生駒市の保有個人情報の管理に関する規程

目次

第１章　総則

（目的）

第１条　この規程は、本市の保有する個人情報の適切な管理に関して必要な事項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。）及び生駒市個人情報の保護に関する法律施行条例（令和４年１２月生駒市条例第２６号。以下「法施行条例」という。）において使用する用語の例による。

（適用の範囲）

第３条　この規程は、法施行条例第２条第２項に規定する実施機関に適用するものとする。

第２章　組織体制

（総括保護管理責任者）

第４条　本市に、総括保護管理責任者１人を置き、市長をもって充てる。

２　総括保護管理責任者は、本市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。

（副総括保護管理責任者）

第５条　本市に、副総括保護管理責任者１人を置き、総務部長をもって充てる。

２　副総括保護管理責任者は、総括保護管理責任者を補佐する任に当たる。

（保護管理責任者）

第６条　各部に、保護管理責任者を置き、各部の部長をもって充てる。

２　保護管理責任者は、その所管する部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）

第７条　各課に、保護管理者１人を置き、各課の課長をもって充てる。

２　保護管理者は、当該課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。

３　保有個人情報を情報システムで取り扱う場合は、保護管理者は、当該情報システムの管理者と連携して、その任に当たる。

（保護担当者）

第８条　保有個人情報を取り扱う各課に、当該課の各係の係長をもって充てる。

２　保護担当者は、保護管理者を補佐し、各課における保有個人情報の管理に関する事務を担当する。

（研修責任者）

第９条　本市に、研修責任者を１人置き、人事課長をもって充てる。

２　研修責任者は、保有個人情報の取扱い及び適切な管理に関する研修を担当する。

（監査責任者）

第１０条　本市に、監査責任者１人を置き、総務部長をもって充てる。

２　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）

第１１条　総括保護管理責任者は、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開催するものとする。

第３章　教育研修

（教育研修）

第１２条　研修責任者は、保有個人情報の取扱いに従事する職員（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及び適切な管理のために必要な教育研修を実施する。

２　保護管理者は、当該課の職員に対し、保有個人情報の取扱い及び適切な管理のために、研修責任者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。

第４章　職員の責務

（職員の責務）

第１３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責任者、副総括保護管理責任者、保護管理責任者、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章　保有個人情報の取扱い

（アクセス制限）

第１４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する権限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うえで、その利用目的を達成するために必要最小限の範囲に限らなければならない。

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ず、アクセスは必要最小限としなければならない。

（複製等の制限）

第１５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、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わなければならない。

(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のある行為

（誤りの訂正等）

第１６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１７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、施錠等を行わなければならない。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（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じなければならない。

（誤送付等の防止）

第１８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じなければならない。

（廃棄等）

第１９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媒体（端末及びサーバ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わなければならない。特に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など、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しなければならない。

（保有個人情報の取扱状況の記録）

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、必要な台帳等を整備して、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しなければならない。

（外的環境の把握）

第２１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、その外国を特定し当該外国の個人情報の保護に関する制度等を把握したうえで、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等

（アクセス制御）

第２２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。以下この章（第３４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。

（アクセス記録）

第２３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、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２４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、当該保有個人情報の不適切なアクセス監視のため、必要な措置を講ずるものとする。

（管理者権限の設定）

第２５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２６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２７条　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２８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ものとする。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ものとする。

（暗号化）

第２９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。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ものとする。

（記録機能を有する機器・媒体の接続制限）

第３０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、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器及び媒体の情報システム端末等への接続の制限（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３１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ものとする。

（端末の盗難防止等）

第３２条　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ものとする。

２　職員は、保護管理者が必要が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３３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３４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を行うものとする。

（バックアップ）

第３５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３６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　情報システム室等の安全管理

（入退管理）

第３７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「情報システム室等」という。）に立ち入る権限を有する者を定めるとともに、必要に応じ、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、情報システム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、情報システム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、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。

（情報システム室等の管理）

第３８条　保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置及び監視設備の設置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、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、情報システム室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３９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。）を取り交わさなければならない。

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じなければならない。

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、第１項及び前項に規定する措置を講じなければならない。

第９章　個人情報の取扱いの委託

（業務の委託等）

第４０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、委託先における責任者及び業務従事者の管理体制及び実施体制、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しなければならない。

(1)　個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等

の義務

(2)　再委託（再委託先が委託先の子会社（会社法(平成１７年法律第８６号)第２条第１項第３号に規定する子会社をいう。）である場合も含む。この号及び第４項において同じ。）の制限又は事前承認等再委託に係る条件に関する事項

(3)　個人情報の複製等の制限に関する事項

(4)　個人情報の安全管理措置に関する事項

(5)　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

(6)　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

(7)　法令及び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

(8)　契約内容の遵守状況についての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、少なくとも年１回以上、原則として実地検査により確認しなければならない。

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

先が委託を受けた業務をさらに委託（二以上の段階にわたる委託を含む。）する場合も同様とする。

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しなければならない。

（その他）

第４１条　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、必要に応じて、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じなければならない。

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４２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しなければならない。

第１１章　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）

第４３条　保有個人情報の漏えい等安全管理のうえで問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事実等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告しなければならない。

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等のＬＡＮケーブルを抜くなど、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、保護管理責任者及び副総括保護管理責任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、直ちに保護管理責任者及び副総括保護管理責任者に当該事案の内容等について報告しなければならない。

４　保護管理責任者は、前項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、被害状況等を総括保護管理責任者に速やかに報告しなければならない。

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４４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、前条各項と並行して、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力しなければならない。

（公表等）

第４５条　保護管理責任者は、法第６８条第１項の規定による個人情報保護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じなければならない。

第１２章　監査及び点検の実施

（監査）

第４６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、第２章から第１１章までに記載する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責任者に報告しなければならない。

（点検）

第４７条　保護管理者は、各課におけ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、その結果を保護管理責任者に報告しなければならない。

２　保護管理責任者は、前項で保護管理者から受けた報告について、必要があると認めるときは、その結果を総括保護管理責任者及び副総括保護管理責任者に報告しなければならない。

（評価及び見直し）

第４８条　総括保護管理責任者及び副総括保護管理責任者は、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指示するものとする。

２　保護管理責任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　その他

（細則）

第４９条　この規程に定めるもののほか、この規程の実施のための手続その他について必要な事項は、別に定める。

附　則

（施行期日）

１　この規程は、令和５年４月１日から施行する。

（生駒市の保有する個人情報管理規程の廃止）

２　生駒市の保有する個人情報管理規程（平成２７年１１月２４日施行）は、廃止する。