みなかみ町情報セキュリティポリシー 概要版

本ポリシーは、みなかみ町が保有する情報資産の機密性、完全性、可用性を確保し、情報セキュリティ対策を総合的かつ体系的に推進することを目的としています。

１）情報資産

情報資産とは、業務を実施するのに必要な情報及びそれを扱う情報システムをいう。

２）適用範囲

本基本方針が適用される行政機関は、町長部局、各行政委員会、議会事務局及び地方公営企業とし、教育委員会所管の学校を除く。

３）情報資産の分類と管理方法

情報資産は、その重要性に応じて「機密性」「完全性」「可用性」の観点から分類され、それぞれに応じた管理が求められる。

《分類》

機密性３：秘密文書に相当する特に高い機密性を要する情報資産。
機密性２：一般に公開することを前提としない情報資産（機密性 3 以外）。
機密性１：機密性 2 または機密性 3 以外の情報資産。
完全性２：誤りや改ざん、消失により住民の権利侵害や業務遂行に支障をきたす情報資産。
完全性１：完全性 2 以外の情報資産。
可用性２：業務上、利用できないことにより住民の権利侵害や業務遂行に支障をきたす情報資産。
可用性１：可用性 2 以外の情報資産。

《主な管理方法》

管理責任：情報セキュリティ管理者が所管する情報資産の管理責任を負い、複製された情報も適切に管理する。
作成・入手・利用：業務上必要な情報のみ作成・入手・利用し、外部からの入手時は分類に基づく取扱制限を適用する。
保管：機密性 2 以上の情報は、施錠可能な場所に保管し、容易に閲覧されないよう管理する。
送受信：機密性 2 以上の情報は、必要に応じてパスワード等による暗号化措置を講じる。
運搬：機密性 2 以上の情報資産を運搬する際は、鍵付きケース等に格納し、不正利用を防止する。
廃棄：情報を復元できない方法で確実に廃棄し、記録を残す。

４）人的セキュリティ

すべての職員等は、情報セキュリティの重要性を理解し、本ポリシーを遵守する義務がある。

《遵守事項》

・情報セキュリティポリシーおよび実施手順を遵守する。
・支給以外のパソコンやモバイル端末等の業務利用は原則禁止。
・業務以外の目的でのウェブ閲覧は禁止。
・情報資産の不正持ち出しや持ち込みは禁止。
・退職時には情報資産を返却し、業務上知り得た情報の秘密を保持する。

《研修・訓練》

定期的に情報セキュリティに関する研修・訓練に参加する義務がある。

《インシデント報告》

情報セキュリティインシデントを認知した場合、速やかに報告する。

《アクセス制御》
IC カード、ID、パスワードの適切な管理と共有禁止。

5）技術的セキュリティ
情報システムやネットワークにおける技術的な側面からセキュリティを確保する。

《コンピュータ・ネットワーク管理》
・サーバの容量設定、バックアップ、ログ取得と分析、障害記録。
・ネットワーク接続の制御（ファイアウォール、アクセス制御、許可なき端末の接続禁止）。
・外部ネットワーク接続時の厳格な許可と監視。
・複合機や IoT 機器のセキュリティ管理。
《電子メールセキュリティ》
・自動転送機能の禁止、誤送信対策、スパムメール対策、暗号化の利用。
ソフトウェア管理
・無許可ソフトウェアの導入禁止、不正コピーソフトウェアの利用禁止。
・不正プログラム対策ソフトの導入と更新、不正アクセス対策。
《ソーシャルメディア・ウェブ会議》
・利用手順の策定、認証情報の厳格管理、機密性 2 以上の情報発信禁止。

6）運用（ポリシーに違反した場合の内容）
情報セキュリティポリシー違反に対しては、以下の措置が講じられる。

《懲戒処分》
情報セキュリティポリシーに違反した職員等およびその監督責任者は、違反の重大性や事象の状況に応じて、地方公務員法に基づく懲戒処分の対象となり得る。
《違反時の対応》
・違反が確認された場合、速やかに是正措置を要求する。
・違反状況が改善されない場合、当該職員等の情報システムやネットワークの使用権限を停止または剥奪することがある。

7）業務委託
外部の事業者に業務を委託したり、外部サービスを利用したりする際には、町が保有する情報資産のセキュリティ確保のため、以下の遵守事項が求められる。

《委託先の選定》
委託内容に応じた情報セキュリティ対策が確保されているかを確認し、国際規格の認証取得状況や監査結果等を考慮して選定する。
《契約による義務付け》
委託契約において、情報セキュリティ要件、遵守義務（秘密保持、目的外利用禁止、再委託制限、監査協力など）、責任範囲、情報資産の返却・廃棄方法を明確に定める。
《外部サービス利用》
機密性 2 以上の情報を取り扱う場合
利用可能な業務範囲の限定、適切な技術的セキュリティ対策（暗号化、アクセス制御等）、厳格な監査・確認体制、インシデント発生時の明確な対応が求められる。
機密性 2 以外の情報を取り扱う場合**: 利用条件を遵守し、情報セキュリティ対策を講じる。
《確認・措置》
委託事業者が適切に措置を講じていることを定期的に確認し、問題があれば統括情報セキュリティ責任者へ報告する。