○学校法人専修大学情報セキュリティ対策に関する規程

令和３年４月１日
制定

目次

第１章　総則

（目的）

第１条　この規程は、学校法人専修大学（以下「本法人」という。）における情報セキュリティ対策に関し基本的な事項を定めることにより、本法人が保有する情報資産の機密性、完全性及び可用性を維持することを目的とする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　ネットワーク　コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

(2)　情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3)　電磁的記録媒体　フロッピーディスク、CD―ROM、USBメモリ等の可搬記憶媒体並びにコンピュータ及びサーバのハードディスク、メモリ等をいう。

(4)　情報資産　情報及び情報システムをいう。

(5)　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維持することをいう。

(6)　情報セキュリティポリシー　この規程及び学校法人専修大学情報セキュリティ対策基準をいう。

(7)　機密性　情報にアクセスすることを認められた者だけが情報にアクセスすることができる状態を確保することをいう。

(8)　完全性　情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

(9)　可用性　情報にアクセスすることを認められた者が必要なときに中断されることなく情報にアクセスすることができる状態を確保することをいう。

(10)　インシデント　情報漏えい等により、管理情報、管理資料又は情報システムの機密性、完全性又は可用性を低下させ、又は喪失することをいう。

(11)　教職員　本法人に雇用されている全ての教員及び職員をいう。

(12)　外部委託事業者　本法人と合意した業務内容を実施する独立した外部組織をいう。

(13)　システム利用者　次に掲げる者をいう。

ア　教職員

イ　学生

ウ　本法人の情報システム又はネットワークを利用する個人及び団体

エ　本法人の情報システム又はネットワークを利用する外部委託事業者

(14)　情報利用者　次に掲げる者（システム利用者を除く。）で、本法人の承認を得てその情報を利用するものをいう。

ア　本法人の業務遂行に協力する個人及び団体

イ　外部委託事業者

（対象とする脅威）

第３条　この規程は、次に掲げる脅威を対象とする。

(1)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃及び部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん及び消去並びに重要情報の詐取、内部不正等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用等、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・

外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥及び機器故障等の非意図的要因による情報資産の漏えい、破壊、消去等

(3)　地震、落雷、火災その他の災害によるサービス及び業務の停止等

(4)　大規模かつ広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5)　電力供給、通信及び水道供給の途絶その他のインフラの障害による機能不全等

（適用範囲）

第４条　この規程は、本法人の情報資産を運用し、管理し、又は利用する全ての者に適用する。

２　この規程を適用する情報資産の範囲は、次のとおりとする。

(1)　本法人が管理するネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

(2)　システム利用者が管理する情報システムで本法人が管理するネットワークに接続するもの

(3)　本法人の業務又は教育研究に関するデータ及びこれらが保存されているもの（これらを記録し、又は印刷した文書を含む。）

(4)　本法人が管理するネットワーク及び情報システムの仕様書、ネットワーク図等のシステム関連文書

(5)　前各号に掲げる範囲に準ずる情報資産

第２章　システム利用者の遵守義務

第５条　システム利用者は、情報セキュリティの重要性についての共通認識を持ち、情報資産の利用に当たっては、法令及び情報セキュリティポリシーを遵守しなければならない。

２　システム利用者は、システム利用者であることにより知り得た秘密を漏らしてはならない。システム利用者でなくなった後も、同様とする。

第３章　情報セキュリティ組織

（情報セキュリティ体制）

第６条　本法人の情報セキュリティ体制は、別表に定めるとおりとする。

（最高情報セキュリティ責任者）

第７条　本法人の情報セキュリティマネジメントを総合的に実施するため、情報セキュリティ対策に責任を持つ者として、最高情報セキュリティ責任者（以

下「最高責任者」という。）を置く。

２　最高責任者は、理事長をもって充てる。

３　最高責任者は、次に掲げる事項についての実施責任を負うものとする。

(1)　情報セキュリティマネジメントの実施状況の把握

(2)　情報セキュリティポリシーの承認

(3)　理事会における情報セキュリティに関する年間報告の実施

(4)　情報セキュリティ委員会委員長の指名

(5)　情報セキュリティ監査責任者の指名

(6)　インシデント発生時の対応体制の構築及び対応状況の把握

(7)　情報セキュリティに関する年間報告書の作成指示及び承認

(8)　情報セキュリティ対策に関する改善指示

(9)　前各号に掲げる事項に準ずる情報セキュリティ対策に関する事項

４　最高責任者に事故があるときは、最高責任者があらかじめ指名する情報セキュリティ実施責任者がその職務を代行する。

（情報セキュリティ実施責任者）

第８条　最高責任者を補佐する者として、情報セキュリティ実施責任者（以下「実施責任者」という。）を置く。

２　実施責任者は、専修大学にあっては専修大学長及び情報システム担当理事、石巻専修大学にあっては石巻専修大学長及び石巻専修大学担当理事をもって充てる。

３　実施責任者は、次に掲げる事項についての実施責任を負うものとする。

(1)　情報セキュリティポリシーの定着に向けた実行管理

(2)　情報セキュリティ年間計画の実施

(3)　情報セキュリティにおけるリスク管理の実施

(4)　情報セキュリティ監査結果に基づく改善指示及び自己点検の実行管理

(5)　情報セキュリティ教育・啓発の実行管理

(6)　前各号に掲げる事項に準ずる情報セキュリティ対策に関する事項

４　実施責任者は、前項各号の実施状況を最高責任者に報告するものとする。

（部局情報セキュリティ責任者）

第９条　部局における情報セキュリティマネジメントを実施する責任を負う者として、各部局に、部局情報セキュリティ責任者（以下「部局責任者」という。）を置く。

２　教育研究組織における部局責任者は、各教育研究組織の長をもって充てる。
３　事務組織における部局責任者は、各所管長をもって充てる。
４　部局責任者は、次に掲げる事項についての実施責任を負うものとする。
(1)　情報セキュリティポリシーの定着に向けた推進活動の実施
(2)　情報セキュリティ監査及び自己点検への対応
(3)　情報セキュリティ教育・啓発の実行及びその効果の測定
(4)　前３号に掲げる事項に準ずる情報セキュリティ対策に関する事項
５　部局責任者は、必要に応じて、情報セキュリティ委員会に出席し、本法人の情報セキュリティ対策について意見を述べることができる。

（情報セキュリティ管理者）

第10条　部局責任者を補佐する者として、各部局に、情報セキュリティ管理者（以下「管理者」という。）を置く。
２　教育研究組織における管理者は、各教育研究組織の長が当該教育研究組織の教員のうちから指名する。
３　事務組織における管理者は、各所管長が当該所管の課長のうちから指名する。
４　管理者は、部局責任者の指示の下、各部局の情報セキュリティに関する実務を担うものとする。

（情報セキュリティ委員会）

第11条　本法人における情報セキュリティ対策について審議する機関として、情報セキュリティ委員会（以下「委員会」という。）を置く。
２　委員会は、次に掲げる者をもって構成する。
(1)　委員長（最高責任者が指名する者）
(2)　専修大学情報科学センター長
(3)　専修大学事務計算センター長
(4)　専修大学の各学部の教授会から選出された者　各１名
(5)　専修大学法科大学院教授会から選出された者　１名
(6)　石巻専修大学情報教育研究センター長
(7)　学校法人専修大学個人情報保護委員会委員長
(8)　石巻専修大学事務部長
(9)　本法人の専任職員のうちから最高責任者が指名する者　若干名
(10)　前各号に掲げる者のほか、委員長が必要と認める者

３　委員長の任期は、２年とし、再任を妨げない。ただし、連続して３期を超えることはできない。
４　第２項第４号、第５号、第９号及び第10号の委員の任期は、２年とする。ただし、再任を妨げない。
５　第２項第２号、第３号、第６号、第７号及び第８号の委員の任期は、当該職にある期間とする。
６　委員会は、必要に応じて、委員以外の者の出席を求め、その意見を聴くことができる。
７　委員会は、次に掲げる事項について審議する。
(1)　情報セキュリティポリシーに関する事項
(2)　情報セキュリティ年間計画に関する事項
(3)　情報セキュリティにおけるリスク管理に関する事項
(4)　情報セキュリティ監査及び自己点検に関する事項
(5)　情報セキュリティ教育・啓発に関する事項
(6)　情報セキュリティに係る年間報告書に関する事項
(7)　前各号に掲げるもののほか、情報セキュリティ対策に関する事項
８　委員会の運営に関し必要な事項は、別に定める。

（情報セキュリティ委員会事務局）

第12条　委員会の事務を担う組織として、情報システム部情報システム課に、情報セキュリティ委員会事務局（以下「事務局」という。）を置く。
２　事務局は、最高責任者及び実施責任者と連携して、本法人の情報セキュリティに関する施策案を作成し、及び検討する。
３　事務局は、委員会で審議する事項の素案を作成する。

（情報セキュリティ監査責任者）

第13条　情報セキュリティマネジメントを監査する者として、情報セキュリティ監査責任者（以下「監査責任者」という。）を置く。
２　監査責任者は、理事長が指名する。
３　監査責任者は、次に掲げる事項についての実施責任を負うものとする。
(1)　情報セキュリティ監査計画の策定
(2)　情報セキュリティ監査の実施
(3)　情報セキュリティ監査結果の最高責任者への報告

第４章　情報セキュリティ対策

第１節　情報資産の分類等

第14条　本法人は、取り扱う情報資産を重要度の観点から格付けし、それに応じた情報資産の分類に基づき情報セキュリティ対策を行うものとする。

第２節　個別情報セキュリティ対策

（物理的な情報セキュリティ対策）

第15条　本法人は、サーバ等、情報システム室等、通信回線等及び教職員のコンピュータ等の管理について、物理的な情報セキュリティ対策を講ずるものとする。

（人的な情報セキュリティ対策）

第16条　本法人は、情報セキュリティに関し遵守すべき事項を定めるとともに、システム利用者に対しては十分な教育・啓発を、情報利用者に対しては必要に応じて啓発を行う等の人的な情報セキュリティ対策を講ずるものとする。

（技術的な情報セキュリティ対策）

第17条　本法人は、コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的な情報セキュリティ対策を講ずるものとする。

（運用面での情報セキュリティ対策）

第18条　本法人は、情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際の情報セキュリティ確保等の情報セキュリティポリシーの運用面での情報セキュリティ対策を講ずるものとする。

第３節　外部サービスを利用する際の措置

第19条　本法人は、業務を外部委託する場合は、情報セキュリティ要件を明記した契約を締結するものとする。この場合において、委託先に十分な情報セキュリティ対策が確保されていることを確認し、必要に応じて、適切な措置を講ずることを求めるものとする。

２　本法人は、ソーシャルメディアその他の外部サービスを利用する場合の規定、運用手順等を整備し、対策を講じておくものとする。

第４節　情報セキュリティ対策に関する基準等の策定

（情報セキュリティ対策に関する基準の策定）

第20条　本法人は、情報セキュリティ対策における具体的な遵守事項、判断基準等を含む学校法人専修大学情報セキュリティ対策基準を策定するものとする。

（情報セキュリティ対策に関する実施手順の策定）

第21条　本法人は、学校法人専修大学情報セキュリティ対策基準に基づき、具体的な手順を含む情報セキュリティ実施手順（ハンドブック）を策定するものとする。

第５節　インシデントへの対応

第22条　本法人は、インシデント発生時は、その被害を最小限に抑えるため、直ちに、必要な措置を講ずるものとする。

２　本法人は、インシデント発生時等に迅速かつ適正に対応するため、あらかじめ、緊急時対応計画を策定するものとする。

３　最高責任者は、インシデント発生時は、その対応体制を構築し、及び対応状況を把握するとともに、事務局に対して必要な指示を行うものとする。

４　事務局は、インシデント発生時は、最高責任者の指示の下、情報収集、インシデント対応処理並びに関係者への緊急連絡及び周知を行うものとする。

５　実施責任者、部局責任者及び管理者並びに委員会は、インシデント発生時は、事務局と連携し、必要に応じて、その対応を行うものとする。

第５章　情報セキュリティ教育・啓発

第23条　本法人は、情報セキュリティポリシーの周知徹底を図るため、情報セキュリティについて、システム利用者に対しては定期的に教育・啓発を、情報利用者に対しては必要に応じて啓発を行うものとする。

第６章　情報セキュリティに関する評価及び見直し

（情報セキュリティ監査及び自己点検の実施）

第24条　本法人は、情報セキュリティポリシーの遵守状況を検証するため、毎年度及び必要に応じて、情報セキュリティ監査及び自己点検を行うものとする。

（情報セキュリティポリシーの見直し）

第25条　本法人は、次に掲げる場合は、情報セキュリティポリシーを見直すものとする。

(1)　情報セキュリティ監査又は自己点検の結果、情報セキュリティポリシーの改善が必要となった場合

(2)　情報セキュリティに関する状況の変化に対応するため、新たな対策が必要となった場合

第７章　雑則

（事務所管）

第26条　この規程に関する事務は、情報システム部情報システム課の所管とする。

（規程の改廃）

第27条　この規程の改廃は、委員会及び常勤役員会の議を経て理事長が行う。

附　則

この規程は、令和３年４月１日から施行する。

別表（第６条関係）

情報セキュリティ体制