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。）における情報資産の機密性、完全性及び可用性を維持するため、学校法人皇學館情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）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ポリシー及び法律を遵守しなければならない。

２．適用範囲

情報セキュリティポリシーの適用範囲は、本学の情報資産とし、外部委託する情報資産も準拠する。

３．適用者

情報セキュリティポリシーの適用者は役員、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、全てである。

４．構成と位置づけ

情報セキュリティポリシーは、以下の３つの階層に分けて策定・管理される文書とする。

情報セキュリティ基本方針は、本学の情報セキュリティ対策を構築するにあたっての基本的な方針を明らかにしたものである。今後この文書を情報セキュリティの拠り所として位置づける。

情報セキュリティ基本方針に従い、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定する。

情報セキュリティ対策を実施するためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定する。

なお、情報セキュリティポリシーは、関連法規と照らして違反することの無いようにしなければならない。主な関連法規としては、以下のものが挙げられる。

- 刑法
- 民法
- 商法
- 不正アクセス行為の禁止等に関する法律
- 個人情報保護法
- 不正競争防止法
- 著作権法
- 建築基準法/同施行令
- 消防法/同施行令/同施行規則

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、情報セキュリティ対策基準、情報セキュリティ実施手順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

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定・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アクセスできることを確実にすることをいう。

（4）完全性

情報及び処理方法の正確さ及び完全である状態を完全防御することをいう。

（5）可用性

認可された利用者が必要なときに情報にアクセスできることを確実にすることをいう。

（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

情報資産の機密性、完全性及び可用性を維持することをいう。

８．体制

本学の情報セキュリティを維持、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役割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、情報セキュリティポリシー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 情報セキュリティポリシー文書の周知責任

情報セキュリティ委員会は、情報セキュリティポリシー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。

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 情報セキュリティポリシーの遵守状況の点検・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ポリシー遵守状況を定期的に監査し、情報セキュリティポリシーの点検・評価を行う。

また、本学構成員の情報セキュリティポリシー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、情報セキュリティポリシー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ポリシーの改訂状況、及び情報セキュリティに関する事故や問題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 ポリシー策定

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ポリシーに記述した対策は、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ポリシー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

サーバ室等について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。

（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対策等を実施する。

（4）運用

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、ネットワークの監視等の運用面における必要な措置を講ずる。また、故障が発生した際の迅速な対応を可能とするため、故障時の対応を講ずる。

11. 4 教育・啓蒙

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、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ポ

リシーの評価、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ポリシーの評価、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

情報セキュリティポリシーに違反した場合は、懲戒処分等の対象とする。情報セキュリティ委員会は、情報セキュリティポリシー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. 情報セキュリティ事故・事件発生時の対応

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. 施行期日

本方針は、平成２１年４月１日より施行する。

15. 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、情報セキュリティポリシーの見直しを実施するものとする。