短大情報セキュリティポリシー

戸板女子短期大学

平成２８年　３月　８日

1　情報セキュリティ基本方針

戸板女子短期大学（以下「短大」という。）では、学術研究、教育、運営業務等を遂行するにあたり、情報基盤の整備とともに、情報資産の保護が不可欠である。よって、本短大の持つ全ての情報資産を、故意や過失の区別なく、学内外からの改ざん、破壊、漏洩等から守り、情報資産の機密性、完全性及び可用性を維持するため、学園情報セキュリティポリシーに基づき、短大情報セキュリティポリシーを制定し、情報セキュリティの確保に最大限取り組むこととする。

この際、個人情報保護を重視し、短大の全員が情報セキュリティの重要性を認識するとともに、意識を向上させ、情報セキュリティポリシーを遵守しなければならない。

2　用語の定義

(1)　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2)　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みであり、基本システムと業務システムからなる。

ア　基本システム

(ｱ)　教職員システム

教職員用パソコン（以下、「ＰＣ」という。）に必須導入される標準ソフトウェア（ＯＳ、業務用アプリケーション、ウィルス対策ソフト、グループウェア等）及びそれを構成するハードウェア並びにネットワーク

(ｲ)　学生システム

学生用ＰＣに必須導入される標準ソフトウェア（ＯＳ、業務用アプリケーション、ウィルス対策ソフト、グループウェア等）及びそれを構成するハードウェア並びにネットワーク

イ　業務システム

各部署で独自に導入する図書館システム、教務システム、学費システム、入試広報システム、就職支援システム

(3)　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。

ア　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

イ　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

ウ　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(4)　情報資産

ネットワーク及び情報システムで取り扱う全ての情報をいう。なお、情報資産には紙等の有体物に出力された情報も含むものとする。

(5) 情報セキュリティポリシー

情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ対策手順をいう。

3 適用範囲

(1) 人的適用範囲

専任教職員、非常勤教職員、契約職員、派遣職員、パート、アルバイトを含む全ての教職員（以下「教職員等」という。）並びに学生の短大全所属人員とする。

(2) 情報資産の範囲

ア ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

イ 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。）

ウ 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

4 対象とする脅威

(1) 部外者の侵入による機器又は情報資産の破壊・盗難、故意の不正アクセス又は不正操作による情報資産の盗聴・改ざん・消去等

(2) 教職員等、学生又は外部委託事業者による機器又は情報資産の持出、誤操作、アクセスの為の認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊・改ざん・消去等、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏えい等

(3) コンピュータウィルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

5 教職員等の遵守義務

教職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守しなければならない。

6 情報セキュリティ対策

(1) 情報セキュリティ管理体制

本短大の情報資産について、情報セキュリティ対策を推進・管理するための全校的な体制を確立する。

(2) 情報資産の分類と管理

本短大の保有する情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ等、情報システムを設置する区域への不正な立ち入り、情報資産、通信回線への損傷・妨害から保護するために、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関する権限や責任を定め、教職員等及び外部委託事業者にセキュリティポリシーの内容を周知徹底するなど、十分な教育及び啓発を行う等の人的な対策を講じる。

(5) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。

7 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9 情報セキュリティ対策基準の策定

短大の様々な情報資産について、情報セキュリティ対策等を講ずるにあたっては、具体的な遵守事項及び判断基準等を統一的なレベルで定める必要がある。よって、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短大情報セキュリィ対策基準を策定するものとする。

10 情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本学園の運営に重大な支障を及ぼすおそれがあることから非公開とする。

11 教職員の責務

学長をはじめとして短大が保有する情報資産を取り扱う全ての教職員等及び外部委託業者は、情報セキュリティの重要性について共通の認識を持つとともに業務の遂行に当たって短大セキュリティポリシーを遵守する責務を負うものとする。また、セキュリティポリシーに基づいた短大情報セキュリティ実施手順を遂行する責務を負うものとする。

12 学生への対応

短大が保有する情報資産を取り扱う全ての教職員等は、授業又は教育目的で情報資産

の使用を学生に認める場合は、遵守すべき事項を学生に明示しなければならない。

附則

本規則は、平成２８年４月１日より施行する。