適切な管理を検証するため、上記第２から第１１までの措置の状況を含む本市における保有個人情報の管理の状況について、定期に、及び必要に応じ随時に監査（外部監査を含む。以下同じ。）を行い、その結果を総括保護管理者に報告する。

（点検）

２　保護管理者は、課等における保有個人情報の記録媒体、処理経路及び保管方法等について、定期に、及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告する。

（評価及び見直し）

３　総括保護管理者及び保護管理者は、監査又は点検の結果等を踏まえ、実効性等の観点から本指針について評価し、必要があると認めるときは、その見直し等の措置を講ずる。

附　則

この指針は、令和６年４月１日から施行する。