情報セキュリティ基本ポリシー

2002 年 10 月 11 日 理事会 決定

1. 前文

学校法人関西学院、関西学院大学、関西学院高等部及び関西学院中学部（以下「本学」という。）は、本学が所有し管理する情報システム・関連設備、プログラム及びデータ等、すべての情報資産について、適切なセキュリティを保障する義務と責任を有する。また、本学の全構成員も同様に、この義務を負うものとする。

2. 定義と役割

1）情報セキュリティの定義

情報セキュリティとは「情報の機密性・完全性・可用性を実現するために情報資産を維持・管理すること」と定義され、以下に掲げる情報資産の損失を招く潜在的原因からそれらを保護することである。

保護されるべき情報資産

・コンピュータ及び情報通信施設・設備
・コンピュータの周辺機器
・関連物品、及びデータ記憶メディア
・システムプログラム及び関連文書
・アプリケーションプログラム及び関連文書
・データ

これらの損失を招く潜在的原因を「脅威」とする。これらの脅威には人為的もしくは自然発生的、偶発的、故意によるものが含まれる。

2）情報セキュリティポリシーの役割

情報セキュリティポリシーは、本学における情報セキュリティの方針を示すものである。これは、本学の全構成員が遵守すべきものであり、本学の情報資産の保護を目的としている。したがって、本学のすべての構成員は、情報資産の使用権限に応じてセキュリティ管理についての義務と責任を負わなければならない。

3. 適用範囲

情報セキュリティポリシーは、本学が所有するすべての情報資産を対象とし、本学の情報システムを利用するすべての構成員に適用される。ここでいう構成員には、本学の情報システムを使用する学外のユーザを含む。

4. 構成

本学の情報セキュリティポリシーは、「情報セキュリティ基本ポリシー(本文書)」（以下「基本ポリシー」という。）と複数の「基準とガイドライン」から構成される。

「基準とガイドライン」は、一般ユーザ及びシステム管理者が情報セキュリティへの責任を果たすための情報セキュリティポリシーの附則であり、情報セキュリティポリシーを詳細に定義しているものである。

「基本ポリシー」と各「基準とガイドライン」を総称して「関西学院情報セキュリティポリシー」とする。

5. 管理体制

1）情報セキュリティ管理体制

本学の情報セキュリティ対策を推進するために情報セキュリティ統括責任者（以下「統括責任者」という。）及び情報セキュリティ管理担当責任者（以下「管理担当責任者」という。）を置く。

統括責任者は常任理事（情報担当）とし、管理担当責任者は情報システム室長とする。

情報セキュリティ担当部署（以下「セキュリティ担当部署」という。）は情報システム室とする。

統括責任者は、教育研究、事務、図書、ネットワークなどの主要システムについて、それぞれ情報セキュリティ管理者（以下「セキュリティ管理者」という。）を置かなければならない。

各セキュリティ管理者は、必要に応じて、部局毎に情報セキュリティ担当者（以下「セキュリティ担当者」という。）を置くものとする。

2）情報セキュリティポリシーの管理

情報セキュリティポリシーの作成、管理・運用は、情報システム室長が責任をもって行わなければならない。

情報セキュリティポリシーは、法的・社会的要求、予想される危険など、必要に応じ変更されるものとする。

「基本ポリシー」の制定及び変更については、情報システム会議で協議の上、理事長及び学長の承認を得なければならない。

「基準とガイドライン」の策定及び変更については、情報システム会議常設運営委員会で協議の上、情報システム室長の承認を得なければならない。

6. 遵守義務と責任及び罰則

1）遵守義務と責任

・ユーザ

すべてのユーザは、情報セキュリティポリシーの関連項目に精通し、情報資産の利用にあたって本ポリシーを遵守しなければならない。また、関連する法令・学内諸規程を遵守し、これに従わなければならない。

すべてのユーザは、情報セキュリティに関する問題が発生した場合には、速やかにセキュリティ担当者もしくは、セキュリティ管理者に報告しなければならない。

個人研究室、共同研究室等で専任教職員ユーザ自らが直接管理する情報資産については、各自がそのセキュリティに関する責任を負わなければならない。

・情報セキュリティ統括責任者

セキュリティ統括責任者は、全学的見地から、本学の情報セキュリティの維持・向上に努め、セキュリティ対策を推進しなければならない。

・情報セキュリティ管理担当責任者

セキュリティ管理担当責任者は、セキュリティ統括責任者を補佐し、本学の情報セキュリティの実際的な維持と、具体的なセキュリティ対策を推進しなければならない。

・情報セキュリティ担当部署

セキュリティ担当部署は、セキュリティポリシーの維持及びセキュリティ対策の企画、推進に努めなければならない。また、情報セキュリティ教育の推進及び啓発に努めなければならない。

・情報セキュリティ管理者

セキュリティ管理者は、情報セキュリティ担当部署と協力し、セキュリティ確保のための技術導入、管理規程の策定等を行い、情報セキュリティの維持・向上に努めなければならない。

・情報セキュリティ担当者

セキュリティ担当者は、セキュリティ管理者と協力し、各部局内でのポリシーの徹底と普及をはかり、情報セキュリティの維持・向上に努めなければならない。

2）違反者に対する措置

情報セキュリティポリシーの違反者に対しては、ネットワーク利用倫理規程に基づき、相当の措置をとることができるものとする。

7. 例外措置

情報セキュリティが脅威に晒された場合には、そのセキュリティリスク及び損失を最小化するためにセキュリティ管理者が行った行為について、その遵守義務を免除することがある。

また、情報セキュリティポリシーの遵守によって、その損失が避けられない場合については、セキュリティ統括責任者の許可の下に、その改善措置がとられるまでの時限的例外措置を設定することができる。

これらの場合には、情報システム会議に顛末が報告されなければならない。

8. 謝意

本学は、情報セキュリティポリシーの作成にあたり Murdoch University の IT セキュリティポリシー関連資料の使用を認めていただいたことに感謝する。

また、本学の考え方に協調いただける場合には、他大学及びその他の機関に、本ポリシーに関する資料を、使用許可を得ることを条件に提供する。

【 用語の定義 】

・情報の機密性（confidentiality of information）

第三者に情報が漏れないようにすること。

情報へ権限のない者のアクセスを許さず、情報が正規の方法で承認を受けた者にのみ開示されること。

・情報の完全性（integrity of data）

情報が正確かつ完全に維持されること。

情報及びプログラムが規程に基づき承認を受けた方法でのみ変更されること。

・情報の可用性（availability of system）

情報システムが定められた方法でいつでも利用できるようにすること。

障害の発生等で情報システムが利用できないような状態に置かないこと。

・ユーザ

本学の情報システムを使用する者。

以　上