豊明市議会情報セキュリティ基本方針に関する規程

（目的）

第１条　この規程は、豊明市議会（以下「市議会」という。）及び豊明市議会事務局（以下「議会事務局」という。）が所掌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の対策（以下「情報セキュリティ対策」という。）を整備するために、豊明市議会情報セキュリティポリシーを定め、市民からの信頼の向上に寄与することを目的とする。

（定義）

第２条　この規程において、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）　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。

（２）　情報システム　コンピュータ（ソフトウェア及びハードウェア）、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。

（３）　情報セキュリティ　以下の要素を維持することをいう。

ア　機密性　情報へのアクセスを認められた者以外への重要な情報の漏えいを防止すること。

イ　完全性　情報の改ざん、破壊による被害を防止すること。

ウ　可用性　情報にアクセスを認められた者に対し、必要な時に情報の利用が可能な状態を確保すること。

（４）　情報セキュリティポリシー　この規程をいい、市議会及び議会事務局が所掌する情報資産を取り扱う業務に携わる者に浸透、普及、定着させ、情報セキュリティ対策の頂点に位置するものである。

（５）　議員　豊明市議会の議員の定数を定める条例（平成１４年３月２７日豊明市条例第１号）中、定数に含まれる議員

（６）　職員等　職員（豊明市職員定数条例（昭和５１年豊明市条例第１号）第１条に規定する職員）、議会事務局に所属するパートタイム会計年度任用職員（豊明市パートタイム会計年度任用職員の給与及び費用弁償に関する条例（令和元年豊明市条例第４２号）第１条に規定するパートタイム会計年度任用職員）及び定年前再任用短時間勤務職員（地

方公務員法（昭和２５年法律第２６１号）第２２条の４第１項又は第２２条の５第１項の規定により採用された職員）（以下「職員等」という。）をいう。

（適用範囲）

第３条　本規程の適用範囲は、次の各号に定めるとおりとする。

（１）　機関等の範囲　本規程が適用される機関等は、議員、市議会及び議会事務局とする。

（２）　情報資産の範囲　本規定が対象とする情報資産は次のとおりとする。

ア　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

イ　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）

ウ　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

（市議会議員、職員等及び委託事業者等の義務）

第４条　議員、市議会及び議会事務局が所掌する情報資産に関する業務に携わる全ての議員、職員等及び委託事業者等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては、情報セキュリティポリシーを遵守する義務を負うものとする。

（情報セキュリティ管理体制）

第５条　情報セキュリティ対策を推進・管理するため、情報セキュリティ責任者を置くものとする。

２　情報セキュリティ責任者は、議長とする。

（情報資産の分類と管理）

第６条　情報資産は、その内容に応じて分類し、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。

（情報資産に対する脅威）

第７条　情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

（１）　不正アクセス、不正操作、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、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、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、通信及び、水道供給の途絶等のインフラ障害からの波及等

（情報セキュリティ対策）

第８条　前条で示した脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

（１）　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、必要な対策を講じる。

（２）　物理的セキュリティ対策

情報資産への損傷･妨害等から保護するために物理的な対策を講ずる。

（３）　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、全ての議員、職員等及び委託事業者に情報セキュリティポリシーの内容を周知徹底する等十分な教育及び啓発が講じられるように必要な対策を講ずる。

（４）　技術及び運用におけるセキュリティ対策

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、情報資産へのアクセス制御、コンピュータ等の管理、情報セキュリティポリシー遵守状況の確認等運用面の対策を講ずる。

（５）　業務委託及び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。

（６）　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、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し、運用改善を行い情報セキュリティの向上を図る。

２　緊急事態が発生した際に迅速な対応を可能とするための対策を講ずる。

（情報セキュリティ対策基準の策定）

第９条　前条の情報セキュリティ対策を講ずるに当たって、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要があるため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

（情報セキュリティ実施手順の策定）

第１０条　情報セキュリティ責任者は、情報セキュリティ対策を実施するために、情報セキュリティ責任者が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

（非公開）

第１１条　情報セキュリティ対策基準及び情報セキュリティ実施手順は、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。

（情報セキュリティ監査及び自己点検の実施）

第１２条　情報セキュリティポリシーが遵守されていることを検証するため、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ものとする。

（評価及び見直しの実施）

第１３条　情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、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、必要に応じて情報セキュリティポリシーの見直しを実施する。

（違反に対する措置）

第１４条　この規程に定める情報セキュリティ対策、情報セキュリティ対策基準及び情報セキュリティ実施手順に違反した職員等については、その重大性、発生した事案の状況等に応じて地方公務員法第２９条第１項による懲戒処分、損害賠償請求等の対象とし必要な措置を執るものとする。

また、議員についても、損害賠償請求等の対象とし必要な措置を執るものとする。

２　この規程に定める情報セキュリティ対策に違反した委託事業者については、その重大性、発生した事案の状況等に応じて損害賠償請求等の対象とし、必要な措置を執るものとする。

（委任）

第１５条　この規程に定めるもののほか、この規程の施行に関し必要な事項は、議長が別に定める。

附　則

この規程は、令和８年４月１日から施行する。