# 地方独立行政法人愛知県美術館機構情報セキュリティポリシー　基本方針

（目的）

**第１条**　地方独立行政法人愛知県美術館機構情報セキュリティポリシー（以下「ポリシー」という。）は、地方独立行政法人愛知県美術館機構（愛知県美術館、愛知県陶磁美術館及び法人事務局をいう。以下「本法人」という。）における情報セキュリティに対する基本方針を明らかにすることにより本法人が保有する情報資産を様々な脅威から守り、県民の信頼を損なうことなく、円滑に運営することを目的とする。

（定義）

**第２条**　このポリシーにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 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。

(2) 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。

(3) 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。

(4) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(5) 情報資産

次の資産を情報資産という。

イ　コンピュータ、情報システム、ネットワーク及び電磁的記録媒体（以下「記録媒体」という。）

ロ　コンピュータ、情報システム及びネットワークで取り扱う情報（これらを印刷した文書を含む。）

ハ　ポリシー、情報セキュリティ実施手順（以下「実施手順」という。）、情報システム仕様書及びネットワーク構成図等の紙媒体によるシステム関連文書（以下「システム関連文書」という。）

(6) 情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(7) 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。

(8) 端末

ネットワーク又は情報システム（以下「ネットワーク等」という。）の構成要

素のうち、サーバや通信制御機器を除くハードウェアをいう。

(9) モバイル端末

端末のうち、業務上の必要に応じて移動させて使用することを目的としたモバイル機器をいい、機器の形態は問わない。

(10)モバイルルータ

ネットワークパソコンをモバイル端末として使用することができるようにする通信装置をいう。

(11)基幹機器

サーバ、ファイアウォール、ルータ等のネットワーク等を構成する主要な情報機器又は通信制御機器をいう。

(12)情報システム室

全庁的なネットワーク又は重要な情報システムの基幹機器を設置し、当該機器の管理運用を行うための部屋をいう。

(13)特定用途機器

テレビ会議システム、IP 電話システム、ネットワークカメラシステム、測定機器等の特定の用途に使用される情報システム特有の機器で、通信回線に接続されているもの又は記録媒体を内蔵しているものをいう。

(14)業務委託事業者

本法人との契約により、本法人が保有する情報資産を取り扱う業務又は本法人のネットワーク等に係る開発、導入、保守等の業務に携わる者をいう。

(15)外部サービス（クラウドサービス）

事業者等の外部の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

**（基本方針）**

**第３条**　本法人における情報セキュリティ対策は、このポリシーに基づき実施するものとする。

２　ポリシーは、基本方針（本書）及び第７条に基づき定める対策基準で構成する。なお、対策基準は、公にすることにより本法人の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。

**（情報セキュリティ管理体制の確立）**

**第４条**　このポリシーの適正な運用による情報セキュリティの確保を図るため、管理体制を確立するものとする。

**（情報資産の管理）**

**第５条**　本法人が保有する全ての情報資産は、当該情報の重要度を考慮しつつ、このポリシーで定める情報セキュリティ対策を講じる等により適切に管理するものとする。

（対象とする脅威）

**第６条**　情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入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、重要情報の搾取、内部不正等

(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インフラの障害からの波及等

（情報セキュリティ対策基準の策定方針）

**第７条**　次に掲げる情報セキュリティ対策について、総合的かつ具体的に対策基準を定めるものとする。

(1) 人的セキュリティ対策 情報セキュリティに関する管理体制の整備、職員に対する情報セキュリティ研修の実施等の対策、職員の違反行為への対応

(2) 情報資産の管理 情報資産の分類、情報資産の管理

(3) 物理的セキュリティ対策 情報機器又は通信制御機器の損傷、盗難、火災、停電等から情報を保護するための施設整備、入退室管理等の対策

(4) 技術的セキュリティ対策 ネットワーク等に係るアクセス制御、不正アクセス対策、不正プログラム対策、端末又は記録媒体等の管理等の対策

(5) 運用面におけるセキュリティ対策 情報セキュリティに関する情報の収集及び提供、実施手順に関する事項、情報セキュリティ対策推進計画の策定

(6) 業務委託と外部サービスの利用 業者やサービスの選定、契約書に関する事項、関係規程の策定

(7) 評価及び見直し 監査の実施、自己点検

（情報セキュリティ実施手順の策定）

**第８条**　本法人において、このポリシーに基づき実施手順を定め、ネットワーク等に係る情報セキュリティ対策を総合的に実施しなければならない。

（職員等の責務）

**第９条**　職員は、このポリシー及びそれぞれのネットワーク等の実施手順（以下「ポリシー等」という。）を十分理解し、遵守しなければならない。

２　職員等は、業務目的以外の目的で情報資産を利用してはならない。

３　職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た秘密を漏らしてはならない。

**（情報セキュリティ監査及び自己点検の実施）**

**第１０条**　ポリシー等の適正かつ円滑な運用に資するため、情報セキュリティ監査及び自己点検を実施するものとする。

**（情報セキュリティポリシー等の見直し）**

**第１１条**　情報セキュリティ監査及び自己点検の結果、ポリシー等の見直しが必要となった場合及び情報セキュリティに関する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を分析し、リスクを検討したうえで、ポリシー等を見直すものとする。

**附　則**

（実施期日）

この基本方針は、令和８年４月１日から実施する。