

## 大阪青山大学 情報セキュリティポリシー

### 1. 基本方針

大阪青山大学（以下「本学」という。）における情報システムは、本学の全ての教育・研究活動及び運営の基盤として設置され、運用される。

本学の情報システムを利用して情報を適切かつ有効に取り扱うことにより教育及び研究の充実に資するためには、情報基盤の整備に加えて、安全かつ信頼される情報セキュリティを確保することが不可欠である。

そのために、本学の情報の保護及び活用並びに適切な情報セキュリティ対策を図ることを目的として、大阪青山大学情報セキュリティポリシー（以下「本ポリシー」という。）を制定する。

本ポリシーが目指すものは、次のとおりとする。

- (1) 本学の情報セキュリティに対する侵害の阻止
- (2) 学内外の情報セキュリティを侵害する行為の抑止
- (3) 情報資産の管理の徹底
- (4) 情報セキュリティ侵害の早期検出と迅速な対応の実現
- (5) 情報セキュリティの評価と更新

### 2. 対象範囲および対象者

本ポリシーの対象範囲は、本学の管理するすべての情報資産である。情報資産には、本学が所有する、もしくは本学のネットワークに接続する情報システム、情報システム内部に記録された情報、またその情報を書き出した書面や記録媒体を含む。本学以外に保管される情報資産であっても、本学保有の情報資産として認められるものは対象となる。

本ポリシーは、本学の情報資産を利用する教職員、学生、委託業者、来学者等など、利用を許可されたすべての者を対象とする。

### 3. 実施方法

本学には、対象者が本ポリシーを理解し、実施できるように教育、指導する責任がある。本ポリシーを実施するための対策基準、実施手順は、別途定めるものとする。

### 4. 対象者の義務

すべての対象者は、本ポリシーを遵守しなければならない。意図の有無を問わず、学内外の情報資産に対する権限のないアクセスや改ざん、複写、破壊、漏洩等をしてはならない。

### 5. 情報セキュリティ責任者

本学は、情報セキュリティを組織的に管理運用する体制を確立するために、情報セキュリティ責任者〔Chief Information Security Officer〕（以下「CISO」という。）を置く。

CISOは、情報システム担当理事をもって充て、本学の情報システム資産の管理・運用を総括する。

6. 法令等の遵守および違反への罰則

情報資産の取り扱いに関しては法令及び規制等についても遵守する必要がある。本ポリシーならびに本ポリシーに基づく対策基準、実施手順に対する違反があった場合の懲戒については、学則または就業規則による。

7. 本ポリシーの評価と更新

本ポリシーに基づく情報セキュリティ対策については、その実効性を定期的に評価し、改善が必要と認められた場合は、速やかに更新する。

8. 本ポリシーの改廃

本ポリシーの改廃は、軽微なものを除き理事会が行う。

以上