入間市個人情報の取扱いに関する管理規程

令和５年３月２８日決裁

目次

第１章　総則

（目的）

第１条　この規程は、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。）その他関係法令に基づき、市の実施機関が保有する個人情報の適正な取扱いの確保に必要な事項及び安全管理措置を定めることを目的とする。

（定義）

第２条　この規程において使用する用語の意義は、法及び入間市個人情報保護法施行条例（令和４年条例第１９号）の用語に定めるところによる。

第２章　管理体制

（総括保護管理者）

第３条　市における全ての保有個人情報に係る安全管理措置を総括する責任者として、総括保護管理者を置く。

２　総括保護管理者には、副市長をもって充てる。

３　総括保護管理者は、各実施機関における保有個人情報の管理に関する事務を総括し、次に掲げる事項を所掌する。

⑴　安全管理措置を講ずるための組織体制の整備に関すること。

⑵　保有個人情報の安全管理に関する教育及び訓練並びに研修の企画及び実施に関すること。

⑶　保有個人情報の安全管理についての指示、指導及び助言に関すること。

⑷　保有個人情報が管理規程等に基づき適正に取り扱われるための、必要かつ適切な監督

に関すること。

⑸　保有個人情報の管理状況の点検又は監査の結果等を踏まえた、管理規程等の見直し等に関すること。

⑹　前各号に掲げるもののほか市全体における保有個人情報の安全管理に関すること。

（保護管理者）

第４条　保有個人情報の適正な取扱い及び安全管理のため、各実施機関において保有個人情報を取り扱う各課等に保護管理者を置く。

２　保護管理者には、保有個人情報を取り扱う各課等の長をもって充てる。

３　保護管理者は、総括保護管理者を補佐し、当該課等における保有個人情報の管理に関する事務の遂行のため、次に掲げる事務を行う。

⑴　個人情報の取得、保有個人情報の利用・提供の承認及び記録等の管理に関すること。

⑵　保有個人情報の取扱状況の把握に関すること。

⑶　保有個人情報が管理規程等に基づき適正に取り扱われるための職員への必要かつ適切な監督に関すること。

⑷　業務の委託先における個人情報の取扱いに関する監督に関すること。

⑸　前各号に掲げるもののほか保有個人情報の安全管理措置に関すること。

４　前項の規定にかかわらず、同一の保有個人情報を複数の課において管理する場合、当該課の保護管理者は互いに連携し、保有個人情報に関する安全管理を行うとともに、当該課における任務を分担し、かつ責任を明確にするものとする。

５　前二項の規定にかかわらず、保有個人情報を情報システムで取り扱う場合、当該課の保護管理者と当該情報システムの管理者は、互いに連携し、保有個人情報に関する安全管理を行うとともに、当該課における任務を分担し、かつ責任を明確にするものとする。

（保護担当者）

第５条　保護管理者を補佐し、保有個人情報の管理に関する事務を担当するために、各実施機関の当該課に保護担当者を置く。

２　保護担当者には、情報セキュリティポリシー（以下、「セキュリティポリシー」という。）に規定する情報セキュリティリーダーをもって充てる。

（システム管理者）

第６条　保有個人情報を取り扱う情報システムを総括するために、システム管理者を置く。

２　システム管理者には、情報政策課長をもって充てる。

３　システム管理者は、情報システムで取り扱う保有個人情報について、安全の確保に必要な措置を講ずるものとする。

（監査責任者）

第７条　保有個人情報の取扱いに関する監査を行うため、監査責任者を置く。

２　監査責任者には、総務課長をもって充てる。

（保有個人情報の適切な管理のための委員会）

第８条　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、定期に又は随

時に開催する。

第３章　教育研修

（教育研修）

第９条　総括保護管理者は、職員（非常勤職員、臨時職員及び派遣職員を含む。以下同じ。）に対し、保有個人情報の適切な管理のために必要な教育研修を行う。

２　総括保護管理者は、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　保護管理者は、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の参加の機会を付与する等必要な措置を講ずるものとする。

第４章　職員の責務

（職員の責務）

第１０条　職員は、法の趣旨に則り、関連する法令及び規程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。

２　職員は、保有個人情報の漏えい等の事案の発生又は兆候を把握した場合及び保有個人情報を取り扱う職員が管理規程等に違反している事実又は兆候を把握した場合は、速やかに保護管理者に報告しなければならない。

第５章　保有個人情報の取扱い

（アクセス制限）

第１１条　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、当該保有個人情報にアクセス（情報に接する行為をいう。以下同じ。）する権限（以下「アクセス権限」という。）を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限定するものとする。

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、業務上の目的以外の目的で保有個人情報にアクセスしてはならない。

（複製等の制限）

第１２条　保護管理者は、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、次に掲げる行為については、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わなければならない。

⑴　保有個人情報の複製

⑵　保有個人情報の送信

⑶　保有個人情報が記録されている情報機器・媒体（以下「情報機器等」という。）及び書類等の外部への送付又は持出し

⑷　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のある行為

（誤りの訂正等）

第１３条　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、訂正等を行わなければならない。

（媒体の管理等）

第１４条　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情報機器等及び書類等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、セキュリティポリシーの定めを順守し、原則として、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずるものとする。

（誤送付等の防止）

第１５条　職員は、保有個人情報を含む電磁的記録又は媒体の誤送信・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保有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やチェックリストの活用等の必要な措置を講ずるものとする。

（廃棄等）

第１６条　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情報機器等及び書類等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ものとする。

２　職員は、保有個人情報の消去や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等必要な措置を講ずるものとする。

（個人情報の取扱い状況等の記録）

第１７条　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状況について記録するものとする。

（外的環境の把握）

第１８条　保有個人情報が、外国（民間事業者が提供するクラウドサービスを利用する場合においてはクラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国が該当する。）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管理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章　情報システムにおける安全の確保

（アクセス制御）

第１９条　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。次条から第３３条まで（第３２条を除く。）において同じ。）の秘匿性等その内容に応じて、認証機能を設定する等のアクセス制御のために必要な措置を講ずるものとする。

２　保護管理者は、前項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ものとする。

（アクセス記録）

第２０条　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、定期的に又は随時分析するために必要な措置を講ずるものとする。

２　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ものとする。

（アクセス状況の監視）

第２１条　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ものとする。

（管理者権限の設定）

第２２条　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ものとする。

（外部からの不正アクセスの防止）

第２３条　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ものとする。

（不正プログラムによる漏えい等の防止）

第２４条　保護管理者は、不正プログラムによる保有個人情報の情報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に必要な措置（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。）を講ずるものとする。

（情報システムにおける保有個人情報の処理）

第２５条　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。

（暗号化等）

第２６条　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ものとする。

２　職員は、前項の規定を踏まえ、その処理する保有個人情報の秘匿性等その内容に応じて、適切なパスワードの選択、漏えい防止の措置等により適切に暗号化を行う。

（記録機能を有する機器・媒体への接続制限）

第２７条　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に、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒

体（以下「外部記録媒体」という。）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を含む。）等の必要な措置を講ずるものとする。

（端末の限定）

第２８条　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ものとする。

（端末の盗難防止等）

第２９条　保護管理者は、端末の盗難又は紛失の防止のため、退庁時には鍵付きのロッカー等で保管、又は端末をワイヤーにて机に固定する等必要な措置を講ずるものとする。

２　職員は、保護管理者が必要であると認めるときを除き、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）

第３０条　職員は、端末の使用に当たっては、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ものとする。

（入力情報の照合等）

第３１条　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の必要な措置を講ずるものとする。

（バックアップ）

第３２条　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、分散保管するために必要な措置を講ずるものとする。

（情報システム設計書等の管理）

第３３条　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ものとする。

第７章　電子計算機室等の安全管理

（入退管理）

第３４条　保護管理者は、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「電子計算機室等」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ものとする。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ものとする。

２　保護管理者は、必要があると認めるときは、電子計算機室等の出入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ものとする。

３　保護管理者は、電子計算機室等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、立入りに係る認証機能を設定し、及び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。）、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ものとする。

（電子計算機室等の管理）

第３５条　保護管理者は、外部からの不正な侵入に備え、電子計算機室等に制御機能、施錠装置、警報装置及び監視設備の整備等の措置を講ずるものとする。

２　保護管理者は、災害等に備え、電子計算機室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずるものとする。

第８章　保有個人情報の提供

（保有個人情報の提供）

第３６条　保護管理者は、法第６９条第２項第３号及び第４号の規定に基づき行政機関等以外の者に保有個人情報を提供する場合には、法第７０条の規定に基づき、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面（電磁的記録を含む。）を取り交わすものとする。

２　保護管理者は、法第６９条第２項第３号及び第４号の規定に基づき行政機関等以外の者に保有個人情報を提供する場合には、法第７０条の規定に基づき、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況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ものとする。

３　保護管理者は、法第６９条第２項第３号の規定に基づき他の行政機関等に保有個人情報を提供する場合において、必要があると認めるときは、法第７０条の規定に基づき、前二項に規定する措置を講ずるものとする。

第９章　個人情報の取扱いの委託

（業務の委託等）

第３７条　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、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じなければならない。また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理並びに実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認するものとする。

⑴　個人情報に関する秘密保持、目的外利用の目的のための利用の禁止等の義務

⑵　再委託の制限又は事前承認等再委託に係る条件に関する事項

⑶　個人情報の複製等の制限に関する事項

⑷　個人情報の安全管理措置に関する事項

⑸　個人情報の漏えい等の事案の発生時における対応に関する事項

⑹　委託終了時における個人情報の消去及び媒体の返却に関する事項

⑺　法令又は契約に違反した場合における契約解除、損害賠償責任その他必要な事項

⑻　契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）

２　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、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。

３　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、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも毎年度１回以上、原則として実地検査により確認するものとする。

４　委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に第１項の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項の措置を講ずるものとする。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

５　保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記するものとする。

６　保有個人情報を提供し、又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずるものとする。

第１０章　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）

第３８条　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ものとする。

第１１章　安全管理上の問題への対応

（事案の報告及び再発防止措置）

第３９条　保有個人情報の漏えい等の事案の発生又は兆候を把握した場合及び職員が管理規程等に違反している事実又は兆候を把握した場合等、漏洩又は漏洩が疑われる事案が発生した場合は、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ものとする。

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速やかに講じなければならない。ただし、外部からの不正アクセスや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しなければならない。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ものとする。

４　総括保護管理者は、前項の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、被害状況等を市長に速やかに報告するものとする。

５　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と

ともに、同種の業務を実施している部局等に再発防止措置を共有するものとする。

（法に基づく報告及び通知）

第４０条　漏えい等が生じた場合であって、法第６８条第１項の規定による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場合には、前条の規定と並行して、速やかに所定の手続を行うとともに、委員会による事案の把握等に協力するものとする。

（公表等）

第４１条　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ものとする。

２　前項の公表を行う事案については、当該事案の内容、経緯、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章　監査及び点検の実施

（監査）

第４２条　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、定期的に又は随時監査を行い、その結果を総括保護管理者に報告するものとする。

（点検）

第４３条　保護管理者は、自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について、定期的に又は随時点検を行い、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ものとする。

（評価及び見直し）

第４４条　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保有個人情報の適切な管理のための措置について評価し、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ものとする。

第１３章　補則

（委任）

第４５条　この規程に定めるもののほか、必要な事項は、別に定める。