

学校法人比治山学園情報セキュリティ基本規程

第1章 総 則

(目的)

第1条 この規程は、学校法人比治山学園情報セキュリティ基本方針」(以下「基本方針」という。)第4条に基づき、情報セキュリティ対策に必要な基本的事項を定めることにより、学校法人比治山学園(以下「学園」という。)の保有又は利用する全ての情報資産を安全に管理し運用するとともに、適切な情報セキュリティ水準の維持・向上を図ることを目的とする。

第2章 情報セキュリティの管理体制

(組織・体制)

第2条 学園における情報セキュリティに関する事業を遂行するための組織・体制を、次のとおり定める。

(1) 情報セキュリティ統括責任者

学園に情報セキュリティ統括責任者を置き、専務理事をもって充てる。情報セキュリティ統括責任者は、学園の情報セキュリティに関する事業を統括する。

(2) 情報セキュリティ代表責任者

学園に情報セキュリティ代表責任者を置き、学長、校長、園長、法人事務局長をもって充てる。情報セキュリティ代表責任者は、学園各部門の情報セキュリティ対策の実施に関し統括する。

(3) 情報セキュリティ実施責任者

学園に情報セキュリティ実施責任者を置き、図書・情報メディア課長をもって充てる。情報セキュリティ実施責任者は、学園全体の情報セキュリティ対策の実施に関し総括し、情報セキュリティ代表責任者と連携して、情報セキュリティ統括責任者を補佐する。

(4) 情報セキュリティ部局責任者

大学・短期大学部の各学部・各学科、各センター、大学事務局の各部署、中高、幼稚園、法人事務局の各部署に情報セキュリティ部局責任者を置く。情報セキュリティ部局責任者は、各部局内の情報セキュリティ対策を実施する。情報セキュリティ部局責任者は、その業務を補佐するために、部局構成員より「情報セキュリティ担当者」を選定することができる。具体的な部局責任者の配置は別途定める。

(会 議)

第3条 情報セキュリティ対策の推進に関する必要事項を審議するため、「学校法人比治山学園情報セキュリティ対策推進会議」(以下「セキュリティ会議」)を置く。

2 セキュリティ会議に関する事項は、別途定める。

第3章 情報資産の分類と管理

(情報資産の分類)

第4条 情報資産は、基本方針で定義されている「情報セキュリティ」における「機密性」及び「完全性」並びに「可用性」の確保の3つの観点に基づき、学園の情報資産を以下の2種類に分類する。

- (1) 第一種情報資産：学園の情報セキュリティが侵害され、情報の漏洩及び破壊や改竄が生じたり、情報へのアクセスが阻害された場合、学園各部門の正常な運営や、(在籍中の学生、生徒、園児や各々の卒業生及び教職員など)学園と関係ある者の個人情報に重大な影響を及ぼすおそれがあるもの。
- (2) 第二種情報資産：第一種情報資産以外の情報資産。
- (3) 第一種、第二種の分類は、原則その情報資産を作成した部局が決定する。

(情報資産の管理)

第5条 情報資産は、原則として、当該情報資産を作成・保有した部局が管理しなければならない。

- 2 学園が所有または契約して利用するサーバ等に保存されず、やむを得ず個人用PC等のクライアント機器に保存された情報資産は、原則として、当該機器を日常利用する者が管理しなければならない。
- 3 各管理者は、第4条に基づいて分類されているそれぞれの情報資産について、その重要度に応じた物理的、人的、技術的な各セキュリティ対策を以下の各号のように実施する。

(1) 物理的セキュリティ対策

情報資産が設置、保存されている場所や施設の安全を保ち、不正なアクセスを防止すること。また、情報資産自体の移動について安全に実施できるような対策を講じること。

(2) 人的セキュリティ対策

ユーザの操作が原因となって情報資産の安全が損なわれないよう、情報資産に係る操作についての禁止事項を定める他、事故が生じた場合の対応の原則を定め、損害が最小限に収まるよう対策を講じること。また情報セキュリティについて学習や訓練を実施し、知識とスキルの向上を図ること。

(3) 技術的セキュリティ対策

IT技術を利用し、学園内外から情報資産へのアクセスや編集等の操作について、安全・円滑に行うことができるよう、対策を講じること。

- 4 第4条で分類した各情報資産の公開・非公開・限定公開等の開示条件は、その資産を管理する部局が決定する。

- 5 第1項から第4項に基づき、情報資産を各部局が適切に管理するために、必要な実施規程、内規等を別途定める。

(インシデントへの対応)

第6条 情報セキュリティ部局責任者は、部局内の情報資産に関するインシデントが発生した場合、以下の各号を速やかに実施する。各号の詳細については、別途定める。また必要に応じ、セキュリティ会議を開催し、対応について協議を行う。

- (1) 所定の経路により、情報セキュリティ統括責任者へインシデントの連絡を行う。
- (2) インシデントが生じた情報資産について、所定の手続きを行い、損害の最小化、損害

が生じた情報資産の復旧等を実施する。

- (3) 前号の対応完了の際、報告書を作成し、情報セキュリティ統括責任者へ提出する。
- (4) 同様なインシデントの再発を防止するために、必要な対策を講じる。

第4章 評価・見直し

(情報セキュリティ対策の点検)

第7条 情報セキュリティ代表責任者は、所管する情報資産に係る物理的・技術的・人的セキュリティ対策について、定期的な点検を実施し、その結果を情報セキュリティ統括責任者に報告する。

(情報セキュリティ対策の改善)

第8条 情報セキュリティ統括責任者は、実施された情報セキュリティ対策について、改善が必要と認められる場合には、情報セキュリティ代表責任者に対して、必要な措置を講じるよう命じる。

- 2 情報セキュリティ代表責任者は、情報セキュリティ統括責任者の命に従い、情報セキュリティ部局責任者に必要な対策を実施するよう指示を行う。また対策後の結果について、情報セキュリティ統括責任者に報告する。

(情報セキュリティ関連規程の更新)

第9条 情報セキュリティ統括責任者は、必要に応じ、この基本規程及び関連規程について見直しを行い、改善が必要と認められる場合は、内容の更新を行う。

(監査)

第10条 学園の情報セキュリティに係る監査は、**学校法人比治山学園監査規程**、及び**学校法人比治山学園内部監査実施要領**に則り、業務監査に準じた方法により実施するものとする。

(事務の所管)

第11条 この規程に関する事務は、法人事務局図書・情報メディア課が行う。

(雑則)

第12条 この規程の施行に関して必要な事項は、情報セキュリティ統括責任者が別途定める。

附 則（令和6年3月22日制定）

- 1 この規程は、令和6年4月1日から施行する。
- 2 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）は、この規程の施行期日をもって廃止する。