

## 学校法人沖縄科学技術大学院大学学園 個人情報保護規則

理事長・学長決定

2024年4月1日

### (目的)

第1条 本規則は個人情報の保護に関する法律(平成15年法律第57号。以下「法」という。)及び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「番号法」という。)に基づき、学校法人沖縄科学技術大学院大学学園(以下「学園」という。)における個人情報の保護について基本的事項を定めることにより、学園の事務及び事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

### (基本方針)

第2条 学園は、学園の有する全ての個人情報個人が個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに鑑み、それらを適正に取扱わなければならない。

2 学園の役職員(派遣職員を含む。以下同じ。)、学生及び訪問者(以下「役職員等」という。)は、個人情報保護の重要性を認識し、本規則にしたがって適切に対応しなければならない。

### (定義)

第3条 本規則における用語の定義は法第2条、第16条、第60条及び番号法第2条の定めるところによる。

### (理事長)

第4条 理事長は、学園における法人の長として、法の規定に従い、学園における個人情報等の管理に係る事項について最終決定を行い、内閣総理大臣及びその他関係大臣または国の個人情報保護委員会その他の政府機関等への申請及び報告等を行うものとする。

### (個人情報統括保護管理者)

第5条 学園に、個人情報統括保護管理者(以下「統括管理者」という。)を置き、事務局長をもって充てるものとする。

2 統括管理者は、理事長の命を受け、学園における個人情報、仮名加工情報、匿名加工情報、個人関連情報その他法により定義され、同法の対象となる情報及び番号法により定義され、同法の対象となる情報(以下、「個人情報等」という。)の管理に関する事務を統括するものとする。

3 統括管理者は、本規則の維持管理及びその施行のため必要となる規程等を策定す

るものとする。

- 4 統括管理者は、本規則の施行と個人情報保護に関する重要事項を決定する上で必要となる学園内の円滑なコミュニケーションの推進及び調整を実施するものとする。

#### (個人情報保護責任者)

- 第6条 各ディビジョン等の部門に、個人情報保護責任者（以下「責任者」という。）を置き、当該ディビジョン等の部門の長をもって充てるものとする。
- 2 責任者は、責任者が所管する各部門内における個人情報保護に関する必要なガイダンスの提供及び必要な監督を実施するものとする。
  - 3 責任者は、通常、PRP第17章で規定される情報資産管理責任者と同一の者が行うものとする。

#### (個人情報保護管理者)

- 第7条 各セクション等の部署に、個人情報保護管理者（以下「管理者」という。）を置き、当該セクション等の部署の長をもって充てるものとする。
- 2 管理者は、当該セクション等の部署における個人情報等の管理に関する事務を統括し、各部署における個人情報等の適切な管理を確保する任に当たるものとする。
  - 3 管理者は、次条第1項により、各部署内において個人情報等の事務を行う担当者を指名したときは、責任者にその旨を報告するとともに、指名した者について統括管理者に届出を行うものとする。

#### (個人情報保護担当者)

- 第8条 各セクション等の部署に、個人情報保護担当者（以下「担当者」という。）1名を置き、法人文書管理規則に定める文書管理担当者の中から当該セクション等の部署の管理者により指名するものとする。
- 2 担当者は、管理者を補佐し、各セクション等の部署における個人情報等の管理に関する事務を担当するものとする。

#### (最高情報責任者)

- 第9条 学園の最高情報責任者（以下「CIO」という。）は、学園の情報システムの管理及びサイバーセキュリティープログラムに関して責任を負うものとする。
- 2 CIOは、統括管理者、責任者及び管理者と連携し、学園の情報システムを用いた個人情報等の適切な管理及び適切な情報システムを整備する任に当たるものとする。
  - 3 CIOは、統括管理者と協力し、個人情報等が含まれる電磁的記録の適切な管理及び保護の確保のため必要な措置を講ずる責任を負うものとする。

#### (最高情報セキュリティ責任者)

- 第10条 学園の最高情報セキュリティ責任者（以下「CISO」という。）は、学園

における情報セキュリティ方針、手続及び管理技術を策定し、情報セキュリティ管理策の実効性をリスクアセスメントなどにより監督する任に当たるものとする。

- 2 CISOは、統括管理者及びCIOと協力し、情報セキュリティを維持する責任を負うものとする。

#### (個人情報保護協議委員会)

第11条 統括管理者は、個人情報等の管理に係る重要事項の決定、連絡及び調整等を行うため、個人情報保護協議委員会（以下「協議委員会」という。）を設置し、定期に又は随時に開催することができる。

- 2 協議委員会は、事務局長を委員長とし、以下の各号に掲げる者から議事ごとに委員長が必要と認める者により構成する。

- (1) CIO
- (2) CISO
- (3) 統括弁護士
- (4) 研究科長
- (5) 副学長（人事担当）
- (6) 副学長（広報担当）
- (7) その他議題に関係する責任者、管理者又は役職員

- 3 協議委員会の運営に関し必要な事項は、統括管理者が定める。

#### (監査責任者)

第12条 学園に、個人情報保護監査責任者（以下「監査責任者」という。）を置き、学園の最高内部監査責任者をもって充てるものとする。

- 2 監査責任者は、定期的に又は必要に応じて、学園の個人情報等の管理状況に対する監査を実施するものとする。

#### (役職員等の研修)

第13条 統括管理者は、個人情報等の取扱いに従事する役職員等に対し、個人情報等の取扱いについて理解を深め、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研修を行うものとする。

- 2 統括管理者は、CIOと連携し、個人情報等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学園の役職員等に対し、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研修を行うものとする。
- 3 統括管理者は、管理者及び担当者に対し、所管する部署等の現場における個人情報等の適切な管理のための教育研修を実施する。
- 4 管理者は役職員等に対し、個人情報等の適切な管理のために総括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ものとする。

**(役職員等の責務)**

- 第14条 役職員等は、法の趣旨に則り、関連する法令及び規則等の定めを遵守するとともに、統括管理者、責任者、管理者及び担当者の指示に従い、個人情報等を取り扱わなければならない。
- 2 役職員等は、その業務に関して知り得た個人情報等の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。

**(利用目的の特定)**

- 第15条 学園は、個人情報を取り扱うに当たっては、当該個人情報を取り扱う事務を遂行するため必要な場合に限り、かつ、その利用の目的(以下「利用目的」という。)をできる限り特定しなければならない。
- 2 学園は、利用目的を変更する場合は、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

**(利用目的による制限)**

- 第16条 学園は、次に掲げる場合を除き、前条の規定により特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。
- (1) 法令に基づく場合
  - (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
  - (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
  - (4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
  - (5) 当該個人情報を学術研究の用に供する目的(以下「学術研究目的」という。)で取り扱う必要があるとき(当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。)
  - (6) 大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者(以下「学術研究機関等」という。)に個人情報を提供する場合であって、当該学術研究機関等が当該個人情報を学術研究目的で取り扱う必要があるとき(当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。)
- 2 学園は、前条の規定により特定された利用目的の範囲を超えて個人情報を取り扱う場合には、前項各号に掲げる場合を除き、あらかじめ本人から同意を得なければならない。

**(不適正な利用の禁止)**

第17条 学園は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

#### (適正な取得)

第18条 学園は偽りその他不正の手段により個人情報を取得してはならない。

2 学園は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

(1) 法令に基づく場合

(2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

(3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

(4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(5) 当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

(6) 学術研究機関等から当該要配慮個人情報を取得する場合であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき（当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（学園と当該学術研究機関等が共同して学術研究を行う場合に限る。）。

(7) 当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、法第五十七条第一項各号に掲げる者その他個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号。以下「施行規則」という。）第6条に定める者により公開されている場合

(8) その他前各号に掲げる場合に準ずるものとして個人情報の保護に関する法律施行令（平成15年政令第507号。以下「施行令」という。）第9条に定める場合

#### (取得に際しての利用目的の通知等)

第19条 学園は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

2 学園は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を

明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

- 3 学園は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。
- 4 前3項の規定は、次に掲げる場合については、適用しない。
  - (1) 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
  - (2) 利用目的を本人に通知し、又は公表することにより学園の権利又は正当な利益を害するおそれがある場合
  - (3) 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
  - (4) 取得の状況からみて利用目的が明らかであると認められる場合

#### (正確性の確保等)

第20条 役職員等は、利用目的の達成に必要な範囲内で、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

- 2 役職員等は、個人データの内容に誤り等を発見した場合には、管理者の指示に従い、訂正等を行わなければならない。
- 3 役職員等は、個人データ又は個人データ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、当該個人情報の復元又は判読が不可能な方法により当該個人データの削除又は当該媒体の廃棄を行わなければならない。

#### (安全管理措置)

第21条 統括管理者は、取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずるとともに、これを役職員等に遵守させなければならない。

#### (業務の委託等)

第22条 管理者は、個人データの取扱いに係る業務を外部に委託する場合には、選定の際に個人データの管理能力の確認を行うなどの、必要な措置を講じなければならない。

- 2 管理者は、個人データの取扱いに係る業務の外部委託に関する契約書について、本規則のほか、C I S Oが別に定めるガイドラインに基づき作成しなければならない。
- 3 管理者は、選定した第三者と前項に規定する業務の委託契約を締結する際には、契約書に、次に掲げる事項を明記するとともに、委託先における業務責任者及び業務従事者の管理及び実施体制並びに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ものとする。

- (1) 学園が講ずべき安全管理措置と同等の措置を講じること
  - (2) 個人データに関する秘密保持、目的外利用の禁止等の義務
  - (3) 再委託(再委託先が委託先の子会社(会社法(平成17年法律第86号、第2条第1項第3号に規定する子会社をいう。)である場合を含む。以下同じ。)の制限又は事前承認等再委託に係る条件に関する事項
  - (4) 個人データの複製等の制限に関する事項
  - (5) 個人データの漏えい等の事案の発生時における対応に関する事項(委託先による保護管理者に対する漏えい等の事案の発生に係る報告を含むがこれに限られない。)
  - (6) 委託終了時における個人データの消去及び媒体の返却に関する事項
  - (7) 違反した場合における契約解除、損害賠償責任その他必要な事項
  - (8) 前各号に掲げるもののほか、委託する個人データの取扱いの性質から必要な事項。
- 4 管理者は、個人データの取扱いに係る業務を外部に委託する場合には、委託する業務に係る個人データの秘匿性等その内容やその量等に応じて、委託先における管理体制及び実施体制や個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認するものとする。
- 5 管理者は、委託先において個人データ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項及び第3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個人データ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。なお、個人データ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。
- 6 管理者は、個人データの取扱を派遣職員に行わせる場合、当該派遣職員に係る労働者派遣契約書に、秘密保持義務等個人情報の取扱に関する事項を明記しなければならない。

#### (アクセス制限)

第23条 管理者は、CIOと連携し、個人データの秘匿性等その内容(匿名化の程度等による個人識別の容易性、要配慮個人情報の有無並びに漏えい等が発生した場合に生じ得る被害の性質及びその程度等を含む。以下同じ。)に応じて、個人データにアクセスする権限を有する役職員等の範囲と権限の内容を、当該役職員等が業務を行う上で必要最小限の範囲に限る。

- 2 アクセス権限を有しない役職員等は、個人データにアクセスしてはならない。
- 3 アクセス権限を有する役職員等であっても、業務上の目的以外の目的で個人データにアクセスしてはならない。

#### (複製等の制限)

第24条 管理者は、役職員等が業務上の目的で個人データ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、当該保有個人情報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なければならない。

- (1) 個人データの複製
- (2) 個人データの送信
- (3) 個人データが記録されている媒体の外部への送付又は持出し
- (4) その他個人データの適切な管理に支障を及ぼすおそれのある行為

2 役職員等は、前項各号の行為を行うときは、管理者の許可を得るものとする。

### (媒体の管理等)

第25条 役職員等は、管理者の指示に従い、個人データが記録されている媒体を管理者により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、耐火金庫への保管又は戸棚の施錠等を行うものとする。

### (第三者提供の制限)

第26条 学園は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

- (1) 法令に基づく場合
- (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
- (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
- (4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- (5) 当該個人データの提供が学術研究の成果を公表し、又は教授するためにやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）。
- (6) 当該個人データを学術研究目的で提供する必要があるとき（当該個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（学園と当該第三者が共同して学術研究を行う場合に限る。）。
- (7) 当該第三者が学術研究機関等である場合であって、当該第三者が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

2 次に掲げる場合において、当該個人データの提供を受ける者は、前項に規定の適用については第三者に該当しないものとする。

- (1) 学園が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合



- (2) 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的並びに当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。
- 3 学園は、前項第2号に規定する個人データの管理について責任を有する者の氏名、名称若しくは住所又は法人にあっては、その代表者の氏名に変更があったときは遅滞なく、同号に規定する利用する者の利用目的又は当該責任を有する者を変更しようとするときはあらかじめ、その旨について、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

### (外国にある第三者への提供の制限)

第27条 前条の規定にかかわらず、学園が外国（本邦の域外にある国又は地域をいう。）にある第三者に個人データを提供する場合は、次に掲げる場合を除き、あらかじめ当該外国の第三者への提供を認める旨の本人の同意を得なければならない。

- (1) 前条第1項各号に該当する場合
- (2) 個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人データの保護に関する制度を有している外国として施行規則第15条に定める国にある第三者に提供する場合
- (3) 個人データの取扱いについて個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして施行規則第16条で定める基準に適合する体制を整備している者に提供する場合
- 2 前項の規定により本人の同意を得ようとする場合には、学園は、施行規則第17条に定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない。
- 3 学園は、個人データを外国にある第三者（第1項に規定する体制を整備している者に限る。）に提供した場合には、施行規則第18条に定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない。

### (第三者提供に係る記録の作成等)

第28条 学園が個人データを第三者に提供したときは、管理者は施行規則第19条に定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他同規則第20条に関する記録を作成しなければならない。ただし、当該個人データの提供が第26条第1項各号又は第2項各号のいずれか（前条第

1 項の規定による個人情報の提供にあつては、第26条第1項各号のいずれかに該当する場合は、この限りでない。

- 2 管理者は前項の記録を、当該記録を作成した日から原則として3年間（施行規則第21条第1号又は第2号に掲げる場合にあつては、当該各号に定める期間）保存しなければならない。

#### （第三者提供を受ける際の確認等）

第29条 学園が第三者から個人データの提供を受けるに際しては、管理者は施行規則第22条に定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第26条第1項各号又は第2項各号のいずれかに該当する場合は、この限りでない。

- (1) 当該第三者の氏名又は名称及び住所並びに法人にあつては、その代表者の氏名
- (2) 当該第三者による当該個人データの取得の経緯

2 前項の第三者は、管理者が同項の規定による確認を行う場合において、学園に対して、当該確認に係る事項を偽ってはならない。

3 管理者は前項の規定による確認を行ったときは、施行規則第23条に定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他同規則第24条に定める事項に関する記録を作成しなければならない。

- 4 管理者は前項の記録について、当該記録を作成した日から原則として3年間（施行規則第25条第1号又は第2号に掲げる場合にあつては、当該各号に定める期間）保存しなければならない。

#### （個人関連情報の第三者提供の制限等）

第30条 学園は第三者が個人関連情報（個人関連情報データベース等を構成するものに限る。以下同じ。）を個人データとして取得することが想定されるときは、第26条第1項各号に掲げる場合を除くほか、次に掲げる事項について、あらかじめ施行規則第26条に定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。

- (1) 当該第三者が学園から個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の当該本人の同意が得られていること
- (2) 外国にある第三者への提供にあつては、前号の本人の同意を得ようとする場合において、施行規則第17条に定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報が当該本人に提供されていること

2 第27条3項の規定は、前項の規定により学園が個人関連情報を提供する場合について準用する。この場合において、同条第3項中「講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供し」とあるのは、「講じ」と読み替えるものとする。

- 3 前条第2項及び第3項の規定は、第1項の規定により学園が確認する場合について準用する。この場合において、同条第3項中「の提供を受けた」とあるのは、「を提供した」と読み替えるものとする。

#### (学術機関等としての責務)

第31条 学園は、学術研究目的で行う個人情報の取扱いについて、法の規定を遵守するとともに、その適正を確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

#### (仮名加工情報の作成等)

第32条 学園は、仮名加工情報（仮名加工情報データベース等を構成するものに限る。）を作成するときは、他の情報と照合しない限り特定の個人を識別することができないようにするために必要なものとして施行規則第31条に定める基準に従い、個人情報を加工しなければならない。

- 2 学園は、仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等（仮名加工情報の作成に用いられた個人情報から削除された記述等及び個人識別符号並びに前項の規定により行われた加工の方法に関する情報をいう。）を取得したときは、削除情報等の漏えいを防止するために必要なものとして同規則32条に定める基準に従い、削除情報等の安全管理のための措置を講じなければならない。
- 3 学園は、第16条の規定にかかわらず、法令に基づく場合を除くほか、第15条第1項の規定により特定された利用目的の達成に必要な範囲を超えて、仮名加工情報（個人情報であるものに限る。以下この条において同じ。）を取り扱ってはならない。
- 4 仮名加工情報についての第19条の規定の適用については、同条第1項及び第3項中「、本人に通知し、又は公表し」とあるのは「公表し」と、同条第4項第1号から第3号までの規定中「本人に通知し、又は公表する」とあるのは「公表する」とする。
- 5 学園は、仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去するよう努めなければならない。なお、この場合においては、第20条の規定は、適用しない。
- 6 学園は、第26条1項及び第27条の規定に関わらず、法令に基づく場合を除き、仮名加工情報である個人データを第三者に提供してはならない。この場合において、第26条2項中「前項」とあるのは、「第32条第6項」と、同項第2号中「、本人に通知し、又は本人が容易に知り得る状態に置いているとき」とあるのは「公表しているとき」と、同条第3項中「本人に通知し、又は本人が容易に知りうる状態に置かなければ」とあるのは「公表しなれば」とし、第28条第1項ただし書中「第26条第1項各号又は第2項各号のいずれか（前条第1項の規定による個人情報の提供にあつては、第26条第1項各号のいずれか）」とあり、

- 及び第29条第1項ただし書中「第26条第1項各号又は第2項各号のいずれか」とあるのは「法令に基づく場合又は第26条第2項各号のいずれか」とする。
- 7 学園は、仮名加工情報を取り扱うにあたっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合してはならない。
  - 8 学園は、仮名加工情報を取扱うにあたっては、電話をかけ、郵便若しくは電磁的方法その他の法第41条第8項に定める方法を用いて送信し又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用してはならない。
  - 9 仮名加工情報、仮名加工情報である個人データについては、第15条第2項、第56条及び第58条の規定は、適用しない。
  - 10 前各項の規定は、学園から仮名加工情報の取扱いの委託（二以上の段階にわたる委託を含む。）を受けた者が受託した業務を行う場合について準用するものとする。

#### （仮名加工情報の第三者提供の制限等）

- 第33条 学園は、法令に基づく場合を除くほか、仮名加工情報（個人情報であるものを除く。以下この条において同じ。）を第三者に提供してはならない。
- 2 第26条第2項の規定は、仮名加工情報の提供を受ける者について準用する。この場合において、同項第2号中「、本人に通知し、又は本人が容易に知り得る状態に置いているとき」とあるのは「公表しているとき」と、同条第3項中「本人に通知し、又は本人が容易に知りうる状態に置かなければ」とあるのは「公表しなれば」と読み替えるものとする。
  - 3 第21条から第25条まで並びに前条第7項及び第8項の規定は、仮名加工情報の取扱いについて準用する。この場合において、第21条中「漏えい等」とあるのは「漏えい」と、前条第7項中「ために、」とあるのは「ために、削除情報等」を取得し、又は」と読み替えるものとする。

#### （特定個人情報の取扱）

- 第34条 特定個人情報の取扱いについては、学園の個人番号及び特定個人情報取扱規程に定める。

#### （行政機関等匿名加工情報の取扱）

- 第35条 行政機関等非識別加工情報の取扱いについては、学園の行政機関等匿名加工情報の提供等に関する規程に定める。

#### （個人情報ファイル）

- 第36条 管理者は、個人情報ファイルを保有するに当たっては、学園の個人情報ファイル登録リスト（以下「PIPL」という。）に登録しなければならない。
- 2 管理者は、PIPLに登録した個人情報ファイルの内容に変更が生じたときは、

PIPLの登録情報を速やかに更新しなければならない。

### (個人情報ファイル簿の作成及び公表)

第37条 学園は、保有している個人情報ファイルについて、それぞれ次に掲げる事項を記載した帳簿(以下「個人情報ファイル簿」という。)を作成し、公表しなければならない。

- (1) 個人情報ファイルの名称
- (2) 学園の名称及び個人情報ファイルが利用に供される事務をつかさどる組織の名称
- (3) 個人情報ファイルの利用目的
- (4) 個人情報ファイルに記録される項目(以下「記録項目」という。)及び本人(他の個人の氏名、生年月日その他の記述等によらないで検索し得る者に限る。以下同じ。)として個人情報ファイルに記録される個人の範囲(以下、「記録範囲」という。)
- (5) 個人情報ファイルに記録される個人情報(以下「記録情報」という。)の収集方法
- (6) 記録情報に要配慮個人情報が含まれるときは、その旨
- (7) 記録情報を学園以外の者に経常的に提供する場合には、その提供先
- (8) 保有個人情報の開示、訂正又は利用停止に係る請求を受理する組織の名称及び所在地
- (9) 保有個人情報の訂正又は利用停止に係る請求について法令の規定により特別の手続きが定められている場合には、その旨
- (10) その他施行令第21条6項に定められた事項

2 個人情報ファイル簿は、法令・コンプライアンスセクションが整備し、保管及び公表する。ただし、次の各号に掲げる個人情報ファイルは個人情報ファイル簿に掲載しないものとする。

- (1) 役職員等の人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項を記録するもの(学園が行う職員の採用試験に関する個人情報ファイルを含む。)
- (2) 専ら試験的な電子計算機処理の用に供するための個人情報ファイル
- (3) 前項の規定による公表に係る個人情報ファイルに記録されている記録情報の全部又は一部を記録した個人情報ファイルであって、その利用目的、記録項目及び記録範囲が当該公表に係るこれらの事項の範囲内のもの
- (4) 一年以内に消去される個人情報のみを記録している個人情報ファイル
- (5) 資料その他の物品・金銭の送付又は業務連絡上必要な連絡のために利用する個人情報ファイルであって、送付又は連絡の相手方の氏名、住所その他の送

付又は連絡に必要な事項のみを記録するもの

- (6) 役職員等が学術研究の用に供するためにその発意に基づき作成し、又は取得する個人情報ファイルであって、記録情報を専ら当該学術研究の目的のために利用するもの
- (7) 記録されている本人の数が1,000人に満たない個人情報ファイル
- (8) その他施行令第20条第3項及び同令第21条第7項に定める個人情報ファイル

- 3 管理者は、個人情報ファイル簿に記載すべき個人情報ファイルを新たに保有したとき又は個人情報ファイル簿に記載されている事項を変更する必要があるときは、個人情報ファイル簿を更新するよう法令・コンプライアンスセクションに連絡しなければならない。

### (アクセス制御)

- 第38条 管理者は、CIOと連携し、個人情報等（情報システムで取り扱うものに限る。以下第52条までの規定（第50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じなければならない。
- 2 管理者は、CIOと連携し、前条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じなければならない。

### (アクセス記録)

- 第39条 管理者は、CIOと連携し、個人情報等の秘匿性等その内容に応じて、当該個人情報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。）を一定の期間保存し、及びアクセス記録を定期に及び必要に応じ随時に分析するために必要な措置を講じなければならない。
- 2 管理者は、CIOと連携し、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じなければならない。

### (アクセス状況の監視)

- 第40条 管理者は、CIOと連携し、個人情報等の秘匿性等その内容及びその量に応じて、当該個人情報等への不適切なアクセスの監視のため、個人情報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じなければならない。

### (管理者権限の設定)

- 第41条 管理者は、個人情報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じなければならない。

#### (外部からの不正アクセスの防止)

第42条 管理者は、CIOと連携し、個人情報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じなければならない。

#### (不正プログラムによる漏えい等の防止)

第43条 管理者は、CIOと連携し、不正プログラムによる個人情報等の漏えい等の防止のため、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。）を講じなければならない。

#### (情報システムにおける個人情報等の処理)

第44条 役職員等は、個人情報等について、情報システムにおいて一時的に加工等を行うため複製等の処理を行う場合には、その対象を必要最小限とし、処理終了後は、不要となった情報を速やかに消去しなければならない。

- 2 管理者は、前項の場合、個人情報等の秘匿性等その内容に応じて、随時、前項の処理に係る消去等の実施状況を重点的に確認しなければならない。

#### (暗号化)

第45条 管理者は、CIOと連携し、個人情報等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じなければならない。

- 2 教職員等は、前項を踏まえ、その処理する個人情報等について、当該個人情報等の秘匿性等その内容に応じて、適切に暗号化を行わなければならない。

#### (記録機能を有する機器及び媒体の接続制限)

第46条 管理者は、CIOと連携し、個人情報等の秘匿性等その内容に応じて、当該個人情報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じなければならない。

#### (端末の限定)

第47条 管理者は、個人情報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じなければならない。

#### (端末の盗難防止等)

第48条 管理者は、端末の盗難又は紛失の防止のため、必要に応じ、端末の固定、執務室の施錠等の措置を講じなければならない。

- 2 役職員等は、管理者が必要を認めるときを除き、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49条 役職員等は、端末の使用に当たっては、個人情報等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じなければならない。

#### (入力情報の照合等)

第50条 役職員等は、情報システムで取り扱う個人情報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情報等の内容の確認、既存の個人情報等との照合等を行わなければならない。

#### (バックアップ)

第51条 管理者は、CIOと連携し、個人情報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じなければならない。

#### (情報システム設計書等の管理)

第52条 管理者は、個人情報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に、その保管、複製、廃棄等について必要な措置を講じなければならない。

#### (入室管理)

第53条 管理者は、CIOと連携し、個人情報等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教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、個人情報等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、同様の措置を講じなければならない。

2 管理者は、CIOと連携し、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じなければならない。

3 管理者は、CIOと連携し情報システム室等及び保管施設の入退室の管理について、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し及び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。）並び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じなければならない。

#### (情報システム室等の管理)

第54条 管理者は、CIOと連携し、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じなければならない。



- 2 管理者は、C I Oと連携し、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講じなければならない。

#### (事案の報告等)

第55条 役職員等は、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担当者が関連する法令及び規程等の定め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を認識した場合には、直ちに当該個人情報等を管理する管理者及び統括管理者に報告又は相談しなければならない。

- 2 管理者は、前項の報告を受けたとき、直ちに責任者に報告しなければならない。また、当該報告が統括管理者に通知されている事を確認しなければならない。
- 3 管理者は、第1項の報告を受けたとき、C I S Oと協力し、外部からの不正アクセスや不正プログラム感染が疑われる当該端末等のLANケーブルを抜くなど、直ちに被害の拡大防止のために必要な措置を行うとともに（役職員等に行わせることを含む。）、事案の発生した状況や原因等を調査、統括管理者に報告書を提出しなければならない。なお、報告書の提出後に判明した事項について、逐次追加報告することを妨げない。
- 4 統括管理者は前項の報告書を元に、管理者に当該事案に係る個人情報等の本人へ対する通知を行うよう指示するものとする。
- 5 管理者は、前項の指示に基づき、当該本人に対し、当該本人の権利利益を保護するために必要な範囲において、事態の概要、保有個人情報の項目、原因、二次被害又はそのおそれの有無及びその内容並びにその他参考となる事項を速やかに通知しなければならない。ただし、当該本人への通知が困難な場合であって、当該本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。なお、通知は、必要に応じて当該本人の関係者又は所属団体等に対しても行うものとする。
- 6 統括管理者は、第1項の報告を受けたとき、C I S Oと連携し、事案の内容等に応じて、当該事案の内容、被害状況等を確認した上で、事案が軽微であるかどうかを判断する。
- 7 統括管理者は、前項において事案が軽微であると判断されたとき、当該事案の管理に関する責任者に対し、再発防止を含む注意喚起を行うこととする。
- 8 統括管理者は、第5項において軽微であると認められない事案が発生した場合、当該事案が生じた旨を速やかに理事長に報告しなければならない。

#### (漏えい等の報告等)

第56条 統括管理者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして次に掲げる事態が生じたときは、施行規則第8条に定めるところ

により、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、学園が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、同規則第9条に定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

- (1) 要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条において同じ。）の漏えい等が発生し、又は発生したおそれがある事態
  - (2) 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
  - (3) 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
  - (4) 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態。
- 2 統括管理者は前項の報告をする場合には、前条各号に定める事態を知った後、速やかに、当該事態に関する次に掲げる事項（報告を使用とする時点において把握しているものに限る。）を国の個人情報保護委員会に報告しなければならない。
- (1) 概要
  - (2) 漏えい等が発生し、又は発生したおそれがある個人データの項目
  - (3) 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
  - (4) 原因
  - (5) 二次被害又はそのおそれの有無及びその内容
  - (6) 本人への対応の実施状況
  - (7) 公表の実施状況
  - (8) 再発防止のための措置
  - (9) その他参考となる事項
- 3 統括管理者は、前項の場合において、当該事態を知った日から30日以内（当該事態が第1項第3号に定めるものである場合にあっては、60日以内）に、当該事態に関する前項各号に定める事項を、国の個人情報保護委員会に報告しなければならない。

#### (再発防止措置)

- 第57条 管理者は、事案の発生した原因を分析し、統括管理者に対し、再発防止策を含む最終報告書を速やかに提出しなければならない。
- 2 管理者は、CISO及び他関係職員とともに、前項において報告した再発防止策を実施しなければならない。

#### (公表等)

- 第58条 統括管理者は、前条第1項の最終報告書をもとに、速やかに事実関係及び

再発防止策等を公表しなければならない。

- 2 統括管理者は、前項の規定により公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに関係省庁及び個人情報保護委員会に情報提供を行うものとする。
- 3 統括管理者は、第1項の報告を行ったときは、その内容について、協議委員会に報告するものとする。
- 4 統括管理者は、第1項の報告を行ったときは、理事長に対し、当該事案に関する最終報告書を提出しなければならない。

#### (監査)

第59条 監査責任者は、個人情報等の適切な管理を検証するため、学園における個人情報等の管理状況について、定期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、その結果を統括管理者に報告するものとする。

#### (点検)

第60条 統括管理者は、責任者に対し、少なくとも年1回、所管する各部門における個人情報等の記録媒体、処理経路、保管方法等について、点検及び報告を求めることができる。

- 2 責任者は、前項の求めがあったときは、所管する各部門の管理者に対し、各部署における個人情報等の記録媒体、処理経路、保管方法等について、点検及び報告を命じ、その結果を統括管理者に報告しなければならない。
- 3 管理者は、前項の命を受けたときは、各部署における個人情報等の記録媒体、処理経路、保管方法等について、点検を実施し、その報告を責任者に報告しなければならない。
- 4 管理者は、各部署等における保有個人情報の記録媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、その結果を責任者に報告し、必要があると認めるときは、その結果について、責任者を通じて統括管理者に報告するものとする。

#### (評価及び見直し)

第61条 統括管理者、責任者、管理者等は、前条の点検又は第59条の監査の結果等を踏まえ、実効性等の観点から個人情報等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、その見直し等を実施するものとする。

#### (行政機関との連携)

第62条 学園は、「個人情報の保護に関する基本方針」（平成16年4月2日閣議決定）を踏まえ、内閣府沖繩振興局と緊密に連携して、その保有する個人情報の適切な管理を行うものとする。

#### (事務局)

第63条 本規則に関する事務は、CIO及びCISOが行う事務にあつては情報セキュリティセクションが、統括管理者が行う事務にあつては法令・コンプライアンスセクションが行う。

**(懲戒)**

第64条 役職員等が本規則の規定に違反した場合、学園は、当該役職員等について、学園の就業規則又は学則等に定める懲戒処分の対象とすることがある。

**(雑則)**

第65条 本規則に定めるもののほか、個人情報保護の事務処理並びに保有個人情報の開示、訂正、利用停止請求等に関して必要な事項は、事務局長が別に定める。

**(旧沖縄科学技術研究基盤整備機構からの移行)**

第66条 旧独立行政法人沖縄科学技術研究基盤整備機構から学園へ移行する際に、機構が保有していた個人情報は、全て学園に引き継がれ、本規則が適用される。

附則

本規則は、2022年4月1日から施行する。

附則

本規則は、2023年1月1日から施行する。

附則

本規則は、2023年8月1日から施行する。

附則

本規則は、2024年4月1日から施行する。