高知市保有個人情報の安全管理のための措置に関する取扱要綱

（令和５年２月 24 日制定）

目次

第１章　総則

（趣旨）

第１条　この要綱は，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。）に定めるところにより，保有個人情報の安全管理のための必要かつ適切な措置に関し，必要な事項を定めるものである。

（定義）

第２条　用語の意義は，法及び高知市個人情報保護法施行条例（令和５年条例第３号）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　総括保護管理者は，市長を補佐し，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４条　保護管理者は，各課等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，保有個人情報を高知市情報資産管理運営規則（平成 19 年規則第 71 号）第２条第３号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５条　保護担当者は，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。

２　保護担当者は，各課等に１人以上置くものとする。

（監査責任者）

第６条　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。

第３章　教育研修

（教育研修）

第７条　総括保護管理者は，職員（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。）をいう。第９条及び第 37 条を除き，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定期的に行うものとする。

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定期的に行うものとする。

３　総括保護管理者は，保護管理者及び保護担当者に対し，課等の現場における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ものとする。

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８条　職員は，法の趣旨にのっとり，関連する法令及び規程等の規定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章　保有個人情報の取扱い

（アクセス制限）

第９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上で必要最小限の範囲に限るものとする。

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，また，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 10 条　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するとともに，職員は，保護管理者の指示に従って当該行為を行うものとする。

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媒体の外部への送付又は持ち出し

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 11 条　職員は，保有個人情報の内容に誤り等を発見した場合は，保護管理者の指示に従ってその訂正等を行うものとする。

（媒体の管理等）

第 12 条　職員は，保護管理者の指示に従って，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，耐火金庫への保管，施錠等を行うものとする。

２　職員は，保有個人情報が記録されている媒体を外部へ送付し，又は持ち出す場合は，原則として，パスワード，ＩＣカード，生体情報等（以下「パスワード等」という。）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，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 13 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，個別の事務又は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て複数の職員による確認，チェックリストの活用等，必要な措置を講ずるものとする。

（廃棄等）

第 14 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保有個人情報の消去又は当該媒体の廃棄を行うものとする。

２　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（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その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ものとする。

（保有個人情報の取扱状況の記録）

第 15 条　保護管理者は，保有個人情報の取扱状況等を一元的に管理するため所定の保有個人情報管理簿を作成し，保有個人情報の利用及び保管等の取扱いの状況を記録しなければならない。

２　前項の保有個人情報管理簿に記録する項目は，別表のとおりとする。

（外的環境の把握）

第 16 条　保護管理者は，保有個人情報を外国において取り扱う場合は，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等

（アクセス制御）

第 17 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。以下第６章（第 29 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，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は，パスワード等の管理に関する規定を整備（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の必要な措置を講ずるものとする。

（アクセス記録）

第 18 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。）を一定の期間保存するとともに，アクセス記録を定期的に分析するための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 19 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，必要な措置を講ずるものとする。

（管理者権限の設定）

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，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，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 21 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，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 22 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 23 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は，その対象を必要最小限に限るとともに，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。

２　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，前項の規定による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 24 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，暗号化のための必要な措置を講ずるものと

する。

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 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，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等（当該機器の更新への対応を含む。），必要な措置を講ずるものとする。

（端末の限定）

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，その処理を行う端末を限定するための必要な措置を講ずるものとする。

（端末の盗難防止等）

第 27 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，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いて，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 28 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に，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，必要な措置を講ずるものとする。

（入力情報の照合等）

第 29 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 30 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 31 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に，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 32 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，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若しくは監視設備による監視，外部電磁的記録媒体等の持込み，利用若しくは持ち出しの制限又は検査等の措置を講じ，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するとともに，パスワード等の管理に関する規定の整備（その定期又は随時の見直しを含む。）又はパスワード等の読取防止等を行うための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 33 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，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34条　保護管理者は，法第69条第２項の規定に基づき市長以外の者に保有個人情報を提供する場合は，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号の規定に基づき市長以外の者に保有個人情報を提供する場合は，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。

第９章　保有個人情報の取扱いの委託等

（業務の委託等）

第 35 条　保有個人情報の取扱いに係る業務の全部又は一部を外部に委託する場合は，高知市個人情報取扱業務委託基準（令和５年４月１日制定）に定める措置を講じなければならない。

２　公の施設（地方自治法（昭和22年法律第67号）第244条第１項に規定する公の施設をいう。）の管理を指定管理者（同法第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５年４月１日制定）に定める措置を講じなければならない。

３　保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合は，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。

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36条　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号に規定する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，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37条　職員は，保有個人情報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は，その事案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（職員に行わせることを含む。）については，直ちに行うものとする。

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，遅滞なく総括保護管理者及び広聴広報課長に報告するものとする。ただし，特に重大と認める事案が発生した場合は，当該事案の内容等を直ちに総括保護管理者及び広聴広報課長に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じ，総括保護管理者に当該措置の内容について報告するとともに，保護管理者は，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38条　保有個人情報の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ものについては，前条の報告及び措置と並行し，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39条　市長は，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を公表するとともに，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　市長は，公表が必要な保有個人情報の漏えいその他の市民の不安を招きかねない事案が発生した場合は，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40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，法その他関係法令及びこの要綱に基づく適正な管理のための措置の状況を含む保有個人情報の管理の状況について，定期に，及び随時に監査（外部監査及び他部署等による点検を含む。以下同じ。）を行うとともに，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41条　保護管理者は，各課等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，及び随時に点検を行うとともに，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42条　保護管理者は，第40条に規定する監査又は前条に規定する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。

附　則

この要綱は，令和５年４月１日から施行する。

別表（第15条関係）

番号	記録項目	内容
1	取扱い年度	個人情報管理簿が管理する保有個人情報の取扱い年度を記載する。
2	実施機関名	高知市個人情報保護法施行条例第２条に規定する実施機関の名称を記載する。
3	課名	保有個人情報が利用に供される事務をつかさどる課室等の名称を記載する。
4	所管課コード	部課別コード表の４桁の数字を記載する。
5	№.	通し番号を記載する。
6	保有個人情報の名称	保有個人情報の名称を個人情報ファイル又は散在情報の単位ごとに記載する。
7	利用の目的	保有個人情報の利用の目的を記載する。
8	所掌事務又は業務の名称	保有個人情報を利用する事務又は業務の名称を記載する。
9	所掌事務又は業務の根拠法令	保有個人情報を利用する事務又は業務の根拠法令（条例を含む）を記載する。
10	個人番号利用事務等	番号法に規定する「個人番号利用事務」若しくは「個人番号関係事務」に該当する場合に記載する。
11	記録される個人の範囲	保有個人情報に記録される本人の範囲を記載する。

12	記録項目	保有個人情報に記録される項目を記載する。
13	要配慮個人情報の有無	法第２条第３項に規定する要配慮個人情報の有無を記載する。
14	収集方法	収集の相手方及び手段を記載する。
15	利用目的の明示	保有個人情報の利用の目的の明示方法を記載すること。法第 62 条に規定する明示の適用除外の場合は，該当条項各号のいずれかの号を記載する。
16	保有個人情報の種別	保有個人情報の個人情報ファイル又は散在情報の別を記載する。
17	（個人情報ファイルに該当する場合） 人数	個人情報ファイルに記録される本人の数を記載する。
18	（個人情報ファイルに該当する場合） ファイル簿の作成・公表の要否	個人情報ファイル簿の作成・公表の要否を記載する。法第 75 条第２項及び第３項に規定する作成・公表の適用除外の場合は，該当条項各号のいずれかの号を記載する。
19	（個人情報ファイルに該当する場合） 処理形態	個人情報ファイルが電子計算機処理によるもの又はマニュアル（手作業）処理によるものかを記載する。
20	（個人情報ファイルに該当する場合） 政令第 21 条第７項に該当する個人情報ファイルの名称	個人情報ファイルがマニュアル（手作業）処理によるもので，その利用目的及び記録範囲が他の電子計算機処理による個人情報ファイルの利用目的及び記録範囲の範囲内である場合は，該当する他の電子計算機処理による個人情報ファイルの名称を記載する。
21	経常的な利用先	保有個人情報の経常的な利用先（目的内利用又は法第 69 条第２項第２号に基づく目的外利用）がある場合，利用先の課名を記載する。
22	内部における利用の制限の有無	法第 69 条第４項に基づく実施機関内部における利用の制限の有無について記載する。
23	経常的な提供先	保有個人情報の経常的な提供先（目的内提供又は法第 69 条第２項第３号及び第４号に基づく目的外提供）がある場合，提供先の名称を記載する。
24	外部委託の有無	保有個人情報の取扱いに関する外部委託の有無を記載する。
25	保有開始年月日	保有個人情報の保有を開始した年月日を記載する。
26	変更年月日	個人情報管理簿の記載内容に変更があった場合の年月日を記載する。
27	保有終了年月日	保有個人情報の保有を終了した年月日を記載する。
28	備考	その他，参考となる事項（個人情報ファイルの作成時期等）を記載する。

備考　保有個人情報管理簿に記載を要しない保有個人情報は，次に掲げる場合とする。

⑴　既に保有個人情報管理簿に記載している保有個人情報に含まれる記録情報の全部又は一部の写しを作成し，作業用又は決裁用として使用する場合。ただし，情報を新たに付加する場合を除く。

⑵　事故等に備えて予備的に作成し，バックアップ等のために保有する場合。ただし，保有個人情報を新たに付加する場合を除く。