令和3年4月1日
情報管理室作成

米子工業高等専門学校情報セキュリティ実施手順

1．目的

情報を不適切に取り扱うことにより，機密性が求められる情報の漏えい，完全性が求められる情報の改ざん等が生じた場合には，学校業務の停止や社会的信用の失墜の要因となる可能性もある。

本手順書は，このようなリスクを軽減するため，教職員等が情報を適切に取り扱うために必要な事項を定めることを目的とする。

2．定義

この手順における用語の定義は，米子工業高等専門学校情報セキュリティポリシー及び米子工業高等専門学校情報セキュリティ管理規程の定めるところによる。

3．対象者

本手順は，米子工業高等専門学校に設置する情報システムを取り扱うすべての教職員を対象とする。

4．実施体制

情報セキュリティ責任者…校長
情報セキュリティ副責任者…情報管理室長，事務部長
情報セキュリティ推進責任者…情報管理室長
連絡・通報・書類提出窓口…情報管理室

5．情報の取扱いに関する全般的な注意事項

（1）情報の作成，入手及び利用は学校業務目的の範囲内で行うこと。
（2）盗難や盗み見（業者や保護者・来校者・学生）による情報遺漏を防ぐために，机上に個人情報等を放置しないようにすること。（名簿，採点済みのテスト，住所録，成績資料等）
（3）離席する際，デスクトップパソコンについてはスクリーンセーバー等でパソコンロックし，ノートパソコンについてはふたを閉じておくこと。
（4）重要資産を廃棄する際には，廃棄するまで施錠管理された場所で保管し，裁断，溶解等で，情報が判読できないように処理すること。
（5）プリンター，コピー，ＦＡＸから出力された文書は速やかに回収すること。
（6）重要な情報が記載されている用紙を，裏紙として再利用しないこと。
（7）個人情報，ＩＤ・パスワード等は，周囲に漏れることのないようにすること。
（8）やむを得ず外部に重要な情報を持ち出すときは，必ず情報セキュリティ推進責任者の許可を得ること。また，外出時の行動については「6．情報資産の持ち出しについて」に従って行動すること。

6．情報の持ち出しについて

（1）学校業務の遂行以外の目的で，重要な情報を学外に持ち出さないこと。
（2）学外に重要な情報を持ち出す場合は，必ず事前に情報セキュリティ推進責任者の許可を得ること。
（→情報管理室に「情報持ち出し許可申請書」（別紙１）を提出し，許可を得ること）

（3）持ち出し時は，盗難・紛失等の情報遺漏リスクを常に意識し，手元から離さないように注意すること。
（4）重要な情報を学外に送信する場合には，以下の方法を用いて当該情報を保護すること。
①通信路の暗号化
②ファイルの暗号化
（5）重要な情報を学外に送信する場合で，改ざんされるおそれが大きく，業務の遂行に影響を与える可能性が高いと判断されるときは，保存されている当該情報に電子署名を付与することが望ましい。
（6）記録媒体内のデータについては，パスワードを設定する等セキュリティ対策を施すこと。また、持ち出し先においても学内と同様に情報を取扱い，学外（自宅等）で利用するパソコンについてもセキュリティ対策を施すこと。
学校外で利用するパソコンについてのセキュリティ対策については「７．私物パソコン等で校内情報を扱う場合のセキュリティ対策」に従うこと。
（7）返却時は，持ち出した情報がすべて揃っているかどうか確認すること。不足があることが分かった場合は、直ちに情報管理室に報告すること。

７．私物パソコンで校内情報を扱う場合のセキュリティ対策

（1）ウイルス対策ソフトをインストールし（体験版不可），自動アップデートを施し常に最新の状態を保つこと。ウイルススキャンを適時に自動で行う設定にすること。
（2）Windows Update 等が行なわれ，最新の状態であること。
（3）個人情報等の重要な情報のハードディスク内への複写，保存は禁止する。
（4）ファイル交換ソフト（Winny 等）がインストールされていないことを確認すること。インストールされている場合は，重要な情報を扱わないこと。

８．私物パソコンの持ち込みについて

（1）個人所有の情報システム機器を持ち込む場合は，事前に情報管理室に「私物パソコン使用申請書」（別紙２）を提出すること。
（2）私物パソコンは教職員ネットワークや業務用ＰＣには接続しないこと。
（3）ウイルス対策ソフトをインストールし（体験版不可），自動アップデートを施し常に最新の状態が保たれていること。ウイルススキャンを適時に自動で行う設定にすること。
（4）Windows Update 等が行なわれ，最新の状態であること。
（5）個人情報等の重要な情報のハードディスク内への複写，保存は禁止する。

９．外部アクセスサーバの設置について

（1）外部からアクセス可能なサーバを校内に設置する場合は，必ず事前に情報セキュリティ推進責任者の許可を得ること。
（→情報管理室に「外部アクセスサーバ設置申請書」（別紙３）を提出し，許可を得ること）
（2）学校業務の遂行以外の目的で，外部アクセスサーバを使用しないこと。

１０．情報システム機器利用時の遵守事項

（1）ハードウェアは無断で改造したり，他のネットワークに接続したりしないこと。
（2）ＯＳやソフトウェアにはセキュリティホールという情報セキュリティ上の欠陥が発見されることがあるため，迅速に最新バージョンへの更新やセキュリティパッチ（修正プログラム）を適用すること。
（3）私物のＵＳＢメモリー等外部記憶装置の移動媒体も，随時ウイルスチェックを行うこと。

11. 離席時の対策

（1）長時間離席する場合は，ファイルや使用ソフトは閉じること。開いたまま離席しないこと。
（2）使用しているＵＳＢメモリー等外部記憶装置を，忘れずに取り外して持って行くこと。
（3）自席のＰＣは，パスワード付きスクリーンセーバー等の設定や起動時のパスワード設定等を施し，他人に勝手に使用されないように注意すること。ノートパソコンのふたは閉じて離席すること。
（4）パソコンに重要データを表示している場合は，他人に盗み見されないよう周囲に配慮すること。

12. ソフトウェアの取り扱い

（1）私用ソフトをインストールしないこと。
（2）ソフトウェアの違法コピーを行わないこと。
（3）学校がライセンス所有するソフトウェアを個人所有のパソコンにインストールしないこと。

13. インターネット利用時における遵守事項

（1）職務に関係の無いホームページの閲覧を行わないこと。
（2）ホームページに記載されている情報を全て信用しないこと。
（3）アクセスしたホームページが有料か無料かの確認を行うこと。
（4）インターネットからむやみにファイルのダウンロードを行わないこと。（業務上必要なものに限る）
（5）インターネットの掲示板等に書き込みを行わないこと。

14. 電子メール利用時における遵守事項

（1）職務以外の目的で電子メールを使用しないこと。
（2）学校メールアドレス（学校管理の個人，役職，部署等のメールアドレス）以外は使用しないこと。
（3）送信時には「内容」「宛先」の確認を行うこと。
（4）個人加入のメールアドレスへむやみに転送しないこと。
（5）不審なメールは，開封したり，添付ファイルを実行したりせず，迷惑メールフォルダに移動するか削除すること。

15. コンピュータウイルスに対する遵守事項

（1）校務用パソコンでは，指定されたウイルス対策ソフトを使用すること。
（2）コンピュータウイルス対策ソフトの定義ファイルは常に最新の状態を保つこと。（自動アップデートを施すこと）
（3）身に覚えのない人から送信された電子メールファイルや添付ファイル，ダウンロードや外部から持ち込まれたプログラムなどを開く場合は，開く前にウイルスチェックを行うこと。
（4）ウイルス感染被害に備え，必要に応じて日頃からバックアップを行っておくこと。
（5）ウイルス感染の可能性が発覚した場合，直ちにそのパソコンからＬＡＮケーブルをすぐに外し（無線 LAN の場合は，無線 LAN 用のユニットを取り外すか，電源を切る），情報管理室に連絡をすること。その際に使用していたＵＳＢメモリー等外部記憶装置を他で使用せずに隔離して，情報管理室の指示に従うこと。

16. インシデントの可能性を発見した場合の手順

インシデントの可能性を発見した場合は，「米子工業高等専門学校インシデント対応について」に従い，すぐに情報管理室へ報告すること。

17. 本手順書に関する相談窓口

（1）教職員等は，緊急時の対応又は本手順書の内容を超えた対応が必要とされる場合には，情報管理室に相談し、指示を受けること。

（2）教職員等は，本手順書の内容について不明点等がある場合には，情報管理室に問い合わせし，回答を得ること。

（窓口：情報管理室 内線５０２８）