学校法人関西金光学園 情報セキュリティ対策基準

１．対象範囲及び用語説明

（１） 部門等の範囲

本対策基準の適用を受けるのは、学校法人関西金光学園（以下「本学園」という。）が設置する関西福祉大学、関西福祉大学金光藤蔭高等学校、金光大阪中学校・高等学校及び金光八尾中学校・高等学校（以下「各学校」といい、学園本部を含む。）とする。

（２） 情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

２．組織体制

（１） 最高情報セキュリティ責任者（CISO:Chief Information Security Officer、以下「CISO」という。）

① 理事長を CISO とする。CISO は、本学園における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

② CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置くことができる。

（２） 情報セキュリティ責任者

① 学園本部長を情報セキュリティ責任者とする。

② 情報セキュリティ責任者は、本学園の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③ 情報セキュリティ責任者は、本学園において所有している情報システムにおける情報セキュリティに関する開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④ 情報セキュリティ責任者は、本学園において所有している情報システムについて、緊急時等における連絡体制の整備その他必要な事項を行う。

（３） 情報セキュリティ管理者

① 学園本部にあっては学園本部長、関西福祉大学にあっては学長、関西福祉大学金光藤蔭高等学校、金光大阪中学校・高等学校及び金光八尾中学校・高等学校にあっては校長をそれぞれ情報セキュリティ管理者とする。

② 情報セキュリティ管理者は、各学校の情報セキュリティ対策に関する権限及び責任を有する。

③ 情報セキュリティ管理者は、教職員等（専任教職員、準専任教職員、期限付常勤教

職員及び非常勤教職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

④　情報セキュリティ管理者は、各学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者（学園本部長）へ速やかに報告を行い、指示を仰がなければならない。

（４）　情報システム管理者

①　情報システム管理者は、情報セキュリティ管理者（学長、校長）が各学校の実情に応じて適切に定める。

②　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

④　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（５）　情報システム担当者

①　情報システム担当者は、情報セキュリティ管理者（学長、校長）が各学校の実情に応じて適切に定める。

②　情報システム担当者は、情報システム管理者（各学校で定める。）の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。

（６）　兼務の禁止

①　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

３．情報資産の分類と管理方法

情報資産の分類及び管理方法については、情報セキュリティ管理者（学長、校長）が各学校の実情に応じて適切に定める。

４．物理的セキュリティ

物理的セキュリティについては、情報セキュリティ管理者（学長、校長）が各学校の実情に応じて適切な対策を講じる。

５．人的セキュリティ

人的セキュリティについては、情報セキュリティ管理者（学長、校長）が各学校の実情に応じて適切な対策を講じる。

６．技術的セキュリティ

技術的セキュリティについては、情報セキュリティ管理者（学長、校長）が各学校の実情に

応じて適切な対策を講じる。

7．運用

7．1．情報セキュリティポリシー等の遵守状況の確認

① 情報セキュリティ責任者（学園本部長）及び情報セキュリティ管理者（学長、校長）は、情報セキュリティポリシー等の遵守状況について確認を行い、問題を認めた場合には、速やかに CISO（理事長）に報告しなければならない。

② CISO（理事長）は、発生した問題について、適切かつ速やかに対処しなければならない。

7．2．懲戒処分等

（1） 懲戒処分

情報セキュリティポリシー等に違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、当該教職員等及び当該監督責任者に適用される就業規則による懲戒処分の対象とする。

（2） 違反時の対応

教職員等に情報セキュリティポリシー等に違反する行動が確認された場合には、情報セキュリティ管理者（学長、校長）は、当該教職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、情報セキュリティ管理者（学長、校長）は、教職員等の権利を停止あるいは剥奪した旨を情報セキュリティ責任者（学園本部長）に報告しなければならない。

8．外部サービスの利用

8．1．外部委託

（1） 外部委託事業者の選定基準

① 情報システム管理者（各学校で定める。）は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

② 情報システム管理者（各学校で定める。）は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（2） 契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で情報セキュリティ要件を明記した契約を締結しなければならない。情報セキュリティ要件は、情報セキュリティ管理者（学長、校長）が各学校の実情に応じて適切に定める。

8．2．約款による外部サービスの利用

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

8．3．ソーシャルメディアサービスの利用

① 情報システム管理者（各学校で定める。）は、各学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関するなりすまし対策及びアカウント乗っ取り対策等を講じなければならない。

② 教職員等は、個人情報、知的財産権に関する情報、本学園の業務の適正な実施に支障を及ぼすおそれがある情報、本学園の名誉・信用を傷つける内容の情報その他これらに類する情報をソーシャルメディアサービスで発信してはならず、本学園その他第三者の知的財産権を侵害しないよう留意しなければならない。退職後も同様とする。

③ 情報セキュリティ管理者（学長、校長）は、利用するソーシャルメディアサービスごとの責任者を定めなければならない。

９．評価・見直し

９．１．監査

CISO（理事長）は、情報セキュリティ監査責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせるものとする。

９．２．見直し

情報システム管理者（各学校で定める。）は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施するものとする。

１０．実施手順

情報セキュリティ管理者（学長、校長）は、本対策基準の個別具体的な実施事項について定めた実施手順を、各学校の実情に応じて定めるものとする。

１１．改廃

この対策基準の改廃は、理事長が行う。

附　則

この対策基準は、平成３０年４月１日から施行する。