筑紫野市議会
情報セキュリティポリシー

基本方針

令和８年４月

筑紫野市議会

改訂履歴

施行年月日	版番号	改訂理由・内容
令和８年４月１日	1.0版	策定

目　　次

1. 目的

本基本方針は、筑紫野市議会（以下「議会」という。）及び筑紫野市議会議員（以下「議員」という。）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、議会における情報セキュリティ対策について基本的な事項を定めることを目的とする。

2. 定義

本基本方針における用語の定義は、次に掲げるものとする。

（1） 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及びその構成機器(ハードウェア及びソフトウェア)をいう。

（2） 情報システム

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

（3） 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。

（4） 情報セキュリティポリシー

この基本方針及び筑紫野市議会情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という。)をいう。

（5） 機密性

情報にアクセスすることを認められた者に限り、当該情報にアクセスできる状態を確保することをいう。

（6） 完全性

情報が破壊、改ざん又は消去をされていない状態を確保することをいう。

（7） 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。

3. 対象とする脅威

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。

（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、重要情報の詐取、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

（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

4. 適用範囲

本基本方針が対象とする情報資産の範囲は、次のとおりとする。

①議会及び議員が議会活動及び議員活動において、職務上作成し又は取得するものであって、ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

②ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

③情報システムの仕様書及びネットワーク図等のシステム関連文書

5. 議員の遵守義務

議員は、情報セキュリティの重要性について共通の認識を持ち、情報資産の取り扱い及び議会活動並びに議員活動の遂行に当たって、情報セキュリティポリシーを遵守しなければならない。

6. 組織体制の確立、情報資産の分類・管理、セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）組織体制

議会及び議員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する組織体制を確立する。

（２）情報資産の分類と管理

議会及び議員の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３）物理的セキュリティ

議員に貸与するタブレット端末及び議員の利用する端末や電磁的記録媒体等の管理について、盗難・紛失防止等の物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、議員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（５）技術的セキュリティ

議員に貸与するタブレット端末等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（６）運用

議員に貸与しているタブレット等の監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合、筑紫野市議会貸与タブレット端末管理及び使用基準（令和６年７月２９日議会改革推進会議決定）第８条第２項の規定に基づき必要な措置を講じるものとする。

（７）業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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し、必要に応じて契約に基づき措置を講じる。

外部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。

（8）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、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。

8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシー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、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。なお、対策基準は、公にすることにより議会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。