

学校法人比治山学園情報セキュリティ対策に関する規程（大学等の部）

第1章 総則

（目的）

第1条 この規程は、比治山大学、比治山大学大学院、比治山大学短期大学部及び比治山大学短期大学部附属幼稚園（以下「本学」という。）における学校法人比治山学園情報セキュリティ基本方針（大学等の部）（以下「基本方針」という。）に則り、情報セキュリティの維持及び向上に関する事項を定めることにより、本学の有する情報資産の保護と活用を図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、当該各号に定めるところによる。

- (1) 情報セキュリティ 次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。
- (2) 情報資産 情報の内容並びにその作成、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。）をいう。ただし、別に定める場合を除き、情報資産は、電磁的なものに限る。
- (3) 情報セキュリティポリシー この規程の他、本学における情報セキュリティに関する次のものをいう。
 - ①基本方針
 - ②情報セキュリティ対策基準（以下「対策基準」という。）
 - ③情報セキュリティ実施手順（以下「実施手順」という。）
- (4) 教職員 本学に勤務する常勤又は非常勤の教職員をいう。

（責務）

第3条 学長は、この規程の目的を達成するため、情報セキュリティ対策に関し必要な措置を講じなければならない。

- 2 教職員は、基本方針、この規程、対策基準及び実施手順を遵守して、その取扱いに係る個々の情報システム及び情報機器を適切に維持・管理し、情報セキュリティの適正な運用に努めなければならない。

- 3 教職員は、新任の教職員及び学生等に対し、情報セキュリティポリシーを周知し、適切な教育をしなければならない。

(対象範囲)

第4条 情報セキュリティポリシーは、次の各号に規定する情報資産を対象とする。

- (1) 本学が管理する情報機器及びネットワーク
- (2) 前号に規定する情報資産に接続された情報機器
- (3) 前号又は第1号に規定する情報資産を利用する者が、本学の教育、研究その他業務のために作成又は取得した情報で、前号又は第1号に規定する情報機器に記憶させたもの

第2章 組織体制

(総括情報セキュリティ責任者)

第5条 学長を補佐し、情報セキュリティに関する業務を総括的に管理・執行するため、総括情報セキュリティ責任者（以下「総括責任者」という。）を置く。

- 2 総括責任者は、副学長（経営企画担当）をもって充てる。

(情報セキュリティ責任者)

第6条 本学に情報セキュリティ責任者（以下「セキュリティ責任者」という。）を置き、学部長、短大部長、幼稚園長、大学事務局長及び情報センター長をもって充てる。

- 2 セキュリティ責任者は、各部署における学内ネットワークに接続される情報システム及び情報機器のセキュリティに関する権限と責任を有する。
- 3 セキュリティ責任者のうち、学内ネットワークに係わる責任者をシステムセキュリティ責任者といい、情報センター長をもって充てる。

(システム管理者)

第7条 本学にシステム管理者を置き、別表に定める各システム管理者は管理対象範囲の情報システム及び情報機器等を維持・管理する。

(情報セキュリティ委員会)

第8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、情報セキュリティ委員会（以下「委員会」という。）を置く。

- (1) 情報セキュリティ対策の基本方針等に関すること。
- (2) 情報セキュリティポリシーの実施状況に係る点検に関すること。

- (3) 対策基準の改定に関すること。
 - (4) 情報セキュリティの維持及び向上のための措置に関すること。
 - (5) その他情報セキュリティに関すること。
- 2 委員会は、総括責任者、セキュリティ責任者及び比治山大学情報センター運営委員会委員で組織する。
 - 3 委員会に委員長を置き、総括責任者をもって充てる。
 - 4 委員長が不在のときは、委員長があらかじめ指名する者が、その職務を行う。
 - 5 委員会は、委員長が招集し、委員の過半数をもって定足数とする。
 - 6 委員会は、必要があると認めるときは、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。

第3章 情報セキュリティ対策

(情報資産の分類及び管理)

第9条 総括責任者は、第4条に規定する情報資産に対してリスク分析を行い、その結果に基づいた適切な分類と管理を実施しなければならない。

- 2 前項の規定の適用に関し必要な事項は、対策基準で定める。

(セキュリティ侵害への対処)

第10条 本学に対するセキュリティ侵害への対処に関し必要な事項は、対策基準で定める。

(ネットワークの監視)

第11条 第4条第1号のネットワークを利用する者は、ネットワークを通じて行われる通信を傍受してはならない。ただし、総括責任者は、セキュリティ確保のために、あらかじめ指名した者に、ネットワークを通じて行われる通信の監視(以下「監視」という。)を行わせることができる。

- 2 前項の監視の範囲及び手続は、対策基準で定める。
- 3 第1項の指名を受けた者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。ただし、本学又は学外に対する重大なセキュリティ侵害を防止するために必要と認められる場合は、対策基準の定めるところにより、監視を行わせる者及び対策基準で特に定める者に伝達することができる。
- 4 第1項に規定する監視によって採取した記録の取扱いその他必要な事項は、対策基準

で定める。

(利用の記録)

第12条 情報機器の利用記録(以下「利用記録」という。)の採取及び取扱いについては、対策基準で定める。

(点検)

第13条 委員会は、情報セキュリティポリシーの実施状況に係る点検を情報センターに行わせ、情報センターは、その結果を委員会に報告するものとする。

(ポリシーの更新)

第14条 委員会は、前条の点検の結果及び本学におけるセキュリティ侵害を勘案し、定期的に情報セキュリティポリシーの更新を審議するものとする。ただし、実施手順の更新は、情報センターに行わせる。

第4章 雑則

(事務)

第15条 情報セキュリティ対策に関する事務は、情報システム室において処理する。

(その他)

第16条 この規程に定めるもののほか、本学の情報セキュリティの維持及び向上に関し必要な事項は、対策基準において定める。

附 則 (平成19年2月23日制定)

この規程は、平成19年2月23日から施行する。

別表（第7条関係）

システム管理者及び管理の対象範囲

システム管理者	管理の対象範囲
情報センター長	学内ネットワーク
学科主任	各学科に係る業務システム
情報システム室長	学務システム
室長（主監を含む。）・課長	各室に係る業務システム
教員	研究室内の端末等情報機器
職員	事務所内の端末等情報機器