

## 情報システム利用規程

### 2201-1 (目的)

第1条 この規程は、学校法人関西学院(以下「本学院」という。)における情報システムの利用に関する事項を定め、情報セキュリティの確保と円滑な情報システムの利用に資することを目的とする。

### 2201-2 (適用範囲)

第2条 この規程は本学院構成員および別途定める手続きにより許可を受けて本学院情報システムを利用する者に適用する。

### 2201-3 (遵守事項)

第3条 利用者等は、本規程、本学院の定める情報セキュリティポリシー及び関連規程、並びに本学院情報システムの利用に関する手順を遵守しなければならない。

### 2201-4 (関西学院システム利用IDの申請)

第4条 本学院情報システムを利用する者は、定められた手順に従い、関西学院システム利用IDの交付を受けなければならない。

2 来訪者に本学院情報システムを利用させる場合、申請者は臨時的な関西学院システム利用IDの交付を受けなければならない。また、申請者は来訪者に本規程を遵守させなければならない。

### 2201-5 (情報機器の利用)

第5条 利用者等は、情報の作成、利用、保存等のための情報機器の利用にあたっては以下の各号に従わなければならない。

- 1 利用者等は、本学院情報ネットワークに情報機器を接続しようとする場合は、定められた手順に従って接続の許可を得なければならない。ただし、情報コンセントや無線LANからあらかじめ指定された方法により本学院情報システムに接続する場合はこの限りではない。
- 2 利用者等は、第1号により許可を受けた情報機器の利用を取りやめる場合には定められた手順に従って届け出なければならない。
- 3 利用者等は、情報漏えいの防止に努めなければならない。
- 4 利用者等は、情報機器の紛失や盗難に注意しなければならない。
- 5 情報機器の紛失および盗難が発生した場合は、職場情報セキュリティ責任者又は個別情報システム担当者に届け出なければならない。

### 2201-6 (利用者等による情報セキュリティ対策教育の受講義務)

第6条 利用者等(臨時的利用者を除く)は、本学院情報システムの利用に関する教育を受講しなければならない。

2 利用者等(臨時的利用者を除く)は、情報セキュリティ対策の訓練に参加しなければならない。

### 2201-7 (制限事項)

第7条 利用者等は、本学院情報システムについて以下の各号に定める行為を行ってはならない。ただし、教育、研究、又はセキュリティ確保のために必要な場合には、統括情報セキュリティ責任者の許可を得て行うことができるものとする。

- 1 ファイルの自動公衆送信機能を持ったファイル交換ソフトウェアを利用する行為
- 2 不正ソフトウェア類似のコードやセキュリティホール実証コードを作成、所持、使用および配布する行為（ただし、教育、研究、又はセキュリティ確保のために必要な場合は、その限りではない）
- 3 情報機器の利用情報を取得する行為
- 4 情報システムのセキュリティ上の脆弱性を検知する行為

#### 2201-8（禁止事項）

第8条 利用者等は、本学院情報システムについて、次の各号に定める行為を行ってはならない。

- 1 当該情報システム及び情報について定められた目的以外の利用
- 2 指定以外の方法での学外からの全学アカウントを用いての本学院情報システムへのアクセス
- 3 あらかじめ指定されていない本学院情報システムを本学院外の者に利用させる行為
- 4 守秘義務に違反する行為
- 5 差別、名誉毀損、侮辱、ハラスメントにあたる行為
- 6 個人情報やプライバシーを侵害する行為
- 7 著作権等の財産権を侵害する行為
- 8 通信の秘密を侵害する行為
- 9 前条に該当しない不正ソフトウェアの作成、所持および配布行為
- 10 過度な負荷等により本学院の円滑な情報システムの運用を妨げる行為
- 11 不正アクセス行為の禁止等に関する法律に反する行為、またはこれに類する行為
- 12 その他法令に基づく処罰の対象となる行為
- 13 上記の行為を助長する行為

#### 2201-9（安全管理義務）

第9条 利用者等は、自己の管理する情報機器について、本学院情報ネットワークとの接続状況に関わらず、安全性を維持する一次的な担当者となることに留意し、次の各号にしたがって利用しなければならない。

- 1 ソフトウェアの状態および不正ソフトウェア対策機能を最新に保つこと。
- 2 不正ソフトウェア対策機能により不正プログラムとして検知されるファイル等を不用意に開かないこと。
- 3 不正ソフトウェア対策機能の自動検査機能を有効にすること。
- 4 不正ソフトウェア対策機能により定期的にすべての電子ファイルに対して、不正プログラムが存在しないことを確認すること。
- 5 外部からデータやソフトウェアを情報機器に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正ソフトウェアが存在しないことを確認すること。
- 6 常に最新のセキュリティ情報に注意し、不正ソフトウェア感染の予防に努めること。

#### 2201-10（規程の改廃）

第10条 この規程の改廃は、情報化推進機構長室会で決定する

#### 附則

- 1 この規程は2023年6月1日から施行する。