

○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 平成27年3月25日細則第15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23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、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者をその利用目的を達成するために必要最小限の役員又は職員若しくは本法人から委託された個人情報の取扱い業務に従事する者(以下「職員等」という。)に限るものとする。

2 アクセス権限を有しない職員等は、保有個人情報にアクセスしてはならない。

3 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ない。

(複製等の制限)

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

(1) 保有個人情報の複製

(2) 保有個人情報の送信

(3) 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出し

(4) 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5条 職員等は、保有個人情報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 職員等は、保護管理者等の指示に従い、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。

(廃棄等)

第7条 職員等は、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には、保護管理者等の指示に従い、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、当該情報の消去又は当該媒体の廃棄を行うものとする。

(取扱状況の記録)

第8条 保護管理者等は、保有個人情報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。

(アクセス制御)

第9条 保護管理者等は、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16条を除き同じ。）の秘匿性等その内容に応じて、アクセスに係る認証機能（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をいう。以下同じ。）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。

(アクセス記録の取得等)

第10条 保護管理者等は、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の記録（以下「アクセス記録」という。）を取得し、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11条 保護管理者等は、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不適切なアクセスの監視のため、一定数以上の保有個人情報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、当該機能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12条 保護管理者等は、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13条 保護管理者等は、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14条 保護管理者等は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、不正プログラムの感染防止等に必要な措置を講ずるものとする。

(暗号化)

第15条 保護管理者等は、保有個人情報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ものとする。

(入力情報の照合等)

第16条 職員等は、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17条 保護管理者等は、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18条 保護管理者等は、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。

(端末の限定)

第19条 保護管理者等は、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に必要な措置を講ずるものとする。

(パスワード等の取扱い)

第20条 保護管理者等は、端末の使用に係る認証機能を設定するとともに、必要があると認めるときは、パスワード等の取扱いに関する定めを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。

(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 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서는ならない。

(第三者の閲覧防止)

第22条 職員等は、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の必要な措置を講ずるものとする。

(記録機能を有する機器・媒体の接続制限)

第23条 保護管理者等は、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、滅失又は毀損の防止のため、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。

(情報システム室等の入退管理)

第24条 保護管理者等は、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、パスワード等の取扱いに関する定めを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25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、保有個人情報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26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。