佐野市個人情報の保護に関する管理基準

第１　総則

１　目的

この基準は、佐野市における個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 66 条に規定する保有個人情報の安全管理のために必要かつ適切な措置について定めることを目的とする。

２　定義

使用する用語は、個人情報保護法及び佐野市個人情報の保護に関する法律施行条例（令和5年佐野市条例第5号）において使用する用語の例によるほか、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）　セキュリティポリシー　佐野市情報セキュリティ基本方針及び佐野市情報セキュリティ対策基準をいう。

（２）　ネットワーク　コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

（３）　情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（４）　媒体　文書及び電磁的記録媒体（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものに係る記録媒体をいう。）をいう。

第２　管理体制

１　総括保護管理者

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するため、総括保護管理者を置き、副市長をもって充てる。

2　副総括保護管理者

総括保護管理者を補佐するため、副総括保護管理者を置き、行政経営部長をもって充てる。この場合において副総括保護管理者は、保有個人情報を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化を行う。

3　部総括保護管理者

保有個人情報を取り扱う部その他これに相当する組織（以下「部等」という。）における保有個人情報を適切に管理するため、部等に部総括保護管理者を置き、各部等の長（部長その他これに相当する職にある者）をもって充てる。

4　保護管理者

（1）　保有個人情報を取り扱う課、室その他これらに相当する組織（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ため、課等に保護管理者を置き、各課等の長をもって充てる。

（2）　保護管理者は、課等における保有個人情報を取り扱う各職員（臨時的に任用される職員、任期を定めて任用される職員、非常勤職員及び派遣労働者を含む。以下同じ。）及びその役割を指定する。

（3）　保護管理者は、課等における職員が取り扱う保有個人情報の範囲を指定する。

5　保護担当者

（1）　保護管理者を補佐し、各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ため、保有個人情報を取り扱う各課等に、保護担当者を一人又は複数人置く。

（２） 保護担当者は、保護管理者が指定する。

６　監査責任者

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ため、監査責任者を置き、行政経営課長をもって充てる。

７　佐野市情報公開・個人情報保護連絡会議

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、佐野市情報公開・個人情報保護連絡会議要綱（平成17年訓令第26号）第１条により設置する佐野市情報公開・個人情報保護連絡会議を開くものとする。

第３　教育研修

（１） 総括保護管理者は、保有個人情報の取扱いに従事する職員に対し、保有個人情報の取扱いについての理解を深め、保有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。

（３） 保護管理者は、当該課等の職員に対し、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の参加の機会を付与する等の必要な措置を講ずるものとする。

第４　職員の責務

職員は、個人情報保護法の趣旨にのっとり、関連する法令及び規程等の定め並びに総括保護管理者、副総括保護管理者、部総括保護管理者、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

１　アクセス制限

（１）　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、アクセス（当該保有個人情報に接する行為をいう。以下同じ。）をする権限（以下「アクセス権限」という。）を有する職員の範囲及びその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限るために必要な措置を講ずるものとする。

（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ず、アクセスは必要最小限としなければならない。

２　複製等の制限

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わなくてはならない。

（１）　保有個人情報の複製

（２）　保有個人情報の送信

（３）　保有個人情報が記載され、又は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のある行為

３　誤りの訂正等

職員は、保有個人情報等を正確かつ最新の内容に保つようにし、当該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。

4　媒体の管理等

職員は、保護管理者の指示に従い、保有個人情報が記載され、又は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、耐熱、耐水及び耐湿を講じた場所での保管、保管場所の施錠等の措置を講ずるものとする。

5　保有個人情報の送信又は運搬

保有個人情報を電子メール等において送信、外部への持ち出し又は車両等により運搬する者は、必要に応じ、暗号化、パスワード設定又は鍵付きケースに収納する等の措置を講ずるものとする。

6　誤送付等の防止

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ずるものとする。

7　廃棄等

職員は、保有個人情報又は保有個人情報が記載され、又は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う。

特に、保有個人情報の消去や保有個人情報が記載され、又は記録されている媒体の廃棄を委託する場合には、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する。

８　保有個人情報の取扱状況の記録

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。

９　外的環境の把握

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管理のために必要かつ適切な措置を講ずるものとする。

第６　情報システムにおける安全の確保等

１　アクセス制御

（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【情報システムにおける安全の確保等】（11【第三者の閲覧防止】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）　前号の必要な措置は、セキュリティポリシーのとおりとする。

２　アクセス記録

（１）　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）　前号の必要な措置は、セキュリティポリシーのとおりとする。

３　アクセス状況の監視

保護管理者は、保有個人情報の秘匿性等その内容及び量に応じて、当該保有個人情報への不適切なアクセスの監視のための設定、当該設定の定期的確認等の必要な措置が講じられていることを確認する。

4　管理者権限の設定

（1）　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、必要な措置を講ずるものとする。

（2）　前号の必要な措置は、セキュリティポリシーのとおりとする。

5　外部からの不正アクセスの防止

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、セキュリティポリシーに規定された措置が講じられていることを確認する。

6　不正プログラムによる漏えい等の防止

保護管理者及び職員は、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にセキュリティポリシーに規定された措置（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。）が講じられていることを確認する。

7　暗号化

（1）　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、セキュリティポリシーの規定に従い、適切に暗号化を行う。

（2）　前号の必要な措置は、セキュリティポリシーのとおりとする。

８　記録機能を有する機器・電磁的記録媒体の接続制限

（１）　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・電磁的記録媒体の情報システム端末等への接続の制限等の必要な措置を講ずるものとする。

（２）　前号の必要な措置は、セキュリティポリシーのとおりとする。

９　端末の限定

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。

10　端末の盗難防止等

（１）　保護管理者は、端末の盗難又は紛失の防止のために必要な措置を講ずるものとする。

（２）　前号の必要な措置は、セキュリティポリシーのとおりとする。

（３）　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てはならない。

11　第三者の閲覧防止

（１）　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、使用状況に応じて必要な措置を講ずるものとする。

（２）　前号の必要な措置は、セキュリティポリシーのとおりとする。

12　入力情報の照合等

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。

13　バックアップ

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。

14　情報システム仕様書等の管理

保護管理者は、ネットワーク構成図、情報システム仕様書について、媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理する。

第７　情報システム室の安全管理

１　入退管理

（１）　ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋等（以下「情報システム室」という。）の入退の制限及び記録、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は、セキュリティポリシーのとおりとする。

（２）　情報システム室の出入口の特定化による入退の管理の容易化等の措置は、セキュリティポリシーのとおりとする。

２　情報システム室の管理

（１）　情報システム室の施錠装置、警報装置及び監視設備の設置等の措置は、セキュリティポリシーのとおりとする。

（２）　情報システム室に、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は、セキュリティポリシーのとおりとする。

第８　保有個人情報の提供

１　保有個人情報の提供

（１）　保護管理者は、個人情報保護法第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、個人情報保護法第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を取り交わす。

（２）　保護管理者は、個人情報保護法第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、個人情報保護法第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。

第９　個人情報の取扱いの委託

１　業務の委託等

（１）　保護管理者は、個人情報の取扱いに係る業務を外部に委託する場合に、個人情報の適切な管理を行う能力を有する者を選定するため、委託に関する契約書に、次の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する。

ア　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に関する事項

イ　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（第９【個人情報の取扱いの委託】１【業務の委託等】（１）及び（４）において同

じ。）。）である場合）の制限又は事前承認等再委託に係る条件に関する事項

ウ　個人情報の複製等の制限に関する事項

エ　個人情報の安全管理措置に関する事項

オ　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

カ　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

キ　契約内容の遵守状況の調査又は報告に関する事項

ク　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

（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おいて、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、原則として実地調査により確認する。

（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、最初の委託者の承諾を得て、委託先に（１）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（３）の措置を実施する。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。

（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　情報システムにおける安全の確保

情報システムで取り扱う保有個人情報の安全の確保に関する事項については、この基準に定めるもののほか、セキュリティポリシーで定めるところによる。

第11　安全管理上の問題への対応

１　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の発生又は兆候を把握した場合、事務取扱担当者が法や保有個人情報の取扱いに係る規程に違反している事実又は兆候を把握した場合等、安全管理の上で問題となる事案の発生又は発生のおそれを認識した場合に、その事案の発生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ずるものとする。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、総括保護管理者及び副総括保護管理者に保有個人情報漏えい等事案報告書（別記様式第１号）により報告する。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及び副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、（３）による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。

（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、同種の事業を実施している課等に再発防止措置を共有する。

（６）　この基準で定めるもののほか、セキュリティポリシーで必要とされる措置を講ずるものとする。

２　個人情報保護法に基づく報告及び通知

漏えい等が生じた場合であって個人情報保護法第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、１【事案の報告及び再発防止措置】（１）から（６）までと並行して、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する。

３　公表等

個人情報保護法第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、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。この場合において、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行政経営課に報告する。

第12　監査及び点検の実施

１　監査

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【管理体制】から第11【安全管理上の問題への対応】までに規定する措置の状況を含む市における保有個人情報の管理の状況について、定期又は随

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。

2　点検

保護管理者は、各課等における保有個人情報の媒体、処理経路、保管方法等について、定期及び随時に点検を行い、必要があると認めたときは、その結果を総括保護管理者及び副総括保護管理者に報告する。

3　評価及び見直し

総括保護管理者等は、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。

別記様式第１（第 11　２関係）

受付日	年　　月　　日
受付番号	

保有個人情報漏えい等事案報告書

年　　月　　日

総括保護管理者

副総括保護管理者

課名

保護管理者

１．報告種別（該当する□に印を付けること。）

新規又は続報の別：□ 新規

□ 続報　前回報告：　　年　　月　　日

速報又は確報の別：□ 速報　□ 確報

２．報告者の概要

報告者	課	
	係	
	報告担当者	
	内線	

３．報告事項

（１）事態の概要（該当する□に印を付けること。）

発生日：　　年　　月　　日

発覚日：　　年　　月　　日

発生事案：□ 漏えい　□ 漏えいのおそれ　□ 滅失
□ 滅失のおそれ　□ 毀損　□ 毀損のおそれ

発見者：□ 自組織/委託先　□ 取引先
□ 取引先以外の外部指摘（例：市民等からの指摘）
□ カード会社/決済代行会社
□ その他（　　）

個人情報の保護に関する法律施行規則第 43 条各号該当性：
□ 第１号（要配慮個人情報）　□ 第２号（財産的被害）
□ 第３号（不正の目的）　□ 第４号（百人超）
□ 非該当（上記に該当しない場合の報告）

報告者から個人情報の取扱いの委託を受けた者（委託先）の有無：
□ 有（名称：　　）
（住所：　　）
（電話：　　）
□ 無

事実経過：

概要：
発覚の経緯・発覚後の事実経過（時系列）：

外部機関による調査の実施状況（規則第43条第3号に該当する場合のみ記載）：

□ 実施済（実施中）【依頼日：　　年　　月　　日】

□ 実施予定【依頼予定日：　　年　　月　　日】

□ 検討中

□ 予定なし

（詳細：　　）

（２）漏えい等が発生し、又は発生したおそれがある保有個人情報の項目（該当する□に印を付けること。）

媒体：□ 紙　□ 電子媒体　□ その他（　　）

種類：□ 市民等　□ 職員　□ その他（　　）

項目：□ 氏名　□ 生年月日　□ 性別

□ 住所　□ 電話番号　□ メールアドレス

□ クレジットカード情報　□ パスワード

□ その他（　　）

（３）漏えい等が発生し、又は発生したおそれがある保有個人情報に係る本人の数

（　　）人

うちクレジットカード情報含む（　　）人

（４）発生原因（該当する□に印を付けること。）

主体：□ 報告課　□ 委託先　□ 不明

原因：□ 不正アクセス

（攻撃箇所：（　　））

（攻撃手法：（　　））

□ 誤交付　□ 誤送付（メール含む。）

□ 誤廃棄　□ 紛失　□ 盗難　□ 職員不正

□その他（　　）

詳細：

（５）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：□ 有　　□ 無　　□ 不明

詳細：

（６）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：□ 対応済（対応中）

□ 対応予定

□ 予定なし

詳細（予定なしの場合は、理由を記載）：

（７）公表の実施状況（該当する□に印を付けること。）

事案の公表：□ 実施済【公表日：　年　　月　　日】

□ 実施予定【公表予定日：　年　　月　　日】

□ 検討中

□ 予定なし

公表の方法：□ ホームページに掲載　　□ 記者会見

□ 報道機関等への資料配布

□ その他（　　）

公表文：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項：

記載要領

１．最上段の受付日及び受付番号の欄には記載しないこと。

２．続報として提出の際には、前回報告から記載を変更した箇所に下線を引くこと。

３．３．（７）の「公表文」には、公表を予定している場合、公表予定の文案を記載又は添付すること。