令和５年３月２４日制定

三重県議会個人情報適正管理指針

１　指針の意義

この指針は、三重県議会個人情報保護条例（令和５年三重県条例第１号。以下「条例」という。）第９条第１項の規定等を踏まえ、議会の保有する個人情報、個人番号及び特定個人情報（以下「保有個人情報等」という。）の安全管理のために必要かつ適切な措置として示すものである。

また、保有個人情報等の漏えい等が生じた場合に本人が被る権利利益の侵害の大きさを考慮し、事務の規模及び性質、保有個人情報の取扱状況（取り扱う保有個人情報の性質及び量を含む。）、保有個人情報等を記録した媒体の性質等に起因するリスクに応じた必要かつ適切な措置を講じることが求められる。

なお、情報セキュリティ等に係ることについては、三重県電子情報安全対策基準の規程について併せて確認することとする。

２　個人情報窓口

保有個人情報等の取扱いに関する案内及び相談、保有個人情報開示請求等の受付は、議会事務局で行うものとする。

なお、窓口の利用時間は、開庁日の８時30分から17時15分までとする。

３　管理体制

【総括保護管理者】

(1)　議会事務局に、総括保護管理者を一人置くこととし、議会事務局長をもって充てる。

総括保護管理者は、議長を補佐し、議会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任に当たる。

【保護管理者】

(2)　議会事務局の各課（以下「各課」という。）に、保護管理者を一人置くこととし、課長又はこれに代わる者をもって充てる。

保護管理者は、各課における保有個人情報等の適切な管理を確保する任に当たる。保有個人情報等を情報システムで取り扱う場合、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】

(3)　各課に、当該課の保護管理者が指名する保護担当者を１人又は複数人置く。

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等の管理に関する事務を担当する。

保護担当者は、原則、「三重県情報公開・個人情報保護制度推進要綱」第５条に定める「推進員」を充てるものとする。

【監査責任者】

(4) 議会事務局における個人情報の保護対策を担当する課（以下「個人情報保護担当課」という。）を総務課とするとともに、監査責任者を１人置くこととし、総務課長をもって充てる。

監査責任者は、保有個人情報等の管理の状況について監査する任に当たる。

4 教育研修等

総括保護管理者は、保有個人情報等の適切な管理のために、保有個人情報等の取扱いに従事する職員、保護管理者及び保護担当者に対して、知事部局の総括保護管理者等が実施する教育研修等への参加の機会を付与する等の必要な措置を講ずる。

5 職員の責務

職員は、条例の趣旨にのっとり、関連する法令及び規程等の定め並びに総括保護管理者、保護管理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。

6 保有個人情報等の取扱い

【アクセス制限】

(1) 保護管理者は、保有個人情報等の秘匿性等その内容（注）に応じて、当該保有個人情報等にアクセスする（紙等に記録されている保有個人情報等に接する行為を含む。以下同じ。）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。

(注) 特定の個人の識別の容易性の程度、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。

(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】

(4) 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、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、保護管理者の指示に従い行う。

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ち出し
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】
(5)　職員は、保有個人情報等の内容に誤り等を発見した場合には、保護管理者に報告するとともに、その指示に従い、訂正等を行う。
【媒体の管理等】
(6)　職員は、保護管理者の指示に従い、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、耐火金庫への保管、施錠等を行う。また、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、事前に保護管理者の許可を得るとともに、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】
(7)　職員は、保有個人情報等を含む電磁的記録又は媒体（注）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。
(注）文書の内容だけでなく、付加情報（ＰＤＦファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合があることに注意する。
【廃棄等】
(8)　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。
　特に、保有個人情報等の消去や保有個人情報等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。）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。
【保有個人情報等の取扱状況の記録】
(9)　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報等の利用及び保管等の取扱いの状況について記録する。

7　情報システムにおける安全の確保等
【アクセス制御】
(1)　保護管理者は、保有個人情報等（情報システムで取り扱うものに限る。7（情報システムにおける安全の確保等）（(15)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（注）。

（注）アクセス制御の措置内容は、6（保有個人情報等の取扱い）（1）により設定した必要最小限のアクセス権限を具体化するものである必要がある。

(2)　保護管理者は、（1）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。

【アクセス記録】

(3)　保護管理者は、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。

(4)　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等の防止のために必要な措置を講ずる。

【管理者権限の設定】

(5)　保護管理者は、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】

(6)　保護管理者は、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】

(7)　保護管理者は、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】

(8)　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し、課内の職員に対し、定期的に声がけを行う。

【暗号化】

(9)　保護管理者は、保有個人情報等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。職員（注）は、これを踏まえ、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、適切に暗号化を行う。

（注）職員が行う暗号化には、適切なパスワードの選択、その漏えい等の防止の措置等が含まれる。

【記録機能を有する機器・媒体の接続制限】

（10）保護管理者は、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】

（11）保護管理者は、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】

（12）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。

（13）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】

（14）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】

（15）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、入力時にダブルチェックを行う等、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】

（16）保護管理者は、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】

（17）保護管理者は、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。

8　情報システム室等の安全管理

【設置場所等の管理】

（1）　保護管理者は、外部からの不正な侵入に備え、設置場所に施錠装置の設置等の措置を講ずる。

（2）　保護管理者は、災害等に備え、設置場所に、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。

9　保有個人情報の提供

【保有個人情報の提供】

(1)　保護管理者は、条例第 12 条第 2 項第 3 号及び第 4 号の規定に基づき、議会以外の者に保有個人情報を提供する場合には、条例第 13 条の規定に基づき、必要に応じ、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)　保護管理者は、条例第 12 条第 2 項第 3 号及び第 4 号の規定に基づき、議会以外の者に保有個人情報を提供する場合には、条例第 13 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。

10　特定個人情報の取扱い

【個人番号の利用の制限】

(1)　保護管理者は、個人番号の利用については、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）であらかじめ定めた事務に限定する。

【特定個人情報の提供の求めの制限】

(2)　個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）を処理するために必要な場合その他番号法で定める場合を除き、個人番号の提供を求めてはならない。

【特定個人情報ファイルの作成の制限】

(3)　個人番号利用事務等を処理するために必要な場合その他番号法で定める場合を除き、特定個人情報ファイルを作成してはならない。

【特定個人情報の収集･保管の制限】

(4)　番号法第 19 条各号のいずれかに該当する場合を除き、特定個人情報（他人の個人番号を含むものに限る。）を収集又は保管してはならない。

【取扱区域】

(5)　保護管理者は、特定個人情報を取り扱う事務を実施する区域を明確にし、物理的な安全管理措置を講ずる。

11　個人情報の取扱いの委託

【事務の委託等】

個人情報取扱事務を外部委託する際は、「三重県事務局個人情報取扱事務委託基準」に基づき、委託を受けたものが個人情報の保護のために講ずべき措置を明らかにしなければならない。

12　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】

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。

13　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】

(1)　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管理者に報告する（注）。

（注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず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。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、個人情報の本人及び関係機関への対応のために講じた措置等について、速やかに個人情報保護担当課を経由して、総括保護管理者に報告する。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、被害状況等を議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、同種の業務を実施している課に再発防止措置を共有する。

(6)　個人情報保護担当課は、（3）の報告を受けたときには、総務部情報公開課にも報告する。

【条例に基づく通知】

(7)　漏えい等が生じた場合であって条例第 11 条の規定による本人への通知を要する場合には、(1)から(5)までと並行して、速やかに所定の手続を行う。

【公表等】

(8)　条例第 11 条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等の本人への対応等の措置を講ずる。

14　監査及び点検の実施

【監査】

(1)　監査責任者は、保有個人情報等の適切な管理を検証するため、３（管理体制）から 13（安全管理上の問題への対応）までに記載する措置の状況を含む議会における保有個人情報等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者に報告する。

【点検】

(2)　保護管理者は、各課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、その結果を総括保護管理者に報告する。

【評価及び見直し】

(3)　総括保護管理者、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

この指針は、令和５年４月１日から施行する。