群馬パース大学 情報セキュリティポリシー

（目　的）

第１条　群馬パース大学（以下、「本学」という。）が学術研究活動、教育活動、社会貢献活動及び業務運営等を安定的かつ効率的に展開するためには、電子情報が持つ情報セキュリティ上の脆弱性を十分認識し、情報セキュリティを確保するとともに、それを実行するための情報システムの整備が不可欠である。
本学においては、教職員等が情報システム及び情報セキュリティの重要性を認識し、教育研究組織の自治を尊重しつつ情報資産の円滑な運用に取り組むものとする。
よって、群馬パース大学情報セキュリティポリシー（以下、「本ポリシー」という。）及び下位規程を定め、情報セキュリティの維持向上に関する事項を整備し、情報資産の保護と活用を図ることを目的とする。

（方　針）

第２条　前条の目的を達するため、以下の施策を講ずることができる。

（１）情報セキュリティを確保、維持、向上するための組織体制の整備
（２）情報資産の保護対策
（３）インシデントへの対処
（４）ネットワーク環境の設計・整備、利用情報の取得
（５）クラウド環境の利用状況の整備、利用情報の取得
（６）外部記憶媒体の利用状況の整備、利用情報の取得
（USB メモリー・SD カード・DVD・外付 HDD 等）
（７）監査等による実施状況の確認、それに伴う本ポリシー及び下位規程の改廃

（対　象）

第３条　本ポリシーは、以下に掲げる情報資産を対象とする。

（１）本学が所有又は管理する情報システム
（ファイルサーバー、学務サーバー、ネットワーク通信機器 等）
（２）情報システムに接続された情報機器で、前号に該当しないもの
（PC、タブレット、スマートフォン 等）
（３）本学との契約又は協定に基づき提供される情報システム
（ウェブサーバー、メールサーバー 等）
（４）業務遂行又は教育研究のために、情報システム又は情報機器に記憶させた各種ファイル（通信情報(ログ)等を含む）及びそのファイルを印刷した書面。

（適　用）

第４条　本ポリシーは、本学における情報資産を利用（管理、運用も含む。以下同様。）する教職員及び臨時利用者に適用するものとする。

２　本学が有する情報資産の利用に関する禁止事項等については、本ポリシー及び下位規程を適用するが、当該法律及びそれに基づく命令の定めるところがあれば、そちらを優先する。

（体　制）

第５条　本ポリシーを順守し正しく実施するため、以下の役職を設置することができる。情報セキュリティ責任者以外の者は、適任者であれば学外から選任することもできる。また、兼務を許可するが、複数人で構成されることを前提とする。

（１）情報セキュリティ責任者及び実施責任者
　　大学協議会において学長が選任する。

（２）情報セキュリティ監査責任者及び監査実施者
　　情報セキュリティ責任者が推薦し、学長がこれを承認する。

（３）情報セキュリティ技術責任者及び技術担当者
　　情報セキュリティ責任者が推薦し、学長がこれを承認する。

（４）情報セキュリティアドバイザー
　　情報セキュリティ責任者が推薦し、学長がこれを承認する。

（情報システム委員会）

第６条　本学の情報セキュリティに関し、次の各号に掲げる事項について審議するため、情報システム委員会を置くことができる。

２　委員会に関する事項は、別に定める。

（インシデント対応チーム）

第７条　インシデントの発生時に迅速かつ円滑な対処を実施するため、情報システム委員会の下にインシデント対応チーム（以下「対応チーム」という。）を置くことができる。

２　対応チームは、インシデントの発生時に情報セキュリティ責任者により招集される。

３　対応チームは、次の各号に掲げる委員で組織する。

（１）情報セキュリティ責任者及び実施責任者

（２）情報セキュリティ技術責任者及び技術担当者

（３）その他情報セキュリティ責任者が指名する者

（情報セキュリティ対策教育）

第８条　情報セキュリティ責任者は、情報セキュリティ技術責任者（以下、「技術責任者」という。）に対し、利用者に対する情報セキュリティ対策教育（以下、「対策教育」という。）の実施を指示することができる。

2　技術責任者は、教育計画を策定し、情報セキュリティ責任者の承認を得て、立案された教育計画に基づき関係者を招集し、対策教育を実施するものとする。

3　対策教育を実施した際、技術責任者は、実施報告書を作成し、情報セキュリティ責任者に報告するものとする。

4　対策教育は、年１回以上実施するものとする。

（監　査）

第９条　情報セキュリティ責任者は、情報セキュリティ監査責任者（以下、「監査責任者」という。）に対し、監査の実施を指示することができる。

2　監査責任者は、実施計画を立案し、情報セキュリティ責任者の承認を得て、立案された監査計画に基づき関係者を招集し、監査を実施するものとする。

3　監査を実施した際、監査責任者は、監査報告書を作成し、情報セキュリティ責任者に報告するものとする。

4　情報セキュリティ責任者は、監査報告書にて対処の必要がある事象を認めた場合、情報システム委員会に諮り、対策を策定し、当該部署の責任者へ伝達し、当該部署にて対策を実施させることができるものとする。

5　当該部署の責任者は、伝達された対策を実施し、対策の効果を情報セキュリティ責任者に報告するものとする。

6　監査は、年１回以上実施するものとする。

（罰　則）

第 10 条　本ポリシー及び下部規程に定められた事項に違反した場合の罰則は、本学が定める就業規則に則って行うほか、別に定めるところによるものとする。

（改　廃）

第 11 条　このポリシーの改廃は、大学協議会の議を経て、学長がこれを行う。

（用語の定義）

（１）情報資産
「対象範囲」に記された本学所有の資産をいう。
契約先の情報システムに蓄えられている「電磁的記録」も含む。

（２）情報セキュリティ
前号に定め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いう。

（３）情報システム
情報の作成、利用及び管理等のための仕組み（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有線又は無線のネットワーク）をいう。

（４）インシデント
情報セキュリティに関し、意図的又は偶発的に生じる、本学の諸規程又

は法律に違反する事件若しくは事故をいう。

※事件(ミス)：事象は認知されたが、損害を与えなかった事案

※事故(アクシデント)：事象を認知し、損害が生じた事案

（５）電磁的記録

電子的方式、磁気的方式、その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。

（６）臨時利用者

教職員及び学生以外の者で、許可を得て本学の情報システムを利用する者をいう。

附　則　このポリシーは、2019 年 4 月 1 日から施行する。