学校法人 悠久崇徳学園　情報セキュリティ対策基準

1　目的

情報セキュリティ対策基準（以下「本対策基準」という。）は、学校法人悠久崇徳学園（以下「法人」という。）の情報セキュリティ基本方針に基づき、法人の情報セキュリティの維持・向上を図るための体制及び教育等に関し、必要な事項を定めるものとする。

2　定義

情報セキュリティポリシーにおいて、次の各号に掲げる用語の定義は、該当各号に定めるとおりとする。

（1）　情報資産

情報が記録されたデータ（記録された媒体は問わない。）及びデータにアクセスするための情報システム（ハードウェア、オペレーティングシステム、ソフトウェア、ネットワーク等）をいう。

（2）　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。

① 機密性

情報の利用を認められた者だけが、情報を利用できる状態を確保することをいう。

② 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。

③ 可用性

情報の利用を認められた者が、必要なときに中断されることなく利用できる状態を確保することをいう。

3　対象とする脅威

（1）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正、オンラインバンキング不正送金、ネット犯罪被害及び加害等

（2）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、システム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

4　管理体制

（1）　情報統括責任者

法人事務局長を情報統括責任者とする。情報統括責任者は、法人における全ての情報システ

ム、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） 情報セキュリティ責任者

大学事務局長を情報統括責任者直属の情報セキュリティ責任者とし、法人における情報セキュリティ対策に関する運用、評価、維持する権限および責任を有する。

（3） 情報システム管理者

危機管理部門に相当する職員を情報システム管理者とし、法人の情報システムにおける導入、設定の変更、運用、更新等を行う権限及び責任を有し、情報システムに対する情報セキュリティ対策の実施に関する権限及び責任を負う。

（4） 情報セキュリティ管理者

学長又は学校長を情報セキュリティ管理者とし、情報セキュリティ責任者の指示等に従い、事業所内の情報資産に関する情報セキュリティ実施手順の維持・管理を行う。

また、その所掌する事業所において、情報資産に対する侵害が発生した場合又は侵害の恐れがある場合には、情報セキュリティ責任者及び情報システム管理者へ速やかに報告し、指示を仰がなければならない。

5 情報資産の分類と管理

（1） 情報資産の分類

法人における情報資産は、機密性、完全性及び可用性により、下記のとおり、必要に応じ取扱制限を行うものとする。

・外部記録媒体等の記録、持ち出し
・私物情報機器の接続
・情報の送信
・必要以上の複製及び配付
・アクセス制限　　等

（2） 情報資産の管理

教職員等は、その所管する情報資産について、次のとおり適切な管理を行わなければならない。また情報セキュリティ管理者は、その情報資産について管理責任を有する。

① 情報の作成

（ア） 教職員等は、業務上必要のない情報を作成してはならない。

（イ） 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

② 情報資産の入手

（ア） 教職員等が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取り扱いをしなければならない。

（イ） 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

③ 情報資産の利用

（ア） 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

④ 情報資産の保管

（ア） 情報セキュリティ管理者又は情報システム管理者は、~~情報資産の分類に従って、~~情報資産を適切に保管しなければならない。

（イ） 情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した外部記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ） 情報セキュリティ管理者又は情報システム管理者は、バックアップで取得したデータを記録する外部記録媒体を長期保管する場合は、自然災害を被る可能性が低い場所等の安全な場所に保管しなければならない。

⑤ 情報の送信

電子メール等により情報を送信する者は、必要に応じて暗号化又はパスワード設定を行わなければならない。

⑥ 情報資産の運搬

（ア） 車両等により情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ） 情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑦ 情報資産の提供・公表

（ア） 情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ） 情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

（ウ） 情報セキュリティ管理者は、外部に公開する情報資産について、完全性を確保しなければならない。

⑧ 情報資産の廃棄

（ア） 情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

（イ） 情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

（ウ） 情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

6　物理的セキュリティ

（1）　機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（2）　サーバの冗長化

【望ましい対策】

情報システム管理者は、重要情報を格納しているサーバを冗長化し、同一データを保持しなければならない。

（3）　機器の電源

情報システム管理者は、サーバ等の重要機器の電源について、停電等による電源供給の停止や落雷等による過電流に備え、当該機器が安全に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（4）　機器の搬入・修理・搬出

①サーバ等の重要機器を外部事業者が搬入及び搬出する際は、情報システム管理者が指名した職員が、必ず立ち会わなければならない。

②修理等で情報を記録した機器を外部に持ち出す際は、委託する事業者との間で守秘義務契約を締結する他、秘密保持体制の確認などを行わなければならない。

（5）　機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

7　人的セキュリティ

（1）　教職員等の基本遵守事項

① 教職員等は、情報セキュリティ対策基準を遵守しなければならない。また、情報セキュリティ対策について不明な点、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相談し、指示を仰がなければならない。

②教職員等は、業務以外の目的で、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③教職員等は、私物パソコンを持ち込み、法人のネットワークに接続してはならない。使用できるパソコンは、法人が支給又は貸与し、かつ使用を許可したパソコンのみとする。

④教職員等は、許可を得ずにパソコン等の端末、USB メモリや CD/DVD などの記録媒体、情報資産及びソフトウェアを外部に持ち出してはならない。

⑤教職員等は、自己の管理するＩＤ／パスワードについて、不用意に他に漏らしたり、メモを

他者の目の触れる場所に放置しないなど秘密保持に努めなければならない。

⑥教職員等は、業務上知り得た情報を他に漏らしてはならない。

⑦教職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合や外部から指摘を受けた場合、速やかに情報セキュリティ管理者に報告しなければならない。

⑧教職員等は、情報セキュリティポリシーに反する行為を発見した場合、直ちに情報セキュリティ管理者に報告を行わなければならない。

⑨教職員等は、職務の遂行において使用する情報資産を保護するために、関係法令を遵守し、これに従わなければならない。

（２）　情報システムの運用にあたっての留意事項

（データの取扱いに関する留意事項）

①教職員等は、業務上必要なファイルをファイルサーバ等の適切な情報システムに保管しなければならない。

②教職員等は、情報システムに正しいデータが入力され、正しく処理されていることを確認しなければならない。

③教職員等は、パソコン等の端末や記録媒体、印刷物等を第三者に使用や閲覧されることがないように、離席時には端末のロックや記録媒体、印刷物等を容易に閲覧できない場所への保管等、適切な措置を講じなければならない。

（インターネット利用に関する制限事項）

④教職員等は、就業時間外であっても業務目的以外のインターネット利用やメール利用を慎まなければならない。

⑤教職員等は、有害なサイト、違法なサイト、悪質なサイト、ウェブメール、無許可のクラウドサービス等にアクセスしてはならない。

（電子メール利用に関する制限事項）

⑥教職員等は、不審なメールや身に覚えがないメールが届いた場合は、添付ファイルは開かず、受信した旨を職場内の周囲に注意を促し、直ちに廃棄しなければならない。

８　技術的セキュリティ

（１）　情報システムの管理

①情報システム管理者は、情報システムの諸元等を記した管理表を作成し、常に最新の状態に更新するように努めなければならない。

②情報システム管理者は、管理表を業務上必要とする者のみが閲覧できる状態にし、紛失等がないよう、適切に管理しなければならない。

（２）　ソフトウェア導入に関する制限事項

①情報システム管理者は、ＯＳやソフトウェアのバージョンとライセンスを適切に管理しなければならない。

②正規のライセンスのないソフトウェア、業務上不必要なソフトウェア、出所不明なソフトウェア、安全性が確認されていないソフトウェアは導入してはならない。

（3） アクセス制御

（外部ネットワークへのアクセス制御）

【望ましい対策】

①情報システム管理者は、有害なサイト、違法なサイト、悪質なサイト等にアクセスできないよう技術的措置を講じなければならない。

（内部ネットワークへのアクセス制御）

②情報システム管理者は、外部から内部ネットワークに不正にアクセスされることがないように技術的措置を講じなければならない。

③情報システム管理者は、無線によるネットワークを導入する場合は、外部から不正にアクセスされることがないように技術的措置を講じなければならない。

④情報システム管理者は、学生等が利用するネットワークについては、内部ネットワークとは物理的に分けて管理しなければならない。

（機密ファイルへのアクセス制御）

⑤情報システム管理者は、機密性が高いファイルにはアクセス権を設け、担当職員以外の職員等がアクセスできないように技術的措置を講じなければならない。

（4） バックアップの実施

情報システム管理者は、ファイルサーバ等に記録された情報について、定期的にバックアップを実施しなければならない。

9 運用

（1） 情報セキュリティポリシーの遵守状況の確認

①情報システム管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに情報セキュリティ責任者に報告しなければならない。

②情報セキュリティ責任者は、発生した問題について問題を認めた場合には、速やかに情報統括責任者に報告し、適切かつ速やかに対処しなければならない。

（2） 侵害時の対応

①情報統括責任者は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において、関係者への連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に対処しなければならない。

② 個人情報の漏洩等が発生し個人の権利利益を害する恐れがある場合、情報セキュリティ責任者は情報統括責任者へ報告及び本人への通知を行う。

③侵害時に適切に対処するため、緊急時の対応手順等を定め準備しておかなければならない。
④法人が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、情報統括責任者は、当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

附則

この対策基準は、2023 年 4 月 1 日から施行する。