上市町個人情報等の取扱いに関する安全管理規程を次のように定め、公表する。

令和５年10月３日

上市町長　中　川　行　孝

上市町訓令第７号

本　　庁
出先機関

上市町個人情報等の取扱いに関する安全管理規程

目次

第１章　総則（第１条・第２条）
第２章　管理体制（第３条―第８条）
第３章　職員の責務（第９条）
第４章　保有個人情報等の取扱い（第10条―第17条）
第５章　情報システムにおける安全の確保等（第18条―第32条）
第６章　電算室等の安全管理（第33条・第34条）
第７章　保有個人情報等の提供及び業務の委託等（第35条・第36条）
第８章　サイバーセキュリティの確保（第37条）
第９章　安全管理上の問題への対応（第38条―第40条）
第10章　監査及び点検の実施（第41条―第43条）
附則

第１章　総則

（趣旨）

第１条　この規程は、町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、

また、個人情報保護法第121条に規定する行政機関等匿名加工情報等の適切な管理のために必要な措置について定めるものとする。

（定義）

第２条　この規程において使用する用語は、個人情報保護法において使用する用語の例による。

第２章　管理体制

（総括責任者）

第３条　町に、総括責任者１人を置き、副町長をもって充てる。

２　総括責任者は、町長を補佐し、町における保有個人情報及び行政機関等匿名加工情報等（以下「保有個人情報等」という。）の管理に関する事務を総括する。

（保護責任者）

第４条　各課及び局（以下「課（局）」という。）に保護責任者１人を置き、課（局）長をもって充てる。

２　保護責任者は、課（局）における保有個人情報等の管理に関する事務を総括する。

３　保護責任者は、保有個人情報等を情報システムで取り扱う場合、当該情報システムの管理者と連携して、前項の事務を行う。

４　保護責任者は、次に掲げる組織体制を整備する。

⑴ 保有個人情報等を取り扱う職員が取扱規程等に違反している事実又は兆候を把握した場合の報告連絡体制

⑵ 保有個人情報等の漏えい、滅失又は毀損等（以下「漏えい等」という。）事案の発生又はおそれを把握した場合の報告連絡体制及び対応体制

（保護担当者）

第５条　課（局）に、保護担当者を置き、当該課（局）の分掌事務を統轄する職員であって、保護責任者が指定するものをもって充てる。

２　保護担当者は、保護責任者を補佐し、課（局）における保有個人情報等の管理に関する事務を行う。

（監査責任者）

第６条　町に、監査責任者１人を置き、総務課長をもって充てる。

２　監査責任者は、町における保有個人情報等の管理の状況について監査する。

（保有個人情報等の適切な管理のための委員会）

第７条　総括責任者は、保有個人情報等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、定期又は随時に開催することができる。

２　総括責任者は、委員会の開催に当たり、必要に応じて情報セキュリティ等について専門的な知識及び経験を有する者等の参加を求めることができる。

（教育研修）

第８条　総括責任者は、保有個人情報等の取扱いに従事する職員に対し、保有個人情報等の取扱いについて理解を深め、保有個人情報等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　総括責任者は、保有個人情報等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、保有個人情報等の適切な管理のため、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　総括責任者は、保護責任者及び保護担当者に対し、課（局）の現場における保有個人情報等の適切な管理のための教育研修を定期的に実施する。

４　保護責任者は、課（局）の職員に対し、保有個人情報等の適切な管理のため、総括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３章　職員の責務

第９条　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責任者、保護責任者及び保護担当者の指示に従い、保有個人情報等を取り扱わなければならない。

第４章　保有個人情報等の取扱い

（アクセス制限）

第10条　保護責任者は、保有個人情報等の秘匿性等その内容（個人識別の容易性（匿名化の程度等）、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性

質・程度等を考慮する。以下同じ。）に応じて、当該保有個人情報等にアクセス（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、保有個人情報等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等にアクセスをしてはならず、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11条　保護責任者は、職員が業務上の目的で保有個人情報等を取り扱う場合であっても、次に掲げる行為については、当該保有個人情報等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、保護責任者の指示に従い行うものとする。

(1) 保有個人情報等の複製

(2) 保有個人情報等の送信

(3) 保有個人情報等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等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12条　職員は、保有個人情報等の内容に誤りを発見した場合には、保護責任者の指示に従い、訂正等を行う。

（媒体の管理等）

第13条　職員は、保護責任者の指示に従い、保有個人情報等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、当該媒体の耐火金庫への保管、保管場所への施錠等の保有個人情報等の漏えい等を防止するための措置を講ずる。

２　職員は、保有個人情報等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ずる。

（誤送付等の防止）

第14条　職員は、保有個人情報等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又はチェックリストの活用等の必要な措置を講ずる。

（廃棄等）

第15条　職員は、保有個人情報等又は保有個人情報等が記録されている媒体（端末機器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、保護責任者の指示に従い、当該保有個人情報等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。

２　前項の場合において、当該情報の消去又は当該媒体の廃棄を委託するとき（２以上の段階にわたる委託を含む。）は、必要に応じて職員が消去若しくは廃棄に立ち会い、又は写真等を付した消去若しくは廃棄を証明する書類等を受け取り、委託先において消去又は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）

第16条　保護責任者は、保有個人情報等の秘匿性等その内容に応じて、台帳等を整備し、当該保有個人情報等の利用、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）

第17条　保有個人情報等が、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、クラウドサービス提供事業者が所在する外国又は個人データが保存されるサーバが所在する外国を含む。）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、保有個人情報等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５章　情報システムにおける安全の確保等

（アクセス制御）

第18条　保護責任者は、保有個人情報等（情報システムで取り扱うものに限る。第30

条を除き、以下この章及び次章において同じ。）の秘匿性等その内容に応じて、認証機能を設定する等の当該保有個人情報等へのアクセスを制御するために必要な措置を講ずる。

２　保護責任者は、前項に規定する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）

第19条　保護責任者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等へのアクセスの状況を記録し、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。

２　保護責任者は、アクセス記録の改ざん、窃取又は不正な削除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）

第20条　保護責任者は、保有個人情報等の秘匿性等その内容及びその量に応じて、当該保有個人情報等への不適切なアクセスの監視のため、保有個人情報等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）

第21条　保護責任者は、保有個人情報等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。

（外部からの不正アクセスの防止）

第22条　保護責任者は、保有個人情報等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）

第23条　保護責任者は、不正プログラムによる保有個人情報等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。

（情報システムにおける保有個人情報等の処理）

第24条　職員は、保有個人情報等について、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とし、処理終了後は不要となった情報を速やかに消去する。

２　保護責任者は、保有個人情報等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）

第25条　保護責任者は、保有個人情報等の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずる。

２　職員は、前項の措置を踏まえ、その処理する保有個人情報等について、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化（適切なパスワードの選択、その漏えい防止の措置等を含む。）を行う。

（記録機能を有する機器・媒体の接続制限）

第26条　保護責任者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等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・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。

（端末の限定）

第27条　保護責任者は、保有個人情報等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。

（端末の盗難防止等）

第28条　保護責任者は、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。

２　職員は、保護責任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29条　職員は、端末の使用に当たっては、保有個人情報等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）

第30条　職員は、情報システムで取り扱う保有個人情報等の重要度に応じて、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等の内容の確認、既存の保有個人情報等との照合等を行う。

（バックアップ）

第31条　保護責任者は、保有個人情報等の重要度に応じて、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。

（情報システム設計書等の管理）

第32条　保護責任者は、保有個人情報等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６章　電算室等の安全管理

（入退管理）

第33条　保護責任者は、保有個人情報等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「電算室等」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、利用及び持出しの制限又は検査等の措置を講ずる。

２　保護責任者は、保有個人情報等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、必要があると認めるときは、前項と同様の措置を講ずる。

３　保護責任者は、必要があると認めるときは、電算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。

４　保護責任者は、電算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。

（電算室等の管理）

第34条　保護責任者は、外部からの不正な侵入に備え、電算室等に施錠装置、警報装置及び監視設備の設置等の措置を講ずる。

２　保護責任者は、災害等に備え、電算室等に、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。

第７章　保有個人情報等の提供及び業務の委託等

（保有個人情報等の提供）

第35条　保護責任者は、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等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（電磁的記録を含む。）を取り交わす。

２　保護責任者は、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等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検査等を行うことにより当該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。

３　保護責任者は、個人情報保護法第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等を提供する場合において、必要があると認めるときは、個人情報保護法第70条の規定に基づき、前２項に規定する措置を講ずる。

（業務の委託等）

第36条　個人情報又は行政機関等匿名加工情報等（以下この条及び次条において「個人

情報等」という。）の取扱いに係る業務の全部又は一部を委託する場合には、個人情報等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ずる。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及び実施体制、個人情報等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。

(1) 個人情報等に関する秘密保持、目的外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。以下この条において同じ。）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) 個人情報等の複製等の制限に関する事項

(4) 個人情報等の安全管理措置に関する事項

(5) 個人情報等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等の消去及び媒体の返却に関する事項

(7) 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等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　保有個人情報等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等の範囲は、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　保有個人情報等の取扱いに係る業務の全部又は一部を委託する場合には、委託する業務に係る保有個人情報等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等の管理の状況について、年１回以上、原則として実地検査により確認する。

４　保有個人情報等の取扱いに係る業務の全部又は一部を委託先が再委託をする場合には、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等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実施する。保有個人情報等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　保有個人情報等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等の取扱いに関する事項を明記する。

６　保有個人情報等を提供し、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、保有個人情報等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。

第８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37条　個人情報等を取り扱い、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、上市町情報セキュリティ基本方針（平成27年上市町訓令第10号）及び上市町情報セキュリティ対策基準（平成27年上市町訓令第11号）を参考として、取り扱う保有個人情報等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９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38条　保有個人情報等の漏えい等安全管理の上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、その事案等を認識した職員は、直ちに当該保有個人情報等を管理する保護責任者に対し、保護担当者を通じて報告する。

２　保護責任者は、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。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　保護責任者は、直ちに総括責任者に当該事案の内容等（報告をしようとする時点において把握しているものに限る。）について報告するとともに、町長に対し報告するものとする。

４　保護責任者は、前項の規定による報告後において、当該事案の発生した経緯、被害状況等を調査し、個人情報等の漏えい等報告について（別記様式）により、総括責任

者に報告する。

５　総括責任者は、前項の規定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、被害状況等を町長に速やかに報告する。

６　保護責任者は、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課（局）に再発防止措置を共有する。

（個人情報保護法に基づく報告及び通知）

第39条　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、前条で定める事項と並行して、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。

（公表等）

第40条　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とともに、必要に応じて当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会へ情報提供を行うこととする。

第10章　監査及び点検の実施

（監査）

第41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章から前章までに規定する措置の状況を含む町における保有個人情報等の管理の状況について、定期及び必要に応じ随時に監査（外部監査の委託を含む。以下同じ。）を行い、その結果を総括責任者に報告する。

（点検）

第42条　保護責任者は、課（局）における保有個人情報等の記録媒体、処理経路、保管方法等について、定期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、その結果を総括責任者に報告する。

（評価及び見直し）

第43条　総括責任者、保護責任者等は、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等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。

附　則

この訓令は、公表の日から施行する。