学校法人ソニー学園情報セキュリティポリシー

情報セキュリティ基本方針

2020 年 4 月 1 日制定

学校法人ソニー学園（以下「本学園」という。）が設置する湘北短期大学（以下「大学」という。）の理念と使命の実現に向けて教育研究活動を円滑に行い、広く社会に貢献していくためには、本学園が保有する情報資産の保護、活用及び情報セキュリティの維持、推進が必要不可欠である。

本学園は、情報システムの運用及び管理について必要な事項を、「学校法人ソニー学園情報セキュリティポリシー」（以下「本ポリシー」という。）として定め、本学園及び大学のすべての構成員が情報セキュリティの重要性を認識するとともに、本学園の情報システムの整備及び情報セキュリティの確保を本ポリシーに基づき継続的かつ発展的に推し進めるものとする。

１．本ポリシーの構成

本ポリシーは、「情報セキュリティ基本方針」「情報セキュリティ規程」及びこれに基づいて定める細則、要綱等で構成する。

２．目的

本ポリシーの目的は、次の各号のとおりとする。

（１）本学園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損ねる行為の抑止
（３）情報資産の分類と管理
（４）情報セキュリティ侵害の早期検出と迅速な対応
（５）情報セキュリティインシデントへの対処
（６）情報セキュリティの評価と更新

３．対象範囲及び対象者

本ポリシーの対象範囲は、本学園が管理する全ての情報資産とする。また、本ポリシーは、本学園の情報資産を利用する全ての者（以下「対象者」という。）で、本学園の役員、評議員及び職員並びに大学の教育職員（非常勤教員を含む。）、事務職員（非常勤職員、派遣職員等を含む。）及び学生（学科生、科目等履修生等）を対象とする。

４．組織・体制

本学園は情報セキュリティを推進する組織・体制として、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者、情報セキュリティ管理責任者、情報セキュリティ管理者を置き、その権限及び責任を明確にする。

５．情報の分類と管理

本学園における情報資産は、機密性、完全性及び可用性を踏まえ、その情報資産の重要度に応じて分類し、それに基づいた管理方法を定める。

６．情報セキュリティ対策

次の対策を実施する。

①物理的セキュリティ対策

本学園における情報資産の保管場所や情報システムの設置場所について、不正な立ち入りや災害等から情報資産を保護するために、入退室管理、施錠、耐火耐震対策等の必要な対策を講じ、また、サーバ機器への物理的接触やクライアント機器の持出、持ち込みへの制限、加えて情報機器の廃棄による情報流出を防ぐための対策を講じること。

②人的セキュリティ対策

本ポリシーが遵守されるよう関連諸規程を整備し、対象者に対して、本ポリシーの周知と遵守のための教育・研修を実施するとともに、情報セキュリティインシデントの報告、対応のために必要な体制を整備すること。

③技術的セキュリティ対策

本学園の情報システムを学内外からの不正なアクセスから保護するために、また、情報システムを通じて情報が改ざんされ又は漏洩すること等を防止するために必要な対策を講じること。

７．対象者の遵守事項

全ての対象者は、本ポリシーを遵守しなければならない。これに違反した者に対しては、就業規則等の定めるところに従い処分を行う。

８．本ポリシーの評価・見直し

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

学校法人ソニー学園情報セキュリティポリシー

情報セキュリティ規程

第１章 総則

（趣旨）

第１条 この規程は、情報セキュリティ基本方針に基づき本学園の情報セキュリティ対策を講ずるにあたり、遵守すべき行為及び判断等の基準を統一し、必要となる基本的な基準（以下「対策基準」という。）を定めるものである。

（用語の定義）

第２条 この規程で使用する用語の定義は、次の各号のとおりとする。なお、この規程で使用する語句の定義は、この規程で定めるものを除き、「情報セキュリティ基本方針」の定義と同じとする。

（１）情報システム

情報ネットワークに接続する機器を含む、情報処理及び情報ネットワークに係るシステムで、次のものをいう。

ア　本学園が所有又は管理するもの

イ　契約又は協定等に基づき他から本学園に提供されるもの

（２）情報

情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

（３）情報資産

情報システム並びに情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

（４）実施手順

情報セキュリティ対策を実施するため、この規程に基づいて適宜策定される細則、要綱をいう。

（５）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。

なお、「機密性」とは情報資産にアクセスすることを許可された者だけが情報資産にアクセスできることを確保することをいい、「完全性」とは情報資産が破壊、改ざん又は消去されていない状態を確保することをいい、「可用性」とは情報資産にアクセスすることを許可された者が必要なときに情報資産にアクセスできることを確保することをいう。

（６）情報セキュリティインシデント

意図的又は偶発的に生じる、本学園の情報セキュリティを脅かす事故、事件及び公開情報の改ざん等をいう。

（７）CSIRT

情報セキュリティインシデントに対処するため設置する組織をいう。

Computer Security Incident Response Team の略。

（８）情報機器

パソコン、サーバ及びスマートデバイス等のコンピュータ本体及びディスプレイ、プリンタ等の周辺機器をいう。

（９）サーバ機器

複数のクライアント機器からアクセスされ、共同で利用される情報機器をいう。

（10）クライアント機器

サーバ機器の提供する機能やデータへアクセスすることで処理を進めていく情報機器をいう。

（11）記録媒体

電磁的に情報を記録した媒体及び情報をプリントアウトした紙媒体等をいう（ＣＤ、ＤＶＤ、フラッシュメモリ、外付けハードディスク等)。

（12）部門

大学の各学科、各センター、図書館及び事務局各部・課・室（部の下部組織である課、室を除く）をいう。

第２章 情報セキュリティの管理体制

（組織・体制）

第３条 本学園の情報基盤を整備し、情報資産の有効活用・セキュリティ確保を実現するための体制として、最高情報セキュリティ責任者、最高情報セキュリティ副責任者、情報セキュリティ管理責任者、情報セキュリティ管理者及び監査責任者を置き、情報セキュリティ担当部署及び情報セキュリティインシデント対応チーム（以下「CSIRT」という。）を設置する。

（最高情報セキュリティ責任者及び最高情報セキュリティ副責任者）

第４条　最高情報セキュリティ責任者は、本学園の情報セキュリティに関する総括的な意思決定をし、学内及び学外に対して最終的な責任を負う。

２　最高情報セキュリティ責任者は理事長とする。

３　最高情報セキュリティ副責任者は、最高情報セキュリティ責任者を補佐し、最高情報セキュリティ責任者に事故あるときは最高情報セキュリティ責任者を代行する。

４　最高情報セキュリティ副責任者は学長をもって充てる。

（情報セキュリティ管理責任者）

第５条　情報セキュリティ管理責任者は、最高情報セキュリティ責任者を補佐し、本学園における情報セキュリティ対策の実施・管理に関し、全体を統括する実質的な責任と権限を持つ。

２　情報セキュリティ管理責任者は法人本部長をもって充てる。

（情報セキュリティ管理者）

第６条　情報セキュリティ管理者は、情報セキュリティ管理責任者の指示により、本学園の保有する情報システムの整備及び運用に関して、この規程及びそれに基づく実施手順等が適切に行われていることを管理する。

２　情報セキュリティ管理者は情報システム部長をもって充てる。

３　情報セキュリティ管理者は、情報システムの運用に携わる者及び対象者に対して、情報システムの運用及び利用並びに情報セキュリティに関する教育を企画し、この規程及び実施手順等の遵守を確実にするための教育を実施しなければならない。

（情報セキュリティ担当部署）

第７条　本学園における情報セキュリティ担当部署は、情報システム部セキュリティ推進室とする。

（CSIRT）

第８条　最高情報セキュリティ責任者は、情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため、別に定める細則により CSIRT を設置する。

２　CSIRT は、情報セキュリティインシデントが発生したときは直ちに最高情報セキュリティ責任者へ報告しなければならない。

第３章　情報資産の分類と管理

（情報資産の分類）

第９条　本学園における情報資産は、機密性、完全性及び可用性を踏まえ、その情報資産の重要度に応じて、次の各号に定めるとおり分類する。

（１）分類Ⅰ　情報セキュリティの侵害が教職員又は学生の生命、財産、プライバシー等へ重大な影響を及ぼすもの

（２）分類Ⅱ　情報セキュリティの侵害が本学園の事務運営及び教育活動の実施に重大な影響を及ぼすもの

（３）分類Ⅲ　情報セキュリティの侵害が本学園の事務運営及び教育活動への影響が軽微であるもの

（４）分類Ⅳ　前各号以外で影響をほとんど及ぼさないもの

（情報資産の管理）

第１０条　前条により分類した情報資産の管理方法については、別に細則に定める。

２　情報資産の管理は、前項に基づき、当該情報資産を作成又は使用する部門が行わなければならない。

第４章　物理的セキュリティ対策

（管理区域の設置）

第１１条 情報セキュリティ管理者は、サーバ機器等の重要な情報システム又は情報資産を、第９条の分類に応じて、それぞれ設定された管理区域内に設置し、正当なアクセス権のない者が使用できないよう、必要に応じて入退室の認証・記録や警備システムの設置等を行い、物理的なセキュリティ確保に努めなければならない。

（情報機器及び記録媒体の盗難対策）

第１２条 対象者は、情報機器及び記録媒体について、定められた盗難予防対策を行わなければならない。

（情報機器及び記録媒体の学外への持ち出し）

第１３条　第９条により分類した情報資産ⅠからⅢに該当する情報が入った情報機器及び記録媒体は、原則として学外へ持ち出してはならない。やむを得ず、情報機器及び記録媒体を学外へ持ち出す場合は、所属する部門の責任者の承認を得るものとし、持出しにあたっては情報の漏えいが発生しないよう、暗号化等の情報セキュリティ対策を講じなければならない。

（情報機器及び記録媒体の学内への持ち込み）

第１４条 情報機器及び記録媒体を学内へ持ち込み使用する場合は、事前にマルウェアに感染していないかのチェックを行う等の情報セキュリティ対策を講じなければならない。

（情報機器及び記録媒体の処分）

第１５条 所定の決裁手続きを経て、情報機器及び記録媒体を破棄する場合は、残存情報が第三者に読み取られることのないよう、情報セキュリティ対策を講じなければならない。

第５章 人的セキュリティ対策

（対象者の遵守事項）

第１６条　対象者は、この規程及び実施手順等を遵守しなければならない。情報セキュリティ対策について不明な点及び遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に報告し、指示を受けなければならない。

（教育・研修）

第１７条　情報セキュリティ管理者は、情報セキュリティに関する啓発や教育を実施するため、必要な研修を実施する等の措置を講じるものとする。

（情報セキュリティインシデントの報告・対応）

第１８条　対象者は、情報セキュリティインシデントを発見した場合には、直ちに情報セキュリティ管理者に報告しなければならない。

２　情報セキュリティ管理者は、発生した情報セキュリティインシデントについて、直ちに必要な措置を講じ、情報セキュリティ管理責任者に報告しなければならない。

３　情報セキュリティ管理責任者は、重大な情報セキュリティインシデントが発生した場合は、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者に報告しなければならない。

４　最高情報セキュリティ責任者は、重大な情報セキュリティインシデントについては常勤理事会に報告するとともに、その対応を審議する必要がある場合は、常勤理事会の議題とするよう要請するものとする。

５　情報セキュリティ管理者は、発生した全ての情報セキュリティインシデントに関する記録を一定期間保存しなければならない。

（委託契約）

第１９条 情報システムの開発又は運用管理を外部委託する場合は、外部委託業者から再委託を受ける業者も含め、情報セキュリティを遵守することを明記した契約を締結しなければならない。

第６章 技術的セキュリティ対策

（ネットワークの運用管理）

第２０条　情報セキュリティ管理者は、ネットワークついて、ファイアウォール等のセキュリティ対策機器を導入し、外部からの不正アクセス等に対する防御や内部から外部への攻撃に対処しなければならない。

２　情報セキュリティ管理者は、情報システムのログを一定期間保存しなければならない。

３　情報セキュリティ管理者は、新たな技術による学内ネットワークへの攻撃に対処できるよう、必要に応じて、セキュリティ対策機器及びセキュリティ対策機器上のソフトウェア（ファームウェアを含む）を更新しなければならない。

４　情報セキュリティ管理者は、本学園のネットワークに所属する情報システムを把握し、適切なセキュリティ対策が講じられていることを確認しなければならない。

５　対象者が本学園のネットワークに情報機器を接続する場合、情報機器にウィルス対策ソフトを導入する等のセキュリティ対策を講じなければならない。

６　前項のセキュリティ対策については、別に定める。

（セキュリティ情報の収集）

第２１条　情報セキュリティ管理者は、セキュリティに関する情報を収集し、セキュリティ対策上必要な措置を講じるとともに、これらの情報を定期的に取りまとめ、それに応じてセキュリティ対策をアップデートしなければならない。

（アクセス制限）

第２２条　情報セキュリティ管理者は、情報の内容に応じて、アクセス可能な対象者を定め、不正なアクセスを阻止するために必要なアクセス制限を行わなければならない。

２　対象者は、アクセス権限のない情報にアクセスしたり、許可されていない情報を利用してはならない。

（バックアップ管理）

第２３条　情報セキュリティ管理者は、機密情報等を保持しているサーバ等に記録された情報について、その重要度に応じて期間を設定し、定期的にバックアップ用の複製をとらなければならない。

（不正アクセス等への対応）

第２４条　情報セキュリティ管理者は、不正アクセスの防止並びに検出するための適切な手段を講じなければならない。不正アクセスが検出された場合は、関連する通信の遮断又は該当する情報機器の切り離しを実施する。

（利用記録の保存）

第２５条　情報セキュリティ管理者は、外部からアクセス可能なサーバ、個人情報等を管理するサーバ及び教職員が業務上利用する情報機器について、システムログや利用ログ等の運用に関する記録を一定期間保存しなければならない。また、最高情報セキュリティ責任者及び最高情

報セキュリティ副責任者、情報セキュリティ管理責任者から運用に関する記録の提供を求められた場合は、速やかに開示しなければならない。

（アカウント及びパスワードの整備）

第２６条　対象者は、自己のアカウントのパスワードを秘密としなければならない。又、十分なセキュリティを維持できるよう、自己のパスワードの設定及び変更に配慮しなければならない。

第７章 評価・見直し

（情報セキュリティ対策の点検）

第２７条　情報セキュリティ管理者は、情報資産に係る物理的・技術的・人的セキュリティ対策について点検を実施し、結果を定期的に情報セキュリティ管理責任者に報告しなければならない。情報セキュリティ管理責任者は、点検結果に問題がある場合は改善を命じ、改善結果を最高情報セキュリティ責任者に報告しなければならない。

（監査責任者）

第２８条　本学園に、最高情報セキュリティ責任者の指名に基づく情報セキュリティ管理責任者及び情報セキュリティ管理者から独立した監査責任者を一人置き、本学園における情報セキュリティの対策状況について、定期的に監査する。

２　監査責任者は、監査結果を最高情報セキュリティ責任者及び最高情報セキュリティ副責任者に報告するものとする。

（情報セキュリティ対策の更新）

第２９条　最高情報セキュリティ責任者は、前条の報告により、改善が必要と認められる場合には、情報セキュリティ管理責任者に対して、情報セキュリティ対策の更新等、必要な措置を講じるよう命じなければならない。

（ポリシーの評価）

第３０条　本ポリシーの実効性については、定期的に評価を行い、改善が必要と認められる場合には、セキュリティレベルの高い、かつ遵守可能なポリシーに更新しなければならない。

第８章　その他

（改廃）

第３１条　この規程の改廃は、常勤理事会の議を経て、理事長が決裁する。

附則

１．この規程は、２０２０年４月１日から施行する。