情報セキュリティ基本方針

1．要旨

学校法人皇學館（以下「本学」という。）が保有する情報資産の安全性及び安定性を確保することを目的とし、学校法人皇學館情報セキュリティ基本方針及びその他情報セキュリティに関する規程（以下「情報セキュリティ関係規程」という。）においてセキュリティ対策を進める上で遵守すべき事項を定め、情報セキュリティの確保に取り組むこととする。

本学の情報資産を利用する者は、情報セキュリティの重要性を認知し、この情報セキュリティ関係規程及び情報セキュリティに関連する法律･法令を遵守しなければならない。

2．適用範囲

情報セキュリティ関係規程の適用範囲は、本学の教育、研究及び運営に関する情報資産とする。また、本学 が外部委託する情報資産も準拠する。

3．適用者

情報セキュリティ関係規程の適用者は役員、皇學館大学、皇學館高等学校、皇學館中学校の教職員（非常勤、嘱託、臨時などの教職員を含む）、学生、生徒の本学構成員及びその他本学情報資産に接する者、全てとする。

4．情報セキュリティ対策の目的及び実施項目

本学の社会的責任を果たし、本学の教育的価値を向上させることを目的に、情報セキュリティを確立し継続的かつ最適な情報セキュリティ活動を実施するため、下記項目を実施することとする。

（1）本学が保有する情報資産を機密性、完全性、可用性の観点から適切に管理、保護する。
（2）情報セキュリティに係る各種法令及び規範を遵守する。
（3）情報セキュリティ基本方針や各種施策を本学の構成員に周知徹底する。
（4）本学の情報セキュリティの実施状況を監視し、継続的な改善に努める。

5．公開対象者

情報セキュリティ基本方針は、本学の情報セキュリティに対する考えの周知を図るために本学の内外に広く公開する。

一方、その他の情報セキュリティ関係規程には、公開することにより本学の情報セキュリティ対策の運用に重大な支障を及ぼす恐れのある情報が含まれることから非公開とする。

6．公開手続き

情報セキュリティ基本方針の学外への公開は、本学の情報セキュリティ委員会の承認を経て行う。

7．基本用語の定義

情報セキュリティポリシー関係規程における用語は、以下の通り定義する。

（1）脅威

情報資産の正常な運用を脅かすもので自然の脅威（地震、火災、風水害など)、情報システムの脅威（情報システムの故障、サービスの停止、誤作動、停電等）及び人的な脅威（不正行為、過失、誤使用・誤操作など）をいう。

（2）脆弱性

情報セキュリティ規程・要員教育の不備、システムの欠陥、建物の構造上の欠陥、定期点検の不備、など脅威を発生し易くさせる要因、脅威を増加させる要因（脆さ、弱点）をいう。

（3）機密性

情報にアクセスすることが認可された者だけが情報資産を利用できることをいう。

（4）完全性

情報資産が、改ざん、滅失、棄損されていないことをいう。

（5）可用性

許可された利用者が必要なときに情報資産を利用できることをいう。

（6）記録媒体

磁気ディスク、光学ディスク及びメモリなどのデータを記録する機器等、ならびに情報が記録された紙、帳票などをいう。

（7）情報機器

ハードウェア及びソフトウェアで構成されるコンピュータと周辺機器及び、スマートフォンやタブレット端末などの通信機能を持つ機器をいう。

（8）ネットワーク

情報機器を相互に接続するための通信網、そのネットワーク機器で構成され、処理を行う仕組みをいう。

（9）情報システム

情報機器、ネットワーク及び記録媒体をいう。

(10) 情報資産

情報システムの開発と運用に係るすべての情報ならびに情報システムで取り扱う全ての情報、及び情報システムをいう。

(11) 情報セキュリティ

情報システムを取り巻くさまざまな脅威から、情報資産を機密性・完全性・可用性の確保を行いつつ、正常に維持することをいう。

(12) 不正プログラム

コンピュータウイルス等の情報システムを利用する者が意図しない結果を情報システムにもたらすソフトウェアの総称をいう。

(13) セキュリティインシデント

情報セキュリティに関する事件、事故、障害等情報資産の機密性、完全性、可用性のいずれか一つでも損なわれるような事態をいう。

8．体制

本学の情報セキュリティ対策の目標を維持、推進するために必要な体制を整備する。

9．情報セキュリティ委員会の設置

本学の情報セキュリティ対策の目標を維持、推進するため、情報セキュリティに関する施策の立案及び推進を行うことを担う情報セキュリティ委員会を設置する。

10. 情報セキュリティ委員会の役割と責務

10. 1 情報セキュリティマネジメントの企画及び計画

情報セキュリティ委員会は、本学における情報セキュリティマネジメントを実施していく企画及び計画を作成し、その計画に則り情報セキュリティマネジメントを実施しなければならない。この企画及び計画には、情報セキュリティマネジメントを遂行する為のリスクアセスメント、リスクマネジメントはもちろんのこと、情報セキュリティ関係規程の見直しや本学構成員への普及・啓発の取り組みも含まれなければならない。

10. 2 情報セキュリティ関係規程の各種通知文書の周知責任

情報セキュリティ委員会は、情報セキュリティ関係規程を策定又は改訂した場合には、迅速に適用対象となる本学構成員へその内容を周知しなければならない。

また、情報セキュリティ事案が発生した場合に発出される、注意喚起及び対応手順等の周知について配慮しなければならない。

10. 3 教育・指導の実施

情報セキュリティ委員会は、情報セキュリティに関する継続的な教育・指導を行う。この教育・指導は、意識向上と技術向上の両面から実施しなければならない。

10. 4 情報セキュリティ関係規程の遵守状況の点検・評価及び改訂

情報セキュリティ委員会は、本学構成員の情報セキュリティ関係規程の遵守状況を定期的に監査し、情報セキュリティ関係規程の点検・評価を行う。

また、本学構成員の情報セキュリティ関係規程に対する意見や要望を収集し、その妥当性を評価するとともに必要に応じて内容の改訂を行うものとする。

10. 5 監査結果の評価及び改訂

情報セキュリティ委員会は、実施した監査の結果に基づき、情報セキュリティ関係規程の妥当性を評価すると共に、必要に応じて、内容の改訂を行わなければならない。

10. 6 報告

情報セキュリティ委員会は、情報セキュリティの維持・管理状況や情報セキュリティ関係規程の改訂状況、及びセキュリティインシデントの発生状況を常勤理事会へ報告しなければならない。

11. 情報セキュリティマネジメント

11. 1 リスク分析

本学の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

11. 2情報セキュリティ関係規程の策定

情報セキュリティ委員会は、情報セキュリティ基本方針及び情報セキュリティ対策基準を策定することとする。情報セキュリティ対策基準に基づく情報セキュリティ対策手順に関しては、情報セキュリティ委員会より指名された者が策定し、運用しなければならない。

11. 3 対策の実施

本学で策定した情報セキュリティ関係規程に記述した対策は、計画的に実施しなければならない。情報セキュリティ担当部門は、セキュリティ対策実施のための計画書を策定し、情報セキュリティ委

員会の承認を得なければならない。

（1）人的セキュリティ対策

情報資産に接する本学構成員・その他の人員の情報セキュリティに関する権限や責任等を定めるとともに、すべての職員に情報セキュリティ関係規程の内容を周知徹底するため、教育・訓練を行う。

（2）物理的セキュリティ対策

本学が所有するコンピュータ、周辺機器、記憶媒体等の情報資産については、盗難、紛失及び自然災害、人的理由による損壊等が発生しないよう、適切な場所で保管するとともに、使用並びに移動の際にも注意を払わなければならない。

特にサーバ室等について膨大かつ重要な情報資産が保管されており、不正な立入り等から保護するため、入退室や機器管理上の物理的な対策を講ずる必要がある。

（3）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス等の不正プログラム対策を実施する。

（4）情報資産の分類

本学が保有する情報資産については、その重要度に応じて利用者を制限するとともに、その利用及び保管方法についても適切な措置を行うものとする。

ア．非公開情報

重要度が高く、漏えいした場合、本学の信用を失墜するとともに運営に重大な支障を来すもの。

イ．限定公開情報

その公開が、構成員に限定されるとともにその利用に制限が加えられるべきもの。

ウ．公開情報

本学構成員及び部外者など、不特定多数に対してデータ及び書面等、各種媒体で公開が可能なもの。

（5）情報資産の新規導入

情報資産の安定稼働のため、新たにコンピュータ及び周辺機器の導入及びシステム・プログラムの導入に際しては、計画案の時点から情報セキュリティ担当者を加えるとともに、情報セキュリティ委員会へ随時報告し、導入への承認を行うものとする。

（6）ネットワークの利用

本学の情報資産が接続するネットワークは、本学が所有するネットワークに限定され、その利用に当たっては、情報セキュリティ委員会の承認を受け接続できるものとする。

例外措置にあっては、事前に情報セキュリティ委員会へ、利用するネットワーク及び接続する 情報資産並びに接続の必要性等を申請し、承認を受けて接続すること。

（7）運用

本学の情報資産を不正プログラムの感染・蔵置及び不正アクセス等によって、機器の誤作動・停止、システム障害、情報漏えい等のセキュリティインシデントが発生しないよう、機器の運用・監視を徹底し未然防止対策を講ずるとともに、発生した際は、迅速に被害の拡大・波及の防止とともに早期復旧に向けた適切な措置を講ずること。

また、情報セキュリティ事案を認知した際は、直ちに構成員へ速報し、組織的に対応すること。

11．4 教育・啓発

本学は、情報資産を扱うすべての者に対し、意識向上と技術レベルの向上の両面から、積極的に情

報セキュリティの教育を行うこととする。

本学の情報資産に関わるすべての者は、本学が提供、もしくは推薦する情報セキュリティの教育を受けなければならない。同時に、本学の情報資産に関わる者は、情報セキュリティに関する最新の情報について入手した際は、自発的に情報セキュリティ委員に提言することが望ましい。

11. 5 監査・評価

情報セキュリティ委員会は、自ら実施する情報セキュリティ監査結果に基づき情報セキュリティ関係規程の評価、見直しを行う。また、情報資産の利用者から届けられた脅威、脆弱性の情報や情報セキュリティの脆弱性に関する情報の収集等の活動から得られる情報をもとに情報セキュリティ関係規程の評価、見直しを行う場合もある。

11. 6 文書の改廃

情報セキュリティ基本方針の改廃は、常勤理事会の承認を必要とする。情報セキュリティ対策基準及び実施手順は、情報セキュリティ委員会が決定する。

12. 違反時の懲戒処分

情報セキュリティ関係規程に違反した場合は、懲戒処分等の対象とする。情報セキュリティ委員会は、情報セキュリティ関係規程に違反した事項の重要度を評価し、適切な処置を講じる。

13. セキュリティインシデント発生時の対応

本学の情報セキュリティが侵害されたと思われる事象が判明した場合や、本学構成員により学内外に係わらず情報セキュリティ侵害が行われた事象が判明した場合は、その影響度に応じた体制を構築しその対応を行う。

14. 評価と見直し

情報セキュリティの実施状況などを踏まえるとともに、情報セキュリティを取り巻く新たな脅威などへの対応のため、情報セキュリティ関係規程の見直しを実施するものとする。

15. 施行期日

本方針は、令和 4 年 3 月 1 日より施行する。