○国立大学法人上越教育大学個人情報保護細則

（平成17年３月16日細則第４号）

最終改正　令和６年１月23日細則第１号

（趣旨）

第１条　この細則は、国立大学法人上越教育大学個人情報保護規程（平成17年規程第５号。以下「規程」という。）第38条の規定に基づき、個人情報の適切な管理について必要な事項を定める。

（定義）

第２条　この細則における用語の意義は、規程第２条の定めるところによる。

（アクセス制限）

第３条　規程第３条に定める保護管理者及び保護担当者（以下「保護管理者等」という。）は、個人データ及び保有個人情報(以下「個人データ等」という。)の秘匿性等その内容に応じて、当該個人データ等にアクセスする権限を有する役員又は職員（派遣労働者を含む。以下「役職員等」という。）の範囲と権限の内容を、当該職員等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役職員等は、保有個人情報にアクセスしてはならない。

３　役職員等は、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。

（複製等の制限）

第４条　役職員等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、保護管理者等は、次の各号に掲げる行為については、当該個人データ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限定し、役職員等は、保護管理者等の指示に従って行わなければならない。

(1) 個人データ等の複製

(2) 個人データ等の送信

(3) 個人データ等が記録されている媒体の外部への送付又は持出し

(4) その他個人データ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５条　役職員等は、個人データ等の内容に誤り等を発見した場合には、保護管理者等の指示に従い、訂正等を行うものとする。

（媒体の管理等）

第６条　役職員等は、保護管理者等の指示に従い、個人データ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、施錠等を行うものとする。

２　個人データ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ものとする。

（誤送付等の防止）

第７条　役職員等は、個人データ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データ等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。

（廃棄等）

第８条　役職員等は、個人データ等又は個人データ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、保護管理者等の指示に従い、当該個人データ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ものとする。

２　個人データ等の消去や個人データ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。）は、必要に応じて役職員等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ものとする。

（取扱状況の記録）

第９条　保護管理者等は、個人データ等の秘匿性等その内容に応じて、台帳等を整備して、当該個人データ等の利用及び保管等の取扱いの状況について記録するものとする。

（外的環境の把握）

第１０条　個人データ等が、外国において取り扱われる場合は、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、個人データ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。

（アクセス制御）

第１１条　保護管理者等は、個人データ等（情報システムで取り扱うものに限る。以下第23条を除き同じ。）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　保護管理者等は、前項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ものとする。

（アクセス記録の取得等）

第１２条　保護管理者等は、個人データ等の秘匿性等その内容に応じて、当該個人データ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。）を一定の期間保存するとともに、定期又は随時にアクセス記録を分析するものとする。

２　保護管理者等は、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１３条　保護管理者等は、個人データ等の秘匿性等その内容及びその量に応じて、当該個人データ等への不適切なアクセスの監視のため、個人データ等を含むか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の必要な措置を講ずるものとする。

（管理者権限の設定）

第１４条　保護管理者等は、個人データ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ものとする。

（外部からの不正アクセスの防止）

第１５条　保護管理者等は、個人データ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ものとする。

（不正プログラムによる漏えい等の防止）

第１６条　保護管理者等は、不正プログラムによる個人データ等の漏えい、滅失又は毀損（以下「漏えい等」という。）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個人データ等の処理）

第１７条　役職員等は、個人データ等について、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ものとする。この場合において、保護管理者等は、当該個人データ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ものとする。

（暗号化）

第１８条　保護管理者等は、個人データ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ものとする。

２　役職員等は、前項の措置を踏まえ、その処理する個人データ等について、当該個人データ等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１９条　保護管理者等は、個人データ等の秘匿性等その内容に応じて、当該個人データ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ものとする。

（端末の限定）

第２０条　保護管理者等は、個人データ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ものとする。

（端末の盗難防止等）

第２１条　保護管理者等は、端末の盗難又は紛失の防止のため、端末の固定及び設置する場所の施錠等の必要な措置を講ずるものとする。

２　役職員等は、保護管理者等が必要が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２２条　役職員等は、端末の使用に当たっては、個人データ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ものとする。

（入力情報の照合等）

第２３条　役職員等は、情報システムで取り扱う個人データ等の重要度に応じて、入力原票と入力内容との照合、処理前後の当該個人データ等の内容の確認、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２４条　保護管理者等は、個人データ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ものとする。

（情報システム設計書等の管理）

第２５条　保護管理者等は、個人データ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ものとする。

（情報システム室等の入退管理）

第２６条　保護管理者等は、個人データ等を取り扱う基幹的なサーバ等の機器を設置する場所（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役職員等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を講ずるものとする。

２　保護管理者等は、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及び所在表示の制限等の措置を講ずるものとする。

３　保護管理者等は、情報システム室等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定めの整備及び定期又は随時にその見直しを実施し、読取防止等の措置を講ずるものとする。

（情報システム室等の管理）

第２７条　保護管理者等は、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、監視設備の設置等の措置を講ずるものとする。

２　保護管理者等は、災害等に備え、情報システム室等に、耐震、防火、防煙及び防水等の必要な措置を講ずるとともに、情報システム室等の予備電源の確保、配線の損傷防止等の措置を講ずるものとする。

３　保護管理者等は、個人データ等を記録する媒体を保管するための場所を設けている場合において、必要があると認めるときは、前条及び前２項に準じた措置を講ずるものとする。

（その他）

第２８条　この細則に定めるもののほか、この細則の実施に関し必要な事項は、別に定める。

附　則

この細則は、平成17年４月１日から施行する。

附　則（平成27年細則第15号（平成27年３月25日））

この細則は、平成27年４月１日から施行する。

附　則（平成27年細則第18号（平成27年12月16日））

この細則は、平成27年12月16日から施行する。

附　則（平成29年細則第９号（平成29年５月29日））

この細則は、平成29年５月30日から施行する。

附　則（平成31年細則第４号（平成31年２月13日））

この細則は、平成31年２月13日から施行する。

附　則（令和６年細則第１号（令和６年１月23日））

この細則は、令和６年１月23日から施行する。