

国立大学法人東京農工大学保有個人情報管理細則の一部改正

現行	改正	改正理由
<p>国立大学法人東京農工大学保有個人情報管理細則</p> <p>目次</p> <p>第1章 総則(第1条・第2条)</p> <p>第2章 管理体制(第3条―第6条の2)</p> <p>第3章 教育研修(第7条)</p> <p>第4章 職員等の責務(第8条)</p> <p>第5章 <u>保有個人情報</u>の取扱い(第9条―第14条の6)</p> <p>第6章 情報システムにおける安全の確保等(第15条―第25条)</p> <p>第7章 情報システム室等の安全管理(第26条・第27条)</p> <p>第8章 <u>保有個人情報</u>の提供及び業務の委託等(第28条・第29条)</p> <p>第9章 安全確保上の問題への対応(第30条・第31条)</p> <p>第10章 監査及び点検の実施(第32条―第34条)</p> <p>第11章 行政機関との連携(第34条の2)</p> <p>第12章 雑則(第35条)</p> <p>附則</p> <p>本則</p> <p>第2章 管理体制 (総括保護管理者)</p> <p>第3条 本学に、<u>保有個人情報</u>総括保護管理者(以下「総括保護</p>	<p>国立大学法人東京農工大学保有個人情報<u>等</u>管理細則</p> <p>目次</p> <p>第1章 総則(第1条・第2条)</p> <p>第2章 管理体制(第3条―第6条の2)</p> <p>第3章 教育研修(第7条)</p> <p>第4章 職員等の責務(第8条)</p> <p>第5章 <u>保有個人情報等</u>の取扱い(第9条―第14条の6)</p> <p>第6章 情報システムにおける安全の確保等(第15条―第25条)</p> <p>第7章 情報システム室等の安全管理(第26条・第27条)</p> <p>第8章 <u>保有個人情報等</u>の提供及び業務の委託等(第28条・第29条)</p> <p>第9章 安全確保上の問題への対応(第30条・第31条)</p> <p>第10章 監査及び点検の実施(第32条―第34条)</p> <p>第11章 行政機関との連携(第34条の2)</p> <p>第12章 雑則(第35条)</p> <p>附則</p> <p>本則</p> <p>第2章 管理体制 (総括保護管理者)</p> <p>第3条 本学に、<u>保有個人情報等</u>総括保護管理者(以下「総括保</p>	

<p>管理者」という。)を1人置き、理事(広報・国際担当)をもって充てる。</p> <p>2 総括保護管理者は、本学における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。</p> <p>(保護管理者)</p> <p>第4条 本学に<u>保有個人情報</u>保護管理者(以下「保護管理者」という。)を置き、国立大学法人東京農工大学事務組織規程第3条から第9条までに規定する課及び室の長並びに同規程第15条に規定する課長をもって充てる。</p> <p>2 保護管理者は、所掌する業務の範囲における<u>保有個人情報</u>の適切な管理を確保する任に当たる。<u>保有個人情報</u>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。</p> <p>(保護担当者)</p> <p>第5条 前条に規定する保護管理者を補佐するため、<u>保有個人情報</u>保護担当者(以下「保護担当者」という。)を置く。</p> <p>2 (略)</p> <p>3 保護担当者は、保護管理者を補佐し、<u>保有個人情報</u>の管理に関する事務を担当する。</p> <p>(監査責任者)</p> <p>第6条 本学に、<u>保有個人情報</u>監査責任者(以下「監査責任者」という。)1人を置き、本学の監事をもって充てる。</p> <p>2 監査責任者は、本学の<u>保有個人情報</u>の管理状況について監査する。</p> <p>第3章 教育研修</p>	<p>護管理者」という。)を1人置き、理事(広報・国際担当)をもって充てる。</p> <p>2 総括保護管理者は、本学における保有個人情報 <u>及び独立行政法人等非識別加工情報</u>(以下「保有個人情報等」という。)の管理に関する事務を総括する任に当たる。</p> <p>(保護管理者)</p> <p>第4条 本学に<u>保有個人情報等</u>保護管理者(以下「保護管理者」という。)を置き、国立大学法人東京農工大学事務組織規程第3条から第9条までに規定する課及び室の長並びに同規程第15条に規定する課長をもって充てる。</p> <p>2 保護管理者は、所掌する業務の範囲における<u>保有個人情報等</u>の適切な管理を確保する任に当たる。<u>保有個人情報等</u>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。</p> <p>(保護担当者)</p> <p>第5条 前条に規定する保護管理者を補佐するため、<u>保有個人情報等</u>保護担当者(以下「保護担当者」という。)を置く。</p> <p>2 (略)</p> <p>3 保護担当者は、保護管理者を補佐し、<u>保有個人情報等</u>の管理に関する事務を担当する。</p> <p>(監査責任者)</p> <p>第6条 本学に、<u>保有個人情報等</u>監査責任者(以下「監査責任者」という。)1人を置き、本学の監事をもって充てる。</p> <p>2 監査責任者は、本学の<u>保有個人情報等</u>の管理状況について監査する。</p> <p>第3章 教育研修</p>	
--	---	--

<p>(教育研修)</p> <p>第7条 総括保護管理者は、<u>保有個人情報</u>の取扱いに従事する役員及び職員(派遣労働者を含む。以下同じ。)(以下「職員等」という。)に対し、<u>保有個人情報</u>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行う。</p> <p>2 総括保護管理者は、<u>保有個人情報</u>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、<u>保有個人情報</u>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。</p> <p>3 総括保護管理者は、保護管理者及び保護担当者に対し、<u>保有個人情報</u>の適切な管理のための教育研修を実施する。</p> <p>4 保護管理者は、所掌する業務を行う職員に対し、<u>保有個人情報</u>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の必要な措置を講ずる。</p> <p>第4章 職員等の責務</p> <p>(職員等の責務)</p> <p>第8条 職員等は、法及び番号法の趣旨に則り、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、<u>保有個人情報</u>を取り扱わなければならない。</p> <p>第5章 <u>保有個人情報</u>の取扱い</p> <p>(アクセス制限)</p> <p>第9条 保護管理者は、<u>保有個人情報</u>の秘匿性等その内容に応じて、当該 <u>保有個人情報</u>にアクセスする権限を有する職員等とその権限の内容を、当該職員等が業務を行う上で必要最小限の範</p>	<p>(教育研修)</p> <p>第7条 総括保護管理者は、<u>保有個人情報等</u>の取扱いに従事する役員及び職員(派遣労働者を含む。以下同じ。)(以下「職員等」という。)に対し、<u>保有個人情報等</u>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行う。</p> <p>2 総括保護管理者は、<u>保有個人情報等</u>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、<u>保有個人情報等</u>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。</p> <p>3 総括保護管理者は、保護管理者及び保護担当者に対し、<u>保有個人情報等</u>の適切な管理のための教育研修を実施する。</p> <p>4 保護管理者は、所掌する業務を行う職員に対し、<u>保有個人情報等</u>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の必要な措置を講ずる。</p> <p>第4章 職員等の責務</p> <p>(職員等の責務)</p> <p>第8条 職員等は、法及び番号法の趣旨に則り、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、<u>保有個人情報等</u>を取り扱わなければならない。</p> <p>第5章 <u>保有個人情報等</u>の取扱い</p> <p>(アクセス制限)</p> <p>第9条 保護管理者は、<u>保有個人情報等</u>の秘匿性等その内容に応じて、当該 <u>保有個人情報等</u>にアクセスする権限を有する職員等とその権限の内容を、当該職員等が業務を行う上で必要最小限</p>	
--	--	--

<p>囲に限る。</p> <p>2 アクセス権限を有しない職員等は、<u>保有個人情報</u>にアクセスしてはならない。</p> <p>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 <u>保有個人情報</u> にアクセスしてはならない。</p> <p>(複製等の制限)</p> <p>第10条 職員等が業務上の目的で <u>保有個人情報</u> を取り扱う場合であっても、保護管理者は、次の各号に掲げる行為については、当該 <u>保有個人情報</u> 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、職員等は、保護管理者の指示に従い行う。</p> <p>(1) <u>保有個人情報</u> の複製</p> <p>(2) <u>保有個人情報</u> の送信</p> <p>(3) <u>保有個人情報</u> が記録されている媒体の外部への送付又は持出し</p> <p>(4) その他 <u>保有個人情報</u> の適切な管理に支障を及ぼすおそれのある行為</p> <p>(誤りの訂正等)</p> <p>第11条 職員等は、<u>保有個人情報</u> 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。</p> <p>(媒体の管理等)</p> <p>第12条 職員等は、保護管理者の指示に従い、<u>保有個人情報</u> 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。</p> <p>(廃棄等)</p>	<p>の範囲に限る。</p> <p>2 アクセス権限を有しない職員等は、<u>保有個人情報等</u> にアクセスしてはならない。</p> <p>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 <u>保有個人情報等</u> にアクセスしてはならない。</p> <p>(複製等の制限)</p> <p>第10条 職員等が業務上の目的で <u>保有個人情報等</u> を取り扱う場合であっても、保護管理者は、次の各号に掲げる行為については、当該 <u>保有個人情報等</u> 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、職員等は、保護管理者の指示に従い行う。</p> <p>(1) <u>保有個人情報等</u> の複製</p> <p>(2) <u>保有個人情報等</u> の送信</p> <p>(3) <u>保有個人情報等</u> が記録されている媒体の外部への送付又は持出し</p> <p>(4) その他 <u>保有個人情報等</u> の適切な管理に支障を及ぼすおそれのある行為</p> <p>(誤りの訂正等)</p> <p>第11条 職員等は、<u>保有個人情報等</u> 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。</p> <p>(媒体の管理等)</p> <p>第12条 職員等は、保護管理者の指示に従い、<u>保有個人情報等</u> 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。</p> <p>(廃棄等)</p>	
---	--	--

<p>第13条 職員等は、<u>保有個人情報</u>又は<u>保有個人情報</u>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<u>保有個人情報</u>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。</p> <p>(<u>保有個人情報</u>の取扱状況の記録)</p> <p>第14条 保護管理者は、<u>保有個人情報</u>の秘匿性等その内容に応じて、台帳等を整備して、当該<u>保有個人情報</u>の利用及び保管等の取扱いの状況について記録する。</p> <p>2 (略)</p> <p>第6章 情報システムにおける安全の確保等</p> <p>(アクセス制御)</p> <p>第15条 保護管理者は、<u>保有個人情報</u>(情報システムで取り扱うものに限る。以下本章(第20条を除く。)において同じ。)の秘匿性等その内容に応じて、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。</p> <p>2 (略)</p> <p>(アクセス記録)</p> <p>第16条 保護管理者は、<u>保有個人情報</u>の秘匿性等その内容に応じて、当該<u>保有個人情報</u>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。</p> <p>2・3 (略)</p>	<p>第13条 職員等は、<u>保有個人情報等</u>又は<u>保有個人情報等</u>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<u>保有個人情報等</u>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。</p> <p>(<u>保有個人情報等</u>の取扱状況の記録)</p> <p>第14条 保護管理者は、<u>保有個人情報等</u>の秘匿性等その内容に応じて、台帳等を整備して、当該<u>保有個人情報等</u>の利用及び保管等の取扱いの状況について記録する。</p> <p>2 (略)</p> <p>第6章 情報システムにおける安全の確保等</p> <p>(アクセス制御)</p> <p>第15条 保護管理者は、<u>保有個人情報等</u>(情報システムで取り扱うものに限る。以下本章(第20条を除く。)において同じ。)の秘匿性等その内容に応じて、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。</p> <p>2 (略)</p> <p>(アクセス記録)</p> <p>第16条 保護管理者は、<u>保有個人情報等</u>の秘匿性等その内容に応じて、当該<u>保有個人情報等</u>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。</p> <p>2・3 (略)</p>	
--	---	--

<p>(アクセス状況の監視)</p> <p>第 16 条の 2 保護管理者は、<u>保有個人情報</u>の秘匿性等その内容及びその量に応じて、当該 <u>保有個人情報</u> への不適切なアクセスの監視のため、<u>保有個人情報</u> 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。</p> <p>(管理者権限の設定)</p> <p>第 16 条の 3 保護管理者は、<u>保有個人情報</u>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。</p> <p>(外部からの不正アクセスの防止)</p> <p>第 17 条 保護管理者は、<u>保有個人情報</u>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。</p> <p>(不正プログラムによる漏えい等の防止)</p> <p>第 18 条 保護管理者は、不正プログラムによる <u>保有個人情報</u>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。</p> <p>(情報システムにおける <u>保有個人情報</u> の処理)</p> <p>第 18 条の 2 職員等は、<u>保有個人情報</u>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 <u>保有個人情報</u>の秘匿性等その内容に応</p>	<p>(アクセス状況の監視)</p> <p>第 16 条の 2 保護管理者は、<u>保有個人情報等</u>の秘匿性等その内容及びその量に応じて、当該 <u>保有個人情報等</u> への不適切なアクセスの監視のため、<u>保有個人情報等</u> 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。</p> <p>(管理者権限の設定)</p> <p>第 16 条の 3 保護管理者は、<u>保有個人情報等</u>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。</p> <p>(外部からの不正アクセスの防止)</p> <p>第 17 条 保護管理者は、<u>保有個人情報等</u>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。</p> <p>(不正プログラムによる漏えい等の防止)</p> <p>第 18 条 保護管理者は、不正プログラムによる <u>保有個人情報等</u>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。</p> <p>(情報システムにおける <u>保有個人情報等</u> の処理)</p> <p>第 18 条の 2 職員等は、<u>保有個人情報等</u>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 <u>保有個人情報等</u>の秘匿性等その内容に</p>	
--	--	--

<p>じて、随時、消去等の実施状況を重点的に確認する。</p> <p>(暗号化)</p> <p>第 19 条 保護管理者は、<u>保有個人情報</u>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。</p> <p>2 職員等は、前項に基づき、その処理する <u>保有個人情報</u>について、当該 <u>保有個人情報</u>の秘匿性等その内容に応じて、適切に暗号化を行う。</p> <p>(記録機能を有する機器・媒体の接続制限)</p> <p>第 19 条の 2 保護管理者は、<u>保有個人情報</u>の秘匿性等その内容に応じて、当該 <u>保有個人情報</u>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。</p> <p>(入力情報の照合等)</p> <p>第 20 条 職員等は、情報システムで取り扱う <u>保有個人情報</u>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 <u>保有個人情報</u>の内容の確認、既存の <u>保有個人情報</u>との照合等を行う。</p> <p>(バックアップ)</p> <p>第 21 条 保護管理者は、<u>保有個人情報</u>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。</p> <p>(情報システム設計書等の管理)</p> <p>第 22 条 保護管理者は、<u>保有個人情報</u>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。</p>	<p>に応じて、随時、消去等の実施状況を重点的に確認する。</p> <p>(暗号化)</p> <p>第 19 条 保護管理者は、<u>保有個人情報等</u>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。</p> <p>2 職員等は、前項に基づき、その処理する <u>保有個人情報等</u>について、当該 <u>保有個人情報等</u>の秘匿性等その内容に応じて、適切に暗号化を行う。</p> <p>(記録機能を有する機器・媒体の接続制限)</p> <p>第 19 条の 2 保護管理者は、<u>保有個人情報等</u>の秘匿性等その内容に応じて、当該 <u>保有個人情報等</u>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。</p> <p>(入力情報の照合等)</p> <p>第 20 条 職員等は、情報システムで取り扱う <u>保有個人情報等</u>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 <u>保有個人情報等</u>の内容の確認、既存の <u>保有個人情報等</u>との照合等を行う。</p> <p>(バックアップ)</p> <p>第 21 条 保護管理者は、<u>保有個人情報等</u>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。</p> <p>(情報システム設計書等の管理)</p> <p>第 22 条 保護管理者は、<u>保有個人情報等</u>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。</p>	
--	--	--

<p>(端末の限定)</p> <p>第23条 保護管理者は、<u>保有個人情報</u>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。</p> <p>(第三者の閲覧防止)</p> <p>第25条 職員等は、端末の使用に当たっては、<u>保有個人情報</u>が第三者に閲覧されないことがないように、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。</p> <p>第7章 情報システム室等の安全管理</p> <p>(入退管理)</p> <p>第26条 保護管理者は、<u>保有個人情報</u>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。また、<u>保有個人情報</u>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、必要があると認めるときは、前項と同様の措置を講ずる。</p> <p>2・3 (略)</p> <p>第8章 <u>保有個人情報</u>の提供及び業務の委託等</p> <p>(<u>保有個人情報</u>の提供)</p> <p>第28条 保護管理者は、法第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に <u>保有個人情報</u>を提供する場合には、原則として、提供先における利用目的、</p>	<p>(端末の限定)</p> <p>第23条 保護管理者は、<u>保有個人情報等</u>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。</p> <p>(第三者の閲覧防止)</p> <p>第25条 職員等は、端末の使用に当たっては、<u>保有個人情報等</u>が第三者に閲覧されないことがないように、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。</p> <p>第7章 情報システム室等の安全管理</p> <p>(入退管理)</p> <p>第26条 保護管理者は、<u>保有個人情報等</u>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。また、<u>保有個人情報等</u>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、必要があると認めるときは、前項と同様の措置を講ずる。</p> <p>2・3 (略)</p> <p>第8章 <u>保有個人情報等</u>の提供及び業務の委託等</p> <p>(<u>保有個人情報等</u>の提供)</p> <p>第28条 保護管理者は、法第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に <u>保有個人情報等</u>を提供する場合には、原則として、提供先における利用目</p>	
--	---	--



<p>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書面を取り交わす。</p> <p>2 保護管理者は、法第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に<u>保有個人情報</u>を提供する場合には、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。</p> <p>3 保護管理者は、法第9条第2項第3号の規定に基づき行政機関又は独立行政法人等に<u>保有個人情報</u>を提供する場合において、必要があると認めるときは、前2項に規定する措置を講ずる。</p> <p>4 (略)</p> <p>(業務の委託等)</p> <p>第29条 <u>保有個人情報</u>の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないように、必要な措置を講ずる。また、契約書に、次の各号に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。</p> <p>(1)～(6) (略)</p> <p>2 (略)</p> <p>3 <u>保有個人情報</u>の取扱いに係る業務を外部に委託する場合には、委託する<u>保有個人情報</u>の秘匿性等その内容に応じて、委託先における個人情報の管理の状況について、年1回以上の定期</p>	<p>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書面を取り交わす。</p> <p>2 保護管理者は、法第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に<u>保有個人情報等</u>を提供する場合には、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。</p> <p>3 保護管理者は、法第9条第2項第3号の規定に基づき行政機関又は独立行政法人等に<u>保有個人情報等</u>を提供する場合において、必要があると認めるときは、前2項に規定する措置を講ずる。</p> <p>4 (略)</p> <p>(業務の委託等)</p> <p>第29条 <u>保有個人情報等</u>の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないように、必要な措置を講ずる。また、契約書に、次の各号に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。</p> <p>(1)～(6) (略)</p> <p>2 (略)</p> <p>3 <u>保有個人情報等</u>の取扱いに係る業務を外部に委託する場合には、委託する<u>保有個人情報等</u>の秘匿性等その内容に応じて、委託先における個人情報の管理の状況について、年1回以上の定</p>	
--	--	--

<p>的検査等により確認する。</p> <p>4 (略)</p> <p>5 委託先において、<u>保有個人情報</u>の取扱いに係る業務が再委託される場合には、委託先に第1項の措置を講じさせるとともに、再委託される業務に係る <u>保有個人情報</u>の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項の措置を実施する。<u>保有個人情報</u>の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。</p> <p>6 (略)</p> <p>7 <u>保有個人情報</u>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には、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。</p> <p style="text-align: center;">第9章 安全確保上の問題への対応 (事案の報告及び再発防止措置)</p> <p>第30条 <u>保有個人情報</u>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本細則その他法令等に違反している事実又は兆候を把握した場合等、安全確保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等は、直ちに当該 <u>保有個人情報</u>を管理する保護管理者に報告する。</p> <p>2～7 (略)</p> <p>(公表等)</p> <p>第31条 学長は、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 <u>保有個人情報</u>の本人への対応等の措置を講ずる。</p> <p>2 (略)</p>	<p>期的検査等により確認する。</p> <p>4 (略)</p> <p>5 委託先において、<u>保有個人情報等</u>の取扱いに係る業務が再委託される場合には、委託先に第1項の措置を講じさせるとともに、再委託される業務に係る <u>保有個人情報等</u>の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項の措置を実施する。<u>保有個人情報等</u>の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。</p> <p>6 (略)</p> <p>7 <u>保有個人情報等</u>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には、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。</p> <p style="text-align: center;">第9章 安全確保上の問題への対応 (事案の報告及び再発防止措置)</p> <p>第30条 <u>保有個人情報等</u>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本細則その他法令等に違反している事実又は兆候を把握した場合等、安全確保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等は、直ちに当該 <u>保有個人情報等</u>を管理する保護管理者に報告する。</p> <p>2～7 (略)</p> <p>(公表等)</p> <p>第31条 学長は、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 <u>保有個人情報等</u>の本人への対応等の措置を講ずる。</p> <p>2 (略)</p>	
---	---	--

<p>第10章 監査及び点検の実施</p> <p>(監査)</p> <p>第32条 監査責任者は、<u>保有個人情報</u>の適切な管理を検証するため、第2章から第9章までに規定する措置の状況を含む本学における<u>保有個人情報</u>の管理の状況について、定期的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。</p> <p>(点検)</p> <p>第33条 保護管理者は、所掌する業務の範囲における<u>保有個人情報</u>の記録媒体、処理経路、保管方法等について、定期的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。</p> <p>(評価及び見直し)</p> <p>第34条 総括保護管理者及び保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から<u>保有個人情報</u>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。</p> <p>2 (略)</p>	<p>第10章 監査及び点検の実施</p> <p>(監査)</p> <p>第32条 監査責任者は、<u>保有個人情報等</u>の適切な管理を検証するため、第2章から第9章までに規定する措置の状況を含む本学における<u>保有個人情報等</u>の管理の状況について、定期的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。</p> <p>(点検)</p> <p>第33条 保護管理者は、所掌する業務の範囲における<u>保有個人情報等</u>の記録媒体、処理経路、保管方法等について、定期的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。</p> <p>(評価及び見直し)</p> <p>第34条 総括保護管理者及び保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から<u>保有個人情報等</u>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。</p> <p>2 (略)</p>	
---	---	--

附 則(平成29年5月30日細則第8号)  
この細則は、平成29年5月30日から施行する。