岡山理科大学情報セキュリティ対策基本規程

（目的）
第1条　本規程は、岡山理科大学（以下「本大学」という。）における情報及び情報システムの情報セキュリティ対策について基本的な事項を定め、もって本大学の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

（適用範囲）
第2条　本規程において適用対象とする者は、本大学情報システムを管理・運用するすべての者、並びに利用者及び臨時利用者とする。
2　本規程において適用対象とする情報を以下に掲げる。
(1) 教職員等が職務上使用することを目的として本大学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）
(2)　その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報
(3)　第1号及び第2号のほか、本大学が調達し、又は開発した情報システムの設計又は管理・運用に関する情報
3　本規程において適用対象とする情報システムは、本規程の適用対象となる情報を取り扱う全ての情報システムとする。

（最高情報セキュリティ責任者）
第3条　本大学における情報セキュリティに関する事柄すべてを統括する最高情報セキュリティ責任者（以下、「CISO」という。）を置く。CISOは学長若しくは副学長をもって充てる。
2　CISOは、次に掲げる事項を統括する。
(1) 情報セキュリティ対策推進のための組織・体制の整備
(2) 情報セキュリティ対策基準の策定、見直し
(3) 対策推進計画の策定、見直し
(4) 情報セキュリティインシデントに対処するために必要な指示その他の措置
(5) 前各号に掲げるもののほか、情報セキュリティに関する重要事項
3　CISOは、全学の情報基盤として供される本大学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。

（情報セキュリティ委員会）
第4条　CISOは、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ委員会を置く。
2　前項の委員会に関して必要な事項は別に定める。

（情報セキュリティ監査責任者）
第5条　情報セキュリティ委員会とは独立に、CISOの指示に基づき行われる情報セキュリティに関わる監査を統括する情報セキュリティ監査責任者1名を置く。

（全学情報セキュリティ対策推進体制）
第6条　CISOは、情報セキュリティ対策推進体制を整備する。
2　CISOは、情報セキュリティ対策推進体制の責任者を定める。
3　CISOは、以下を含む情報セキュリティ対策推進体制の役割を規定する。
(1) 情報セキュリティ関係規程及び対策推進計画の策定に係る業務
(2) 情報セキュリティ関係規程の運用に係る業務
(3) 例外措置に係る業務
(4) 情報セキュリティ対策の教育の実施に係る業務
(5) 情報セキュリティ対策の自己点検に係る業務
(6) 情報セキュリティ関係規程及び対策推進計画の見直しに係る業務

（情報基盤センター長）
第7条　情報基盤センター長は、CISOの命を受け、本大学の情報セキュリティ対策の実施全体に責任を

持ち、CISOを補佐する。
2　情報基盤センター長は、CISOの命を受け、以下に掲げる事項を統括する。
(1) 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定
(2)　情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する業務の取りまとめ
(3) 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備
(4) 例外措置の適用審査記録の台帳整備等
(5) 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等
(6) 前各号に掲げるもののほか、情報セキュリティ対策に係る業務

（情報基盤センター）
第8条　情報基盤センターは本大学の情報セキュリティ対策を統括する部署として、以下に掲げる業務を行う。
(1) 本大学情報セキュリティ委員会の運営に関する業務
(2) 本大学情報システムの運用と利用における情報セキュリティポリシーの実施状況の取りまとめ
(3) 講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
(4) 本大学情報システムのセキュリティに関する連絡と通報
(5) CISO及び部局総括責任者の支援

（部局総括責任者）
第9条　CISOは、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまり（以下、「部局等」という。）に、情報セキュリティ対策に関する事項を統括する者として、部局総括責任者1名を置く。部局総括責任者は、CISOの命を受け、部局等における情報セキュリティ対策を推進するため、次に掲げる事項を統括する。
(1)　部局等を構成する部署に、情報セキュリティ対策の実施に責任を負う情報セキュリティ管理者の配置
(2) 部局等に存在する一つの情報セキュリティ管理単位にその情報セキュリティ対策の実施に責任を負う技術責任者の配置
(3) 部局等に存在する情報システムに情報セキュリティ対策を担当する技術担当者の配置
(4) 情報セキュリティインシデントの原因調査、再発防止策等の実施
(5) 情報セキュリティに係る自己点検計画の策定及び実施手順の整備
(6) 前各号に掲げるもののほか、部局等の情報セキュリティ対策に関する業務

（部局等の情報セキュリティ対策推進体制）
第10条　部局総括責任者は部局内の情報セキュリティ管理者、技術責任者及びその他部局総括責任者が必要と認める者と協力し以下に掲げる事項を実施する。
(1) 部局等における情報セキュリティポリシーの遵守状況の調査と周知徹底
(2) 部局等におけるリスク管理及び非常時行動計画の策定及び実施
(3) 部局等における情報セキュリティインシデントの再発防止策の策定及び実施
(4) 部局等における技術担当者向け教育の計画と企画

（技術責任者）
第11条　教職員等が独自に情報システムを導入する場合、若しくは本大学支給以外の端末で本規程第2条第2項の情報を扱う場合、当該教職員等は技術責任者として当該情報システム及び本大学支給以外の端末における情報セキュリティ対策に関する業務を担う。
2　部局総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する業務の責任者として、当該情報システムに関する技術責任者を、当該情報システムの企画に着手するまでに選任する。
3　技術責任者は、所管する情報システムの管理業務において必要な単位に技術担当者を置くことができる。

（全学情報セキュリティアドバイザー）
第12条　CISOは、情報セキュリティについて専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして置く。
2　全学情報セキュリティアドバイザーは、以下に掲げる業務を行う。
(1) 全学の情報セキュリティ対策の推進に係るCISOへの助言

(2) 情報セキュリティ関係規程の整備に係る助言
(3) 対策推進計画の策定に係る助言
(4) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
(5) 情報セキュリティに係る技術的事項に係る助言
(6)　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
(7) 利用者に対する日常的な相談対応
(8) 情報セキュリティインシデントへの対処の支援
(9) 前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（情報セキュリティインシデント対応体制）
第13条　CISOは、CSIRTを整備し、その役割を明確化する。
2　CISOは、教職員等のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任する。選任した者のうち、本大学における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置く。また、CSIRT内の業務統括及び外部との連携等を行う教職員等を定める。
3　CISOは、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。
4　CISOは、以下を含むCSIRTの役割を規定する。
(1)　本大学に関わる情報セキュリティインシデント発生時の対処の一元管理
ア　全学における情報セキュリティインシデント対処の管理
イ　情報セキュリティインシデントの可能性の報告受付
ウ　本大学における情報セキュリティインシデントに関する情報の集約
エ　情報セキュリティインシデントのCISO等への報告
オ　情報セキュリティインシデントへの対処に関する指示系統の一本化
(2)　情報セキュリティインシデントへの迅速かつ的確な対処
ア　情報セキュリティインシデントであるかの評価
イ　被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
ウ　文部科学省への連絡
エ　外部専門機関等からの情報セキュリティインシデントに係る情報の収集
オ　他の機関等との情報セキュリティインシデントに係る情報の共有
カ　情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施
5　CISOは、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築する。
6　CISOは、全学における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定する。

（兼務を禁止する役割）
第14条　教職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しない。
(1) 承認又は許可（以下、「承認等」という。）の申請者と当該承認等を行う者
(2) 監査を受ける者とその監査を実施する者

（対策基準の策定）
第15条　CISOは、本大学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえ、情報セキュリティ委員会における審議を経て、サイバーセキュリティ戦略本部決定「政府機関等の情報セキュリティ対策のための統一基準」に準拠する対策基準を定める。

（改廃）
第16条　本規程の改廃は、大学協議会の審議を経て、学長が決定する。

附　則（令和4年7月27日　第4回大学協議会）
この規程は、令和4年7月27日から施行する。