広島県教育委員会情報セキュリティ基本方針

第１　目的

基本方針は、県教育委員会が保有する情報資産の機密性、完全性及び可用性を維持するため、情報資産の取扱い等の情報セキュリティ対策の基本的な考え方及び方策を定め、県教育委員会における情報資産の管理を徹底することを目的とする。

第２　対象機関

対象となる機関は、県教育委員会事務局並びにこれに属する地方機関、教育機関、県立学校及び県教育委員会が運営する情報システムを利用する市町立学校等とする。

第３　用語の定義

１　情報

情報システムで取り扱う電磁的データをいう。

２　情報資産

本基本方針が対象とする情報資産は、情報及び情報を管理する仕組み（情報システム並びに情報システムの開発、運用及び保守のための資料等を含む。）をいうものとし、これらに該当しない文書は、文書管理に係る規則及び規程等により適正に管理するものとする。

３　情報システム

コンピュータのハードウェア・ソフトウェア、ネットワーク及び記録媒体等で構成されるものであって、これら全体で業務処理を行うための情報処理の体系をいう。

４　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。

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。

６　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。

７　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。

８　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、情報にアクセスできる状態を確保することをいう。

第４　教職員の遵守義務

県教育委員会の保有する情報資産に関する業務に携わるすべての教職員及び事務局職員（以下「教職員」という。）は、情報セキュリティの重要性についての共通の認識を持つとともに、業務の遂行に当たってはセキュリティポリシー及び実施手順を遵守する義務を負う。

なお、幼児・児童・生徒（以下「児童生徒等」という。）に情報資産を利用させるに当たっては、各実施機関の長の責務として、ネットワーク利用のルールやマナーを児童生徒等に

指導しなければならない。

第５　情報セキュリティ管理体制

県教育委員会の保有する情報資産について、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

第６　情報資産の分類

情報資産について、機密性、完全性及び可用性に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

第７　情報資産への脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施するものとする。

１　部外者の侵入、不正アクセス、コンピュータウイルス等不正プログラム（以下「ウイルス」という。）による攻撃、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、不当な目的による利用等

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、プログラム上の欠陥、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、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、火災等の災害並びに事故、故障等によるサービス及び業務の停止

第８　情報セキュリティ対策

第７で示した脅威から情報資産を保護するために、次のセキュリティ対策を講じるものとする。

１　物理的セキュリティ対策

情報システムを設置する施設への不正な立入りの防止や、パソコン等の機器及び記録媒体等の適切な管理など、情報資産を損傷・妨害等から保護するために物理的な対策を講じる。

２　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、教職員に基本方針及び情報セキュリティに関する法令等の内容を周知徹底するなど、十分な教育及び啓発が行われるよう必要な対策を講じる。

３　技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、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等の技術的な対策を講じる。

４　運用

各種対策の実施状況を確認するため、情報システムの監視、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の運用面の対策を講じる。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

５　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者において必要なセキュリティ対策が確保され

ていることを確認する等の必要な措置を講じる。また、外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

第９　対策基準の策定

第８の情報セキュリティ対策を講じるに当たって、遵守すべき行為、判断等の基準を統一的に定めるため、必要となる基本的な要件を明記した対策基準を策定するものとする。

なお、対策基準は公にすることにより本県の学校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。

第 10　実施手順の策定

セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の情報システムについて具体的な手順を明記した実施手順を策定するものとする。

なお、実施手順は公にすることにより本県の学校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。

第 11　情報セキュリティ監査及び自己点検の実施

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。

第 12　評価及び見直し

情報セキュリティ監査及び自己点検の実施による検証結果等を踏まえるとともに、情報セキュリティを取り巻く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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等のリスクを検討したうえで、セキュリティポリシー及び実施手順の見直しを適宜行うこととする。