学校法人冲永学園 情報セキュリティポリシー

1. 目的

教育機関における情報の高度化、有用性に鑑み、学校法人冲永学園（以下「本法人」という）が、教育活動および法人運営を円滑に行い、広く社会に貢献するためには、情報システムの整備と情報セキュリティの確保が必要不可欠である。本法人では、情報セキュリティの重要性を認識し、情報システムの運用および管理に取り組むため、「学校法人冲永学園情報セキュリティポリシー（以下、本ポリシーという）」を定める。なお、本ポリシーは情報セキュリティの基本方針を定めるもので、実施のための対策基準、実施手順は、別途定めるものとする。

2. 基本方針

(1) 本法人の情報セキュリティに対する侵害の阻止
(2) 学内外の情報セキュリティを侵害する行為の抑止
(3) 情報資産の分類と管理・運用
(4) 情報セキュリティ侵害の早期検出と迅速な対応の実現
(5) 情報セキュリティの評価と更新

3. 対象範囲および対象者

本ポリシーが適用される対象範囲および対象者は次のとおりとする。

(1) 対象範囲

本ポリシーの対象範囲は、本法人が管理するすべての情報資産である。

情報資産には、本法人が所有する、もしくは本法人のネットワークに接続する情報システム、情報システム内部に記録された情報、またその情報を書き出した書面や記録媒体を含む。

本法人以外に保管される情報資産であっても、保有する情報資産と認められるものは対象とする。

(2) 対象者

本ポリシーの対象者は、役員、教職員(非常勤を含む)、その他本法人の業務に従事するすべての者とする。また、本法人の情報システムまたは情報資産を利用する園児、児童、生徒、学生、委託業者、来学者その他法人が利用を許可したすべての者については、その利用形態に応じた情報セキュリティ上の措置を適用する。

4. 組織・体制

本法人は、情報セキュリティを組織的に運用および管理する体制を確立するため、次のとおり、その役割と責任を定める。

(1) 情報セキュリティ最高責任者(CISO)

本法人に、情報セキュリティ最高責任者(Chief Information Security Officer。以下「CISO」という)を置く。

CISOは、適切な情報セキュリティ対策を図るための権限および責任を有する。

(2) 情報セキュリティ実施責任者

対象者に本ポリシーの内容を周知徹底し、情報セキュリティを長期的に維持するために、情報セキュリティ実施責任者（以下、実施責任者という）を置く。実施責任者は、本法人全体の情報システムを管理する者で、CISOの指示により情報セキュリティに関する権限や責任を定め、また、十分な教育および啓発が行われるよう必要な対策を講じる。

(3) 情報セキュリティ管理責任者

各学校、園および事務部門等における情報セキュリティを運営、管理するために、情報セキュリティ管理責任者（以下、管理責任者という）を置く。

管理責任者は、各学校、園および事務部門等における情報セキュリティに関する権限と責任を有し、当該部局の個々の情報機器、ソフトウェアおよび情報を管理、監督する。

5. 対象者の義務

すべての対象者は、本ポリシーの他、実施のための対策基準、実施手順を遵守しなければならない。

(1) 対象者の一般的な義務

ア. 対象者は、情報セキュリティを損ねる行為をしてはならない。

イ. 実施責任者もしくは管理責任者から、セキュリティ維持管理のために協力を依頼された場合には従わなければならない。

ウ. 情報セキュリティに関する事故やシステム上の障害を発見した場合には、実施責任者または管理責任者に直ちに報告しなければならない。

エ. 個人、所属部署、学級、研究室等その他対象者が直接管理する情報資産については、各対象者がそのセキュリティに関する責任を負うものとする。

(2) 情報セキュリティ管理責任者

教育、研究、事務等の各情報セキュリティ管理責任者は、学内外から情報システムの不正使用やデータの不正な利用等にかかわる通報等があった場合には、速やかに調査を行うものとする。

(3) 情報セキュリティ実施責任者

前号による調査の結果、不正が確認されたときは、別に定める実施手順等に基づき、関係する通信の遮断、該当する情報システムの切り離し等の必要な措置を講ずるものとする。

6. 情報セキュリティに対する侵害の抑止等

本法人は、学内外を問わず、次のとおり人的または電子的な情報の侵害の抑止を行う。

(1) 情報セキュリティを侵害する行為の抑止

学内外を問わず、あらゆる組織、団体、個人等の情報資産を侵害してはならない。

(2) アクセス制御

情報の内容に応じて利用者ごとのアクセス権限を定め、不正なアクセスを防止するための適切なアクセス制御を行わなければならない。すべての利用者は、アクセス権限のない情報や、許可されていない情報を利用してはならない。

7. 情報資産の分類と管理・運用

本法人は、情報資産が果たすべき役割と影響を十分に認識し、次のとおり常にその機密性、完全性、可用性に配慮して適切に分類し、管理する。

(1) 機密性

ある情報に対し認められた者だけがアクセスでき、その状態を確保する。

(2) 完全性

情報が破壊、改ざん、または消去されていない状態を確保する。

(3) 可用性

情報へのアクセスを認められた者が、必要な時に情報にアクセスできる状態を確保する。

8. 情報セキュリティ侵害の早期検出と迅速な対応の実現

本法人は、各種情報システムのアクセスログ等の情報を定期的に確認し、情報セキュリティ侵害の早期検出に努める。また、インシデント発生時の体制を整備し、事案発生のときは、迅速かつ適切な対応を実現する。

9. 法令等の遵守および違反への罰則

情報資産の取り扱いに関しては、法令および規制等についても遵守する必要がある。本ポリシーならびに本ポリシーに基づく対策基準、実施手順に対する違反があった場合の罰則については、別に定める学内規則等に従い対処する。

10. 本ポリシーの評価と更新

本ポリシーに基づく情報セキュリティ対策については、その実効性を定期的に評価し、改善が必要と認められた場合は、速やかに更新する。

以上

2026 年 10 月制定