セキュリティポリシー基本方針

１．目的

人間総合科学大学（以下「本学」という。）における教育・研究活動及び業務には、情報基盤の充実に加え、情報資産のセキュリティ確保が不可欠である。

そのため、必要な方針を明文化した人間総合科学大学情報セキュリティポリシー（以下、「ポリシー」という。）を定め、情報管理体制を構築するものとする。

本ポリシーが目指すものは次のとおりである。

（1）不正アクセス、改ざん、漏洩等から本学の情報資産を守り、情報セキュリティを確保すること。

（2）学内外の情報セキュリティを損ねる加害行為を防止し、本学の社会的信頼を保つこと。

（3）本学内におけるセキュリティ侵害等の早期検出と迅速な対応の実現すること。

２．ポリシーの構成と位置付け

本ポリシーは、本学の情報セキュリティに関する方針を総合的に取りまとめたものである。

３．ポリシーの対象範囲

本ポリシーが対象とする対象者及び対象物は以下のとおりである。

・3-1. 対象者

本学の情報資産にアクセスする全ての者とする。

・3-2. 対象物

（１）本学の情報資産のみならず、本学以外の情報システムであっても、本学のネットワークに一時的に接続されたものまでを含む。

（２）本学のネットワークに接続されていない状態であっても、本学の情報資産を保持している情報システムについては、その適用範囲に含む。

４．ポリシー遵守義務

ポリシーの対象範囲に定める対象者は、本学の所有する情報資産に関わる業務において、情報セキュリティの重要性について共通の認識を持つとともに業務の遂行に当たって基本方針を遵守するものとする。

また、役員・職員は、学生及びその他本学保有の情報資産に対するアクセスを認められている者に、これを遵守させる義務を負うものとする。

５．組織・体制

本学の情報資産を守るため、本学に最高情報セキュリティ責任者（CISO）を置くこととする。

最高情報セキュリティ責任者は、本学の情報セキュリティに関する統括的な意思決定と学園内外に対する責任を負うとともに、組織全体として体制を確立し、情報セキュリティの管理を実施する。

６．情報セキュリティ対策

本学の情報資産を保護するために、以下の情報セキュリティ対策を講じる。これらの対策は、対策基準に定め運用に当たる。

・6-1．物理的セキュリティ対策

情報システムの設置場所について、安全性を保ち、不正な立ち入りを阻止する対策を講じる。また、持ち運びを前提とした情報システムの情報資産を保護するための対策にも十分に配慮する。

・6-2．人的セキュリティ対策

組織・体制で定める責任者や担当者及び利用者としての役割及び責任を明確にし、全ての対象者に対して、ポリシーの内容を周知徹底させるために必要な対策を行う。

・6-3. 技術的セキュリティ対策

本学の情報資産を学外又は学内からの不正アクセスなどから適切に保護するため、情報資産へのアクセス制限、ネットワーク管理などの必要な対策を講じる。

・6-4. 運用対策

（1）ポリシーの遵守状況の確認、ネットワークの管理などの運用面に関して必要な措置を講じる。

（2）緊急事態が発生した場合の迅速な対応を可能とするため、緊急時の対応計画を定める。

また、情報資産への侵害あるいは本学外の情報資産に対する侵害が発生した際の対応手順を定める。

7． 情報セキュリティ監査及び評価・見直しの実施

・7-1. 監査

最高情報セキュリティ責任者は、各部局等の情報セキュリティがポリシーに沿って実施されているかを検証するために、計画的に監査を実施する。

・7-2. 評価及び見直し

最高情報セキュリティ責任者は、情報セキュリティ監査の結果について評価を実施する。

また、情報セキュリティを取り巻く状況の変化に鑑み、ポリシーに定める事項の見直しを実施する。

8．教育・研修

最高情報セキュリティ責任者は、ポリシーの周知と遵守のために、対象者に対してセキュリティ説明会等の教育・研修を実施する。

9．法令遵守の義務

ポリシー適用対象者は、ポリシーを遵守するとともに関連する法令等を遵守し、これに従わなければならない。

１０．罰則

ポリシー適用対象者は、故意又は重大な過失により著しくポリシーの遵守事項の違反行為に該当する場合は、本学規則や契約書の定めにより措置される。