

# 公立大学法人横浜市立大学産学官連携に係る秘密情報管理実施細則

制 定 令和 6 年 4 月 1 日

## (目的)

第1条 この細則は、公立大学法人横浜市立大学産学官連携に係る秘密情報管理実施基準（以下「実施基準」という。）第11条に基づき、秘密情報を適正に取扱うための措置について定めることを目的とする。

## (定義)

第2条 本細則における用語の意義は、実施基準第2条に定めるところによる。

## (対象)

第3条 実施基準第3条の秘密情報は、次の範囲とする。

- (1) 公立大学法人横浜市立大学（以下、「本学」という。）独自の秘密情報のうち、非公開で外部に漏らしてはいけない情報
- (2) 産学官連携に伴い、本学が秘密保持義務を負うことを前提に、企業等から提供された秘密情報
- (3) 産学官連携による成果に含まれ、企業等または本学が指定もしくは双方にて指定し、双方が同意する秘密情報

## (秘密情報の形態)

第4条 実施基準第4条の形態は次の範囲とする。

研究データに記載された秘密情報は、「横浜市立大学 研究データ管理・公開ポリシーの解説」の研究データの定義に記載の通り、例えば研究に関する知見が記載された資料、実験データ、実験ノート、公表前原稿、発明届出書、特許出願書類、研究計画書、研究報告書、契約書、会議議事録、研究成果が記載された資料などである。

研究過程で得られる情報は、ネガティブインフォメーションを含む。

## (情報の取扱い)

第5条 教職員等は別表第1に従い、秘密情報を取扱うものとする。

## (総括責任者の責務)

第6条 総括責任者は、本秘密情報の管理を統括する。

- 2 総括責任者は、管理責任者に秘密情報管理に関する事項に関して指示及び指導を行う。

## (管理責任者の責務)

第7条 管理責任者は、統括責任者の指示に従い、教室等における秘密情報を適切に管理しなければならない。

- 2 管理責任者は、対象となる情報の内容を確認し、秘密情報を特定する。
- 3 管理責任者は、内容に応じて情報の格付けを決定した上でアクセス権者を指定し、別表1に基づき、漏えい対策を講じるものとする。
- 4 管理責任者は、アクセス権者に対し漏えい対策を周知し、特に学生等が秘密情報を取扱う際には、学生等に事前に適切な指導をしなければならない。
- 5 管理責任者は、学生等に厳密情報へのアクセスを認める場合、当該学生等に対し

て誓約書に署名させ、総括責任者に提出しなければならない。

- 6 管理責任者は、学生等に企業との共同研究又は受託研究に参画することを決めた場合、事前に参画することの利益及び不利益について十分な説明を行った上で、当該学生等の参画への自発的な意思を確認しなければならない。また、参画の意思のある学生等に対して誓約書に署名させ、総括責任者に提出しなければならない。
- 7 管理責任者は、卒業、退学、除籍等により学生としての身分を失う学生等に対して、実際の運用等及び共同研究又は受託研究に従事した際に負っている秘密保持義務の内容、期間等を確認させなければならない。
- 8 管理責任者は、研究管理体制の構築をしなければならない。

(事故対応)

第8条 教職員等は、実施基準第9条に従って、適切に対処する。

(研究支援業務に従事する教職員等の責務)

第9条 研究支援業務に従事する教職員等は、業務担当部署外へ秘密情報を持ち出す、配布する際は、管理責任者の許可を得るものとする。

(誓約書の提出)

第10条 教職員等は、次の各号に掲げる事項を含む誓約書を、所定の方法により総括責任者に対して提出する。

- (1) 秘密情報管理に係る規定を遵守すること。
- (2) 秘密情報を漏えいしないこと。
- (3) 学生等に企業との共同研究又は受託研究に参画することを決めた場合、事前に参画することの利益及び不利益について十分な説明を行うこと。

#### 附 則

この細則は、令和6年4月1日から施行する。

別表第1（第5条関連）

区分	極秘	厳秘	秘
基準	漏えいすることにより、企業等及び／または本学の事業に極めて深刻な影響若しくは不利益を受けるものであって、総括責任者が指定する者以外に漏らしてはいけない情報	知的財産に関する研究情報(将来技術移転やライセンスが可能になるものも含む)や顧客情報、企業から慎重な秘密管理を要請される情報など、漏えいすることにより、企業等及び／または本学の競争力が低下するおそれがあるものであって、管理責任者が指定する者以外に漏らしてはいけない情報	極秘、厳秘に該当しない秘密情報であって、管理責任者が指定する者以外に漏らしてはいけない情報
表示	秘密記録媒体に、明確に認識できるように「極秘」または「Top Secret」、および「持出厳禁」と表示する。	秘密記録媒体に、明確に認識できるよう「厳秘」または「Strict Secret」と表示する。	秘密記録媒体に、明確に認識できるよう「秘」または「Confidential」と表示する。
閲覧	・総括責任者が指定するアクセス権者のみ可 ・秘密電子化情報は指定の専用機器からのみ可 ・閲覧時は、閲覧者名、日時等を記録する。	・管理責任者が指定するアクセス権者のみ可 ※厳秘情報にアクセスする学生については、誓約書を提出した学生に限る。 ・秘密電子化情報には、ログインパスワード等が設定されている情報機器からのみアクセスするようする。 ・アクセス権者以外に読み取られないよう、閲覧場所や情報機器画面には保護フィルムを貼付するなどして、注意する。	
保管	・秘密電子化情報は非ネットワーク接続の専用機器に保管する。 ・秘密記録媒体は、施錠された保管庫（キャビネット、引き出し等）に保管する。	・原則、学生は保管不可。やむを得ない場合は管理責任者の許可を得るものとする。 ・他の情報と分離して保管する。 ・秘密電子化情報はログインパスワードが設定されている情報機器に保管し、ファイルにパスワードを設定または暗号化する。 ・秘密記録媒体、秘密成果有体物は施錠された保管庫（キャビネット、引き出し等）に保管する。鍵は管理責任者が管理する。 ・秘密記録媒体を保管している部屋に、外部者が入室する際は極力外部者のみにさせない。	・他の情報と分離して保管する。 ・秘密電子化情報はログインパスワードが設定されている情報機器に保管する。 ・秘密記録媒体、秘密成果有体物は施錠された保管庫（キャビネット、引き出し等）に保管する。鍵は管理責任者が管理する。 ・秘密記録媒体を保管している部屋に、外部者が入室する際は極力外部者のみにさせない。
配布	不可	・業務上やむを得ない場合を除いて、配付不可 ・やむを得ない場合に限り、管理責任者または管理責任者の許可を得たアクセス権者のみ行うことができる。 ・原則、秘密電子化情報はクラウドや大容量ファイル転送サービスなどオンラインストレージを使用し、さらにパスワードを設定する。その際、原則ダウンロードは不可とし、やむを得ず認める場合はダウンロード期間、回数を最小限とする。 ・秘密記録媒体を会議等で資料として配付する場合は、終了後回収する。	・管理責任者または管理責任者の許可を得たアクセス権者のみ配布を行うことができる。 ・秘密電子化情報はメール送信する場合には、暗号化、パスワード設定等を行い、適切な漏えい対策を講じる。 ・秘密記録媒体を会議等で資料として配付する場合は、終了後回収する。
複製	不可	・業務上やむを得ない場合を除いて、複製及び撮影不可 ・やむを得ない場合に限り、管理責任者または管理責任者の許可を得たアクセス権者のみ行うことができる。 ・印刷する場合は、原則としてアクセス権者が占有する個室等に設置されたプリンタで行う。それ以外の場所に設置されたプリンタで印刷する場合には、印刷中からプリンタの前に待機し、完了後直ちに回収する。	・管理責任者または管理責任者の許可を得たアクセス権者のみ複製及び撮影を行うことができる。 ・印刷する場合は、原則としてアクセス権者が占有する個室等に設置されたプリンタで行う。それ以外の場所に設置されたプリンタで印刷する場合には、印刷中からプリンタの前に待機し、完了後直ちに回収する。
持ち出し	不可	・業務上やむを得ない場合を除いて、持ち出し不可 ・やむを得ない場合に限り、管理責任者または管理責任者の許可を得たアクセス権者のみ行うことができる。 ・原則、学生は持ち出し不可。やむを得えない場合は、管理責任者または管理責任者の許可を得たアクセス権者のみ行うことができる。 ・持ち出す場合は持ち出した者自らが携行し、紛失しないよう適切な措置を講じる。 ・秘密記録媒体を送付する際には密封の上親展でおくる。	・管理責任者または管理責任者の許可を得たアクセス権者のみ持ち出しを行うことができる。 ・持ち出す場合は持ち出した者自らが携行し、紛失しないよう適切な措置を講じる。 ・秘密記録媒体を送付する際には密封の上親展でおくる
廃棄	・廃棄、消去及び返却に当たっては、総括責任者の許可を得なければならない。 ・廃棄、消去にあたっては、総括責任者の責任の下で、裁断、焼却、溶解等で復元不可能な形にして行わなければならぬ。 ・秘密電子化情報をフォルダ等から消去する際は、第三者が残留情報を読みとることができないように情報を消去しなければならない。 ・秘密記録媒体のうち、電子記録媒体は大学によって指定された場所に持ち込み、破壊するなどして処分する。	・廃棄、消去及び返却に当たっては、管理責任者の許可を得なければならない。 ・廃棄、消去にあたっては、管理責任者の責任の下で、裁断、焼却、溶解等で復元不可能な形にして行わなければならぬ。 ・秘密電子化情報をフォルダ等から消去する際は、第三者が残留情報を読みとることができないように情報を消去しなければならない。 ・秘密記録媒体のうち、電子記録媒体は大学によって指定された場所に持ち込み、破壊するなどして処分する。	・廃棄、消去に当たっては、管理責任者の責任の下で、裁断、焼却、溶解等で復元不可能な形にして行わなければならぬ。 ・秘密電子化情報をフォルダ等から消去する際は、第三者が残留情報を読みとることができないように情報を消去しなければならない。 ・秘密記録媒体のうち、電子記録媒体は大学によって指定された場所に持ち込み、破壊するなどして処分する。

## 別表第2（第8条関連）

情報漏えい事故発生直後の対応は以下の通りとする。

1. 管理責任者は、速やかに研究・产学連携推進課課長に連絡する
2. 研究・产学連携推進課長は、コンプライアンス推進を所管する課の長に報告する。  
(第一報)  
「公立大学法人横浜市立大学における事務処理ミス等及び事件・事故に係る報告及び公表基準」第3条に基づき、同基準別記の様式を用いる。
3. 研究・产学連携推進課長は、事故対応が完了した時点で、最終報としてコンプライアンス推進を所管する課の長に報告する。(最終報告)