愛知県公立大学法人における特定個人情報等の取扱いに関する規程

平成 27 年 12 月 7 日制定

第１章　特定個人情報等の安全管理に関する基本方針

（特定個人情報等の保護に関する考え方）

第１条　愛知県公立大学法人（以下「本法人」という。）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「番号利用法」という。）に定められた事務において特定個人情報等を取り扱う。番号利用法においては、特定個人情報等の利用範囲を限定する等、厳格な保護措置を定めていることから、特定個人情報等の取扱いに関する規程を定め、教職員等に遵守させる等の措置を講じ、適正に特定個人情報等を取り扱うために必要な事項を定める。

（特定個人情報等の保護方針）

第２条　特定個人情報等を取り扱う全ての事務において、次のとおり特定個人情報等を適正に取り扱う。

(1) 特定個人情報等の適正な取扱いに関する次の法令等を遵守する。

ア　番号利用法

イ　個人情報の保護に関する法律（平成 15 年法律第 57 号）

ウ　個人情報の保護に関する法律施行条例（令和 4 年愛知県条例第 51 号）

エ　特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成 26 年特定個人情報保護委員会告示第 6 号）

オ　愛知県公立大学法人情報セキュリティポリシー

カ　愛知県公立大学法人情報セキュリティガイドライン

(2) 特定個人情報等の漏えい、滅失及び毀損の防止その他の適切な管理のために必要な安全管理措置を講ずる。

(3) 特定個人情報等は、番号利用法に定められた事務のうち必要な手続の利用目的の達成に必要な範囲内で適正に利用、収集・保管及び提供をするとともに、不要となった場合は速やかに廃棄する。また、目的外利用を防止するための措置を講ずる。

(4) 特定個人情報等を取り扱う事務の全部又は一部を委託する場合には、委託先（再委託先を含む。）において、番号利用法に基づき本法人自らが果たすべき安全管理措置と同等の措置が講じられるよう、必要かつ適切な監督を行う。

(5) この規程は、継続的に見直し、その改善に努める。

第２章　特定個人情報等の安全管理措置

第１節　定義

（定義）

第３条　この規程における用語の定義は、番号利用法第 2 条第 5 項、第 8 項、第 9 項、第 11 項及び第 13 項の定めるところによるほか、次に定めるところによる。

(1) 特定個人情報等　特定個人情報及び個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。以下同じ。）をいう。

(2) 個人番号関係事務　個人番号を取扱う関係事務をいう。

(3) 取扱要領　取扱い業務の範囲ごとに、特定個人情報等の取扱いを定めた要領をいう。
(4) 規程等　この規程及び取扱要領をいう。
(5) 特定個人情報システム　個人番号をデータベースに記録し、読み出し、更新し、及び削除するシステムをいう。ただし、データベースエンジンを搭載しない特定個人情報ファイルを除く。
(6) 取扱区域　特定個人情報等を取り扱う事務を実施する区域をいう。
(7) 情報システム室　全学的なネットワーク又は重要な情報システムの基幹機器を設置し、当該機器の管理運用を行うためのサーバ室等をいう。
(8) 情報システム室等　情報システム室及び特定個人情報等を取り扱うためにこれに準じたセキュリティ対策が求められる区域をいう。
(9) 課室　愛知県立大学及び愛知県立芸術大学並びに法人事務部門及び監査室の各課室をいう。

（取扱い事務の範囲）
第４条　本法人が特定個人情報等を取り扱う事務は、原則として以下のとおりとする。
(1) 給与所得・退職所得に係る源泉徴収票作成事務
(2) 住民税特別徴収関係事務
(3) 共済組合関係届出事務
(4) 健康保険・厚生年金保険関係届出事務
(5) 国民年金第３号被保険者関係届出事務
(6) 雇用保険関係届出事務
(7) 労働災害補償保険法関係届出事務
(8) 報酬等に係る支払調書作成事務
(9) 財産形成貯蓄制度関係届出事務
(10) 組合員貯金・福祉貯金関係届出事務

第２節 管理体制

（総括保護管理者及び最高情報セキュリティ責任者）
第５条　本法人に、総括保護管理者及び最高情報セキュリティ責任者を置く。
２　総括保護管理者には法人事務部門長をもって充て、最高情報セキュリティ責任者には理事長（愛知県公立大学法人情報セキュリティポリシーⅡの１に定める者）をもって充てる。
３　総括保護管理者は、最高情報セキュリティ責任者を補佐し、特定個人情報等の管理に関する事務を総括する任に当たる。
４　総括保護管理者は、特定個人情報等に関する重要な決定、連絡・調整等を行うために必要があるときは、関係教職員を構成員とする部会を設け、定期に又は随時に開催することができる。
５　最高情報セキュリティ責任者は、特定個人情報等を扱う情報システム、ネットワーク等の統括責任者とし、この規程の第６節及び第７節の規定その他の特定個人情報ファイルの適切な管理状況について監督する任に当たる。
６　最高情報セキュリティ責任者は、特定個人情報等の情報セキュリティ全般に関する重要な決定、連絡・調整等を行うために必要があるときは、関係職員を構成員とする会議を随時に開催することができる。

（保護管理者）
第６条　特定個人情報等を取り扱う課室に、保護管理者を１人置くこととし、当該課室の長又は当該課室の長が指名する者を持って充てる。
２　保護管理者は、次の任務を行う。
(1) 課室における特定個人情報等を適切に管理すること。
(2) 事務取扱担当者及びその役割を指定すること。
(3) 特定個人情報ファイルの取扱状況を確認するために次に掲げる内容を記録すること。
ア　特定個人情報ファイルの名称
イ　特定個人情報ファイルを利用する課室
ウ　特定個人情報ファイルの利用目的
エ　特定個人情報ファイルに記録される個人の範囲
オ　特定個人情報ファイルの収集方法

（事務取扱担当者）
第７条　特定個人情報等を取り扱う者として、事務取扱担当者を置くことができる。

（取扱要領）
第８条　個人番号関係事務の主たる保護管理者は、当該個人番号関係事務について取扱要領を定めることとし、次に掲げる事項を記載する。
(1)　事務取扱担当者が規程等に違反している事実又は兆候を把握した場合の保護管理者への報告連絡体制及び手順
(2)　保護管理者が特定個人情報等の漏えい、滅失、毀損等（以下「漏えい等」という。）の事案の発生又は兆候を把握した場合の総括保護管理者への報告連絡体制及び手順
(3)　特定個人情報等の収集・保管、利用及び廃棄に係る運用体制及び手順
(4)　特定個人情報等を他の課室と取り扱う場合の任務分担及び責任体制
(5)　特定個人情報等の漏えい等の事案の発生又は兆候を把握した場合の対応体制及び手順

第３節　教育研修
第９条　総括保護管理者は、特定個人情報等の取扱いに従事する事務取扱担当者に対し、特定個人情報等の取扱いについて理解を深め、特定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　総括保護管理者は、保護管理者に対し、所属における特定個人情報等の適正な管理のために必要な教育研修を行う。
３　最高情報セキュリティ責任者は、事務取扱担当者に対し、特定個人情報等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行う。
４　最高情報セキュリティ責任者は、事務取扱担当者のうち特定個人情報ファイルを取り扱う事務に従事する者に対し、番号利用法第 29 条の２に定めるサイバーセキュリティの確保に関する事項その他の事項に関する研修を行う。

第４節　教職員の責務
第 10 条　事務取扱担当者は、番号利用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及び保護管理者の指示に従い、特定個人情報等を適切に取り扱わなければならない。

2　教職員は、特定個人情報等の漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者が規程等に違反している事実又は兆候を把握した場合は、速やかに保護管理者に報告しなければならない。

第５節　特定個人情報等の取扱い

（取扱制限）

第 11 条　保護管理者は、特定個人情報等を取り扱う者をその利用目的を達成するために必要最小限の事務取扱担当者に限る。

2　取扱権限を有しない教職員は、特定個人情報等を取り扱ってはならない。

3　事務取扱担当者は、取扱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特定個人情報等を取り扱ってはならない。

4　事務取扱担当者は、業務上の目的で特定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、保護管理者の指示に従い行う。

(1) 特定個人情報等の複製（PDF 等の文書ファイルの作成を含む。）
(2) 特定個人情報等の送信
(3) 特定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) 特定個人情報等の印刷
(5) 紙媒体の特定個人情報等の読取り機器等による電子化

（誤りの訂正等）

第 12 条　事務取扱担当者は、特定個人情報等の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行う。

（媒体等の廃棄）

第 13 条　事務取扱担当者は、特定個人情報等が記録されている電磁的記録媒体等（端末、サーバに内蔵されているハードディスク及びデータ等を含む。）が不要となった場合には、保護管理者の指示に従い、当該特定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削除又は当該媒体の廃棄をしなければならない。

2　事務取扱担当者は、特定個人情報等が記載された紙媒体を保存期間経過後に速やかに焼却、細断、粉砕等の復元不可能な方法により廃棄しなければならない。

3　事務取扱担当者は、特定個人情報等を記録されている紙媒体又は電磁的記録媒体等を削除又は廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。

（特定個人情報等の取扱状況の記録）

第 14 条　保護管理者は、当該特定個人情報等の利用、保管等の状況について記録する。

（特定個人情報等の利用の制限）

第 15 条　事務取扱担当者は、取扱要領において定める方法以外の方法で特定個人情報等を利用してはならない。

（個人番号の提供の求めの制限）
第 16 条　事務取扱担当者は、個人番号関係事務を処理するために必要な場合その他の番号利用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）
第 17 条　事務取扱担当者は、個人番号関係事務を処理するために必要な場合その他の番号利用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。

（特定個人情報等の収集・保管の制限）
第 18 条　教職員は、番号利用法第 19 条各号のいずれかに該当する場合を除き、特定個人情報等を収集し、又は保管してはならない。

（取扱区域）
第 19 条　保護管理者は、取扱区域を明確にし、物理的な安全管理措置を講ずる。
２　保護管理者は、取扱区域が本法人の管理外となる場合であっても、本法人と同等以上の措置が講じられるよう、取扱区域の管理先を監督する。

（第三者の閲覧防止）
第 20 条　保護管理者は、事務取扱担当者が端末の使用に当たり、背後等から第三者により特定個人情報等を閲覧できないよう、座席配置の工夫等、必要な措置を講ずる。
２　事務取扱担当者は、第三者が特定個人情報等の印刷された紙媒体において個人番号を閲覧できないよう必要な措置を講ずる。
３　事務取扱担当者は、端末の使用に当たり、特定個人情報等が第三者に閲覧されることのないよう、特定個人情報等を取り扱う以外の場合は、特定個人情報システムからログオフを行う等、特定個人情報等が漏えいしないための必要な措置を講ずる。
４　保護管理者は、特定個人情報システムの使用中に一定時間、何の操作もなく経過した場合は、再度、認証機能により事務取扱担当者の正当性を確認する等の必要な措置を講ずる。

（特定個人情報等の持出し）
第 21 条　特定個人情報等の取扱区域外への持出しは、個人番号利用事務等を実施する取扱区域間を搬送する場合に限る。
２　特定個人情報等を取扱区域外へ持ち出す場合には、特定個人情報等を含む紙媒体及び外部記録媒体を封かんし、第三者が容易に特定個人情報等を閲覧できないよう必要な措置を講ずる。
３　特定個人情報等を含む紙媒体及び外部記録媒体の搬送は、事務取扱担当者による搬送を原則とし、同一日に完了する。なお、やむを得ず郵送する場合は、簡易書留等で記録する。
４　特定個人情報等を含む紙媒体及び外部記録媒体の搬送を委託するに当たっては、厳封し、紛失又は盗難による漏えい等に対する必要な措置を講ずる。
５　特定個人情報等を含む外部記録媒体の搬送に当たっては、必ず特定個人情報ファイルを暗号化し、復号化に必要となるパスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）は外部記録媒体と別に搬送し、又は電子的な方法等により搬送先に通知する。

第６節　特定個人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、特定個人情報システムの利用に当たっては、パスワード等を使用して権限や利用者を識別する機能（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。

２　保護管理者は、事務取扱担当者が異動、退職、死亡等により特定個人情報等へのアクセスが不要となった時点で特定個人情報システムを即時に利用できなくなるよう必要な措置を講ずる。

３　保護管理者は、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。

４　事務取扱担当者は、特定個人情報システムを利用する場合に、利用者を一意に特定できるアカウントを利用して特定個人情報等へのアクセスを行う。

５　事務取扱担当者は、特定個人情報システムのアカウントを共用してはならない。

６　保護管理者は、データベースに記録している特定個人情報等へのアクセスを事務取扱担当者に限定するために必要な措置を講ずる。

（アクセス記録）

第 23 条　保護管理者は、特定個人情報システムの利用に当たっては、特定個人情報等へのアクセス状況を記録し、その記録を一定の期間保存し、定期に又は随時に分析するために必要な措置を講ずる。また、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。

２　保護管理者は、アクセス記録の分析、搾取等による特定個人情報等の漏えい等の防止のため、アクセス記録に特定個人情報等を記録しない。

（アクセス状況の監視）

第 24 条　保護管理者は、当該特定個人情報等への不適切なアクセスの監視のため、アクセス記録の定期的な確認等の必要な措置を講ずる。

２　保護管理者は、事務取扱担当者が特定個人情報システムを使用する必要がない場合には、アクセスしないよう指導・監督する。

３　事務取扱担当者は、業務上の必要がない場合には、特定個人情報システムを使用してはならない。

（管理者権限の設定）

第 25 条　保護管理者は、特定個人情報システムの管理者権限が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、管理者権限を必要最小限としなければならない。

（外部からの不正アクセスの防止）

第 26 条　特定個人情報システムの外部からの不正アクセスを防止するために必要な措置を講ずる。

２　保護管理者は、特定個人情報システムに不正アクセス等がないか、把握に努めなければならない。

（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、特定個人情報システムに対して、ファームウエアのアップデート及

びソフトウェアのセキュリティパッチ適用を適切に行い、常にセキュリティが保たれる状態にする。
２　保護管理者は、特定個人情報システムに対して、システムで使用しているＯＳ、ミドルウェア等のメーカーサポートが切れることのないよう必要な措置を講ずる。
３　保護管理者は、特定個人情報システムに対して、その他不正プログラムの感染防止等に必要な措置を講ずる。

（ファイル管理）
第 28 条　保護管理者は、特定個人情報ファイルの管理を特定のフォルダに限定する等の措置を講じることで、特定個人情報ファイルの所在を常に把握し、特定個人情報ファイルの管理を行う。

（暗号化）
第 29 条　事務取扱担当者は、インターネットと接続されたネットワークに特定個人情報ファイルを保存しなければならない場合には、暗号化等の必要な措置を講ずる。

（入力情報の照合等）
第 30 条　主たる保護管理者は、事務取扱担当者が誤った個人番号を特定個人情報システムに登録しないよう、事務取扱担当者を監督する。

（バックアップ）
第 31 条　保護管理者は、特定個人情報システム及びそのデータのバックアップを作成し、分散保管する場合は、必要な安全措置を講ずる。バックアップデータに個人番号が含まれる場合には、特定個人情報等として取り扱う。

（特定個人情報システム設計書等の管理）
第 32 条　保護管理者は、特定個人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留意する。

（端末の限定）
第 33 条　個人番号関係事務の保護管理者は、特定個人情報等の処理を行う端末を限定するために必要な措置を講じなければならない。

（端末の盗難防止等）
第 34 条　保護管理者は、特定個人情報ファイルが存在する端末の盗難又は紛失の防止のため、当該端末の固定、執務室の施錠等の必要な措置を講ずる。
２　事務取扱担当者は、保護管理者が必要と認めるときを除き、特定個人情報等が保存された端末を外部へ持ち出してはならない。

第７節　情報システム室等の安全管理

（入退管理）
第 35 条　最高情報セキュリティ責任者は、法人内に情報システム室を整備する。
２　最高情報セキュリティ責任者又は保護管理者は、情報システム室等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。

3　保護管理者は、特定個人情報等を記録する媒体等の保管を施錠可能な机又は書庫、施錠可能な保管庫等に限定し、事務取扱担当者以外が容易に持ち出すことができない措置を講ずる。

4　最高情報セキュリティ責任者又は保護管理者は、情報システム室等の出入口の特定化による入退管理の容易化、所在表示の制限等の措置を講ずる。

（情報システム室等の管理）

第 36 条　保護管理者は、情報システム室等が法人外に設置される場合には、最高情報セキュリティ責任者の承認を受けるとともに、最高情報セキュリティ責任者の定期的な点検を受ける。

2　最高情報セキュリティ責任者は、法人外の情報システム室等において適切な特定個人情報等の取扱いが担保されない可能性があると判断する場合には、情報システム室等の設置を許可しない。

3　最高情報セキュリティ責任者が整備する情報システム室は、愛知県公立大学法人情報セキュリティポリシー及び愛知県公立大学法人情報セキュリティガイドラインを遵守し安全管理措置を講ずる。

第８節　特定個人情報等の提供及び業務の委託等

（特定個人情報等の提供）

第 37 条　保護管理者は、番号利用法で限定的に明記された場合を除き、特定個人情報等を提供してはならない。

2　保護管理者は、番号利用法の規定により特定個人情報等を提供する場合には、通信経路における情報漏えい等を防止するための措置を講ずる。

（委託を受けた者に対するセキュリティ対策）

第 38 条　保護管理者は、個人番号関係事務の全部又は一部を委託する場合には、委託を受けた者において、本法人が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。

2　保護管理者は、個人番号関係事務の全部又は一部の委託をする際には、委託を受けた者において、別に定める個人情報取扱事務委託基準を遵守させるとともに、本法人が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。

3　保護管理者は、個人番号関係事務の全部又は一部の委託を受けた者が再委託をする際には、本法人が果たすべき安全管理措置と同等の措置が講じられることを確認した上で再委託の諾否を判断しなければならない。

第９節　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 39 条　特定個人情報等の漏えい等の安全確保の上で問題となる事案が発生した場合に、その事実を知った教職員等は、直ちに当該特定個人情報等を管理する保護管理者に報告する。

２　保護管理者は、事案の発生した経緯、被害状況等の事務を所管する事務部門長及び総括保護管理者に報告する。
３　総括保護管理者は、必要があると認めるときは、関係機関（個人情報保護委員会、文部科学省、愛知県等）に事案を報告する。
４　保護管理者は、自ら管理責任を有する特定個人情報等が外部に流出した可能性があるときは、速やかにその事実を当該特定個人情報等の本人に対して連絡するとともに、本人及びその関係者が二次的な被害に遭うことを防止するための必要な措置を講ずる。

（再発防止措置及び公表等）
第 40 条　特定個人情報等の漏えい等の事案が発生した場合、事務を所管する事務部門長及び総括保護管理者は、関係部署と協力し事案の発生した原因の分析及び再発防止のために必要な措置を講じるとともに、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。

第 10 節　監督及び点検の実施

（監督）
第 41 条　総括保護管理者は、この規程の遵守状況について定期に又は必要に応じ随時監督する。
２　保護管理者は、総括保護管理者から改善の必要があると指摘された事項について、速やかに必要な措置を講じなければならない。

（自己点検）
第 42 条　保護管理者は、取扱要領に基づく特定個人情報等の管理の状況について、定期に又は必要に応じ随時点検する。
２　総括保護管理者は、必要があると認めるときは、保護管理者に対し、点検結果の報告を求めることができる。

（規程等の見直し）
第 43 条　総括保護管理者は、監督及び点検の結果により、この規程の見直しが必要であると認められる場合には、この規程を見直す。
２　主たる保護管理者は、監督及び点検の結果により、取扱要領の見直しが必要であると認められる場合には、取扱要領を見直す。

附則
この規程は、平成 27 年 12 月 7 日から施行する。
附則
この規程は、平成 27 年 12 月 25 日から施行する。
附則
この規程は、平成 28 年 1 月 1 日から施行する。
附則
この規程は、令和 3 年 4 月 1 日から施行する。
附則

この規程は、令和５年４月１日から施行する。