東北公益文科大学情報セキュリティポリシー

制定　令和４年４月 20 日

１．基本方針

東北公益文科大学（以下「本学」という。）が保有・管理する全ての情報資産は、本学の運営において非常に重要な資産である。

この情報資産が外部に漏えいするなどした場合、本学の教育研究活動の停滞や社会的信用の失墜などといった、極めて重大な事態と被害を招くこととなる。

このような事態を未然に防ぐため、本学に所属する教職員及び学生、又、本学の委託業者等の関係者（以下「本学関係者」という。）は不断の努力をもって、情報資産を保全しなければならない。また、本学の情報資産を利用する者は、本情報セキュリティポリシー（以下「本ポリシー」という。）を遵守するとともに、情報資産に対する権限のないアクセスや複写、改ざん、破壊又は遺漏等をしてはならない。

２．定　義

（１）　情報システム

情報の作成、利用及び管理のための仕組みで、ハードウェア及びソフトウェアからなる情報機器並びに情報ネットワーク等をいう。

（２）　情報資産

情報システムに記録された情報及び情報システムに関係する書面に記載された情報をいう。

（３）　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。

① 機密性　　アクセスを許可された者だけが情報資産にアクセスできることを確実にすること

② 完全性　　情報資産及び処理方法が正確であること及び完全であることを保護すること

③ 可用性　　許可された利用者が必要なときに、情報資産にアクセスできることを確実にすること

３．目　標

本ポリシーにおいて、本学における情報セキュリティの方針を示すとともに、次に掲げる事項を目指すこととする。

（１）　本学の情報セキュリティに対する侵害の阻止

（２）　本学内外の情報セキュリティを侵害する行為の抑止

（３）　情報資産の分類と管理の徹底

（４）　情報セキュリティに関する情報の取得に係る支援

４． 組織・体制

本学における情報セキュリティに関しての管理体制を整備するため、情報セキュリティの権限及び責任を有する「最高情報セキュリティ責任者」を置くものとし、学長をもって充てる。

また、最高情報セキュリティ責任者を補佐し、各部署における情報管理の実施及び緊急時の対応にあたるため、「情報セキュリティ管理者」を置くものとし、学部長をもって充てる。

情報セキュリティに関する会議の開催にあたっては、最高情報セキュリティ責任者が必要とする者の出席を求め、開催することとする。

なお、情報セキュリティの実行に関する対策及び諸対応基盤情報ネットワークシステム等に支障を及ぼす恐れのある情報セキュリティインシデントに迅速に対応するため、東北公益文科大学インフォメーションマネジメントセンター運営委員会(以下「IMC 運営委員会」という。)に情報セキュリティ部会を置くものとする。

５． 保護すべき財産及び権利

情報ネットワーク及び情報システム等の資源を適正な利用により保護するため、情報セキュリティを実現するための体制整備及びシステムの監視など、適切な対策を行うものとする。

ただし、私的利用により生じた損失や障害についての責任を負わない。

６．情報セキュリティの侵害行為の防止

本学は不正アクセスを常時高い確率で感知できる監視システムを構築するとともに、不正アクセスを検出した場合には、適時適切に対策を講じることとする。

本学関係者は、あらゆる教育・研究機関、企業、公共団体等の組織、個人等の情報資産を侵害してはならない。また、本ポリシーの他、情報セキュリティに関連する法令、知的財産権に関連する法令、個人情報の保護に関連する法令及び情報セキュリティに関連する諸規程等を遵守しなければならない。

７．違反行為に係る対応

本ポリシー及び関連法令等に違反した教職員が故意又は重大な過失により本学に損害を与えた場合は、学校法人東北公益文科大学就業規則等の規定により処分する場合がある。

また、本ポリシー及び関連法令等に違反した学生に対しては、学則等により処分する場合がある。

８．事故等に係る対応

情報セキュリティに関連する重大な事故等に対しては、最高情報セキュリティ責

任者及び情報セキュリティ管理者により、迅速に対策を講じることとするとともに、再発防止に係る対策に取組むこととする。

９．情報資産に対する事故(情報セキュリティインシデント)に係る対応

情報セキュリティインシデントの発生が確認された場合は、情報セキュリティ管理者の指示により、IMC 運営委員会情報セキュリティ部会が中心となり、全学的に対応するものとする。

10．情報の分類と管理

情報資産について、IMC 運営委員会情報セキュリティ部会において、その内容に応じて分類し、その重要度に応じた情報セキュリティ対策を講じることとする。

また、情報の漏洩を防止するため、情報機器及び記録媒体の交換、破棄、持ち込み及び持ち出しには適切な処置を講じるとともに、コンピュータウイルス等の悪意的なソフトウェアを検出した場合についても、適時適切に処置を講じるものとする。

11．情報セキュリティ対策の実行

本ポリシーに基づき、物理的、人的及び技術的な対策の実施手順を定め、実行するものとする。

なお、実施手順については、情報セキュリティ管理者の指示により、IMC 運営委員会情報セキュリティ部会が中心となり、取りまとめるものとする。

附　則

本ポリシーは、令和４年５月１日から施行する。