○東京藝術大学情報セキュリティ管理規則

（平成28年10月20日制定）

第１章　総則

（趣旨）

第１条　この規則は、本学における情報セキュリティ管理に関し必要な基本事項を定める。

（適用範囲）

第２条　この規則は、役職員、学生その他情報資産を取り扱う全ての者（学外者を含む。以下「利用者」という。）に適用する。

（定義）

第３条　この規則において、次の各号に掲げる用語の定義は、それぞれ当該各号に定めるところによる。

（１）個人情報　独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号。以下「保護法」という。）第２条第２項に規定する個人情報をいう。

（２）保有個人情報　保護法第２条第３項に規定する保有個人情報をいう。

（３）個人番号　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）第２条第５項に規定する個人番号をいう。

（４）情報ネットワーク　情報機器(ハードウェア)を相互に接続するための通信回線網及びその構成機器をいう。

（５）情報システム　情報処理及び情報ネットワークに係るシステムで、次に掲げるものをいい、その他本学情報ネットワークに接続する機器を含むものとする。

イ　本学が所有又は管理するもの

ロ　本学との契約あるいは他の協定に従って提供されるもの

ハ　本学の個人情報又は保有個人情報を取り扱うもの

（６）情報資産　情報システム並びに本学が作成又は取得したものであって、電磁的記録媒体及び紙媒体に記録された情報をいう。

（７）機密性　情報資産に対し、アクセスを許可された者だけがこれにアクセスできる特性をいう。

（８）完全性　情報資産が、破壊、改ざん又は消去されていない特性をいう。

（９）可用性　情報資産へのアクセスを許可された者が、必要時に中断することなく、当該情報資産にアクセスできる特性をいう。

(10) 情報セキュリティ　情報資産の機密性、完全性及び可用性を確保することをいう。

(11) 暗号化　第三者に容易に解読されないよう、定められた演算を施しデータを変換することをいう。

(12) 主体認証情報　情報システムにアクセスしようとする利用者又は電子計算機が、当該情報システムにアクセスする正当な権限を有することを証するため

に、情報システムに提示する情報をいう。
(13) インシデント　意図的又は偶発的に生じる情報セキュリティを害する事象（情報セキュリティを害するリスクを高めるものを含む。）をいう。
(14) 違反行為　情報資産の取扱いに関し、本学の規則等に反する直接的又は間接的な行為をいう。
(15) 部局　各学部、各研究科、附属図書館、大学美術館、社会連携センター、言語・音声トレーニングセンター、演奏芸術センター、保健管理センター、芸術情報センター、藝大アートプラザ、美術学部附属古美術研究施設、音楽学部附属音楽高等学校及び事務局をいう。

第２章　情報管理の組織及び体制

（情報セキュリティ統括責任者）

第４条　本学の情報セキュリティの管理に関し総括する者として、東京藝術大学情報戦略規則第３条に基づく、情報セキュリティ統括責任者（以下「CISO」という。）を置く。

２　CISOは、東京藝術大学情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）及び情報セキュリティポリシーに基づく関係諸規則等（以下「情報セキュリティ関係諸規則等」という。）を整備する。

３　CISOは、情報資産の諸問題に対する措置を講ずる。

４　CISOは、インシデントの発生を未然に防止し、又はその発生後の対応策を講ずるため、全学又は部局における情報セキュリティの実施状況を調査することができる。

５　CISOは、本学の情報セキュリティ上のリスクが高くインシデントの発生を未然に防止する必要性が高い場合又はインシデント発生後の対応策として必要と認める場合、本学又は特定の部局の情報システムの全部又はその一部を停止することを第８条に規定する全学情報システム・セキュリティ責任者又は第10条に規定する部局情報保護管理責任者に命ずるものとする。

６　CISOは、本学の情報セキュリティに関わる情報を入手した場合、第10条に規定する部局情報保護管理責任者に通知し、情報セキュリティの維持を図る。

７　CISOは、情報セキュリティに関する全学的な教育を統括する。

８　CISOに事故あるときは、CISOがあらかじめ指名する者がその職務を代行する。

（情報セキュリティアドバイザー）

第５条　CISOを補佐するため、必要に応じて情報セキュリティアドバイザーを置くことができる。

２　情報セキュリティアドバイザーは、情報セキュリティに関する専門的知識及び経験を有する者のうちから、CISOが委嘱する。

３　情報セキュリティアドバイザーは、CISOに対し、情報セキュリティに関する助言を行う。

（情報セキュリティ委員会）

第６条　本学の情報セキュリティに関する重要事項を審議するため、情報セキュリティ委員会（以下「委員会」という。）を置く。

２　委員会に関し必要な事項は、別に定める。

（情報システム緊急対応チーム）

第７条　本学におけるインシデント発生時に迅速かつ円滑な対応を図るため、情報システム緊急対応チーム（Computer Emergency Response Team。以下「TUA-CERT」という。）を置く。

２　TUA-CERTに関し必要な事項は、別に定める。

（全学情報システム・セキュリティ責任者）

第８条　全学の情報システム管理を実施し、CISOを補佐するため、全学情報システム・セキュリティ責任者を置き、東京藝術大学情報戦略統括室（以下「統括室」という。）室長補佐をもって充てる。

２　全学情報システム・セキュリティ責任者は、情報システムの対外接続に関する業務を統括し、全学の情報システムの管理を実施するために必要な事項を定めることができる。

３　全学情報システム・セキュリティ責任者は、本学の情報セキュリティが脅かされると判断する緊急の場合には、必要な対応を執る権限を有する。

（全学情報システム・セキュリティ管理者）

第９条　全学情報システム・セキュリティ責任者を補佐するため、全学情報システム・セキュリティ管理者を置き、統括室情報セキュリティ担当主任をもって充てる。

２　全学情報システム・セキュリティ管理者は、情報システムの対外接続に関する実務を実施する。

（部局情報保護管理責任者）

第１０条　情報資産及び情報システムを保有する部局に、部局情報保護管理責任者を置き、当該部局の長をもって充てる。

２　部局情報保護管理責任者は、部局の情報セキュリティに関し責任を負う。

３　部局情報保護管理責任者は、前項の職責に関して、CISOに助言を求めることができる。

４　部局情報保護管理責任者は、当該部局において情報資産の機密性、完全性若しくは可用性が脅かされる事態が認められ、又は疑われる場合、全学情報システム・セキュリティ責任者に報告するとともに、対応措置を施した結果を報告する責務を有する。

５　部局情報保護管理責任者は、第４条第６項の通知を受けた場合、速やかに関係する者に連絡し、必要な措置を講じ、その実施状況を記録するものとする。

（部局情報保護管理者）

第１１条　部局情報保護管理責任者を補佐するため、部局情報保護管理者を置く。

２　部局情報保護管理者は、部局情報保護管理責任者が指名する。

（部局情報セキュリティアドバイザー）

第１２条　部局情報保護管理責任者を補佐するため、必要に応じて部局情報セキュリティアドバイザーを置くことができる。

２　部局情報セキュリティアドバイザーは、情報セキュリティに関する専門的知識及び経験を有する者のうちから、部局情報保護管理責任者が委嘱する。

３　部局情報セキュリティアドバイザーは、部局情報保護管理責任者に対し、情報セキュリティに関する助言を行う。

（情報システム責任者）
第１３条　部局情報保護管理責任者は、当該部局が所有又は管理する全ての情報システムごとに情報システム責任者を指名する。この場合において、情報システム責任者は、本学の職員でなければならない。
２　情報システム責任者が本学の所属を離れる場合、部局情報保護管理責任者は、後任の情報システム責任者を速やかに指名する。
３　情報システム責任者は、当該情報システムの情報セキュリティに関し責任を負うものとする。

第３章　情報セキュリティの実施

（情報資産の管理及び取扱いにおける対策）
第１４条　情報資産を取り扱う者は、当該情報資産の特性に応じて適切な情報セキュリティ対策を講じるものとし、本学の情報セキュリティ水準の低下を招く行為を行ってはならない。
２　前項に定めるもののほか、情報資産の管理及び取扱いに関する事項は、別に定める。
（情報システムのセキュリティ管理等における対策）
第１５条　情報システムを運用、管理又は利用する者は、本学の情報セキュリティ水準の低下を招く行為を行ってはならない。
２　前項に定めるもののほか、情報システムのセキュリティ管理等に関する事項は、別に定める。
（暗号化及び主体認証情報）
第１６条　情報資産を暗号化する際の鍵及び主体認証情報は、自己以外の者に推知されることが困難であるものを使用し、その管理に当たっては、他人に知られることのないよう十分に注意しなければならない。
２　前項に定めるもののほか、情報資産の暗号化等に関する事項は、別に定める。
（本学が所有又は管理しない情報システムに係るセキュリティ管理措置）
第１７条　本学が所有又は管理しない情報システムにより情報資産を取り扱う場合も、本学の情報セキュリティ関係諸規則等に従ってセキュリティ対策を施さなければならない。
２　本学が所有又は管理しない情報システムの使用等に関し必要な事項は、別に定める。
（外部委託）
第１８条　本学の情報システム又は情報資産の取扱いに関して外部委託を行う場合は、委託先において情報セキュリティが徹底されるよう、必要な措置を講じなければならない。
（保有個人情報に関する特則）
第１９条　この規則に定めるもののほか、保有個人情報及び個人番号の適切な管理に関し必要な事項は、東京藝術大学個人情報管理規則及び東京藝術大学特定個人情報取扱規則に定めるところによる。

第４章　教育・研修

（情報セキュリティ教育）

第２０条　CISOは、情報セキュリティ関係諸規則等について、全学情報システム・セキュリティ責任者、部局情報保護管理責任者、部局情報保護管理者、情報システム責任者及び職員（以下「教育啓発対象者」という。）に対し、その啓発を行うものとする。

２　CISOは、教育啓発対象者が各年度につき少なくとも１回は研修会等を受講できるように、情報セキュリティ対策の教育に係る計画を企画・立案するとともに、その実施体制を整備するものとする。

３　部局情報保護管理責任者は、部局内の利用者に対して、情報セキュリティ関係諸規則等及びその適正な実施について、適時啓発を行うものとする。

第５章　緊急時の対応等

（緊急時における体制の整備）

第２１条　CISOは、情報セキュリティに関するインシデントが発生した場合、TUA-CERTへ指示を行い、被害の拡大を防ぐとともに、インシデントから復旧するための体制を整備するものとする。

２　CISOは、インシデントについて利用者から部局情報保護管理責任者に対する報告の手順を整備し、当該報告の手順を全ての利用者に周知するものとする。

３　CISOは、インシデントが発生した際の対応手順を整備するものとする。

４　CISOは、インシデントに備え、本学の教育、研究及び事務の遂行のため特に重要と認めた情報システムについて、当該情報システムを所有又は管理する部局の部局情報保護管理責任者及び当該情報システムの情報システム責任者の緊急連絡先、連絡手段及び連絡内容を含む緊急連絡網を整備するものとする。

５　CISOは、インシデントについて学外から報告を受けるための窓口を設置し、当該窓口への連絡手段を学外に公表するものとする。

（インシデント対応）

第２２条　部局情報保護管理責任者は、別に定める情報セキュリティインシデント発生時の報告・連絡要領に基づき、インシデントが発生した場合には、直ちにTUA-CERTに報告するものとする。

２　TUA-CERTは、当該部局情報保護管理責任者と協力してインシデントの原因を調査し、及び再発防止策を策定し、その結果を報告書としてCISOに提出するものとする。

３　CISOは、TUA-CERTからインシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講じるものとする。

４　インシデントの原因が利用者の違反行為による場合、CISOは、学長又は関係する部局情報保護管理責任者に対し、当該違反行為を報告するものとする。

５　前項の規定による報告を受けた学長は、当該違反行為を行った職員又は学生に対して、東京藝術大学就業規則、東京藝術大学学則、東京藝術大学大学院学則その他関係諸規則に基づき、処分等を行うことができる。

第６章　自己点検・評価

（情報セキュリティ管理の見直し）

第２３条　情報セキュリティ関係諸規則等を整備した者は、各規則等の見直しの必要性を適時検討し、必要がある場合は、その見直しを行うものとする。
２　CISOは、全学の情報資産の取扱い及び情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合には、当該対策について見直しを行うとともに、必要な措置を講ずるものとする。
３　部局情報保護管理責任者は、部局の情報資産の取扱い及び情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合には、当該対策について見直しを行うとともに、必要な措置を講ずるものとする。
（自己点検）
第２４条　CISOは、年度自己点検計画を策定するものとする。
２　部局情報保護管理責任者は、CISOが定める年度自己点検計画に基づき、当該部局の職員に対して、自己点検を実施するものとする。
３　部局情報保護管理責任者は、自己点検の結果を評価し、必要があると判断した場合には、当該部局の職員に改善を指示するものとする。
４　部局情報保護管理責任者は、自己点検の結果及び改善の結果をCISOに報告するものとする。
５　前項の報告を受けたCISOは、状況の改善が見られないと判断した場合は、当該部局の情報システムの全部又は一部の利用停止を全学情報システム・セキュリティ責任者に命ずることができる。
（調査）
第２５条　CISOは、必要があるときは、全学の情報システム又は各部局の情報システムの情報セキュリティ関係諸規則等の実施状況、セキュリティ対策の実施状況及び第４条第６項の通知の対応状況について調査を行うことができる。この場合において、全学情報システム・セキュリティ責任者及び部局情報保護管理責任者は、CISOによる調査が円滑かつ適正に実施できるように協力しなければならない。
２　前項の調査の結果、改善の必要があると判断した場合、CISOは、全学情報システム・セキュリティ責任者又は部局情報保護管理責任者に対し改善計画の策定を指示し、併せて委員会に報告するものとする。
３　全学情報システム・セキュリティ責任者又は部局情報保護管理責任者は、前項の改善計画を策定及び実施し、実施状況をCISOに報告するものとする。
４　前項の報告を受けたCISOは、状況の改善が見られないと判断した場合は、当該部局の情報システムの全部又は一部の利用停止を全学情報システム・セキュリティ責任者に命ずることができる。
（監督・検査）
第２６条　CISOは、部局等における情報セキュリティの状況について、必要に応じ監督及び検査を行い、その結果を学長に報告するものとする。

第７章　例外措置

（例外措置）
第２７条　特別な事情によりこの規則によることができない場合又はこの規則によることが著しく不適当であると認められた場合には、CISOの定めるところにより

審査の上、例外措置を適用することができる。
2　CISOは、例外措置の適用の可否を審査する者（以下「許可権限者」という。）及び審査手続を定めるものとする。
3　部局情報保護管理責任者は、例外措置の適用を要すると認められる場合には、あらかじめ許可権限者に申請するものとする。ただし、緊急を要すると認められる場合は、例外措置の適用後速やかに許可権限者の追認を得なければならない。
4　許可権限者は、前項本文の申請があった場合には、第２項の審査手続に従って審査し、例外措置の適用の可否を決定するものとする。
5　許可権限者は、例外措置の審査状況を台帳に記録し、定期的に全学情報システム・セキュリティ責任者に報告するものとする。
6　全学情報システム・セキュリティ責任者は、例外措置の審査状況を踏まえた情報セキュリティ関係諸規則等の見直しの検討を行い、CISOに報告するものとする。

第８章　雑則

（雑則）
第２８条　この規則に定めるもののほか、情報セキュリティ管理の実施に関し必要な事項は、別に定める。

附 則

この規則は、平成28年10月20日から施行し、平成28年４月１日から適用する。