茨城町議会情報セキュリティポリシー

茨城町議会

令和８年３月３０日　策　定

目　次

第１章　情報セキュリティ基本方針

１．目的

本情報セキュリティポリシーは、茨城町議会（以下「議会」という。）の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により、議会が保有する情報資産及び茨城町（以下「本町」という。）から提供される情報資産の機密性、完全性及び可用性を維持することを目的とする。

２．定義

本情報セキュリティポリシーにおいて、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)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

本情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

(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。

(６)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。

(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。

(８)インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

３．対象とする脅威

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)外的脅威

不正アクセス、ウイルス攻撃、サービス不能攻撃など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）人的脅威

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）災害

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）パンデミック

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）インフラ障害

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

本基本方針の適用範囲は、次の各号に定めるものとする。

（１）行政機関の範囲

議会とする。ただし、議会事務局は、本町が掲げる方針に準じる。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①議会が管理するネットワーク及び関連する設備並びに電磁記録媒体

②議会が管理する情報システム及び関連する設備並びに電磁記録媒体

③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。)

④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、職務の遂行に当たって本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．情報セキュリティ対策

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

（１）組織体制

本町の情報資産について、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

本町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）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、インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。また、高度な情報セキュリティ対策として、情報機密性の高いアプリケーションの導入により実施する。

（4）物理的セキュリティ

通信回線及び本町が貸与する情報通信端末機器(以下「タブレット端末等」という。)の管理について、物理的な対策を講じる。

（5）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。

（6）技術的セキュリティ

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。

（7）運用

情報システムの監視、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等に迅かつ適切に対応する。

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

情報セキュリティの自己点検の結果、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、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、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

第６項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。

１０．情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

第２章　情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、議会における情報資産に関する情報セキュリティ対策の基準を定めたものである。

１．組織体制

(１)議会情報セキュリティ最高責任者

議会情報セキュリティ最高責任者(以下「責任者」という。)は、議長が担うものとし、権限及び責務は次のとおりとする。

①議会における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任。

②必要に応じて、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置き、その業務内容を定める。

③必要に応じて、情報セキュリティ副責任者(以下「副責任者」という。)を置くことができる。副責任者は、責任者を補佐し、議会における情報セキュリティに関する事務を整理し、責任者の命を受けて議会の情報セキュリティに関する事務を統括するものとする。

④本対策基準に定められた自らの担務を、副責任者又は管理者に担わせることができる。

(２)情報セキュリティ・システム管理者

情報セキュリティ・システム管理者(以下「管理者」という。)は、議会事務局長が担うものとし、権限及び責務は次のとおりとする。

①責任者及び副責任者の補佐。

②ネットワーク及び情報システムの導入、設定の変更、運用、見直し等並びに情報セキュリティ対策に関する権限及び責任。

③ネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理並びにセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、必要かつ十分な措置の実施。

④情報システム担当者に対して、情報セキュリティに関する指導及び助言。

⑤緊急時等の円滑な情報共有を図るため、責任者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網の整備。

⑥緊急時の責任者への早急に報告と回復のための対策。

⑦情報セキュリティ関係規程に係る課題及び問題点を含む運用状況の把握と責任者への報告。

(３)情報システム担当者

情報システム担当者(以下「担当者」という。)は、議会事務局書記が担い、管理者の指示等に従い、情報システムの導入、設定の変更、運用、更新等の作業等、その他必要な事務を行う。

２．情報資産の分類と管理

（1）情報資産の分類

本町における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

○機密性による情報資産の分類

分類	分類基準	取扱制限
自治体機密性３Ａ	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・支給された端末以外での作業の原則禁止（自治体機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体機密性３Ｂ	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性３Ｃ	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
自治体機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産	－

○完全性による情報資産の分類

分類	分類基準	取扱制限
自治体完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤り又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体完全性１	自治体完全性２の情報資産以外の情報資産	－

○可用性による情報資産の分類

分類	分類基準	取扱制限
自治体可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
自治体可用性１	自治体可用性２の情報資産以外の情報資産	―

(２)情報資産の管理及び取扱い等

①情報資産の管理

管理者は、情報資産の管理ついて、次の対策を講じるものとする。

・情報システムのセキュリティ要件に係る事項の情報システム台帳の整備。

・複製等された情報資産に関し、原本の情報資産の分類に基づく管理。

・情報資産の分類の表示等は、ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等の適切な管理。

②情報資産の取扱い

本町又は議会事務局が作成した情報資産を入手した議員は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

③議員の情報資産の利用

情報資産の利用にあたって議員は、次の事項を遵守しなければならない。

・職務以外の目的に情報資産を利用してはならない。

・電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

④情報資産の保管

情報資産の保管にあたって管理者は、次の事項を遵守するものとする。

・情報資産の分類に従った、適切な情報資産の保管すること。

・情報資産を記録した電磁的記録媒体を長期保管する場合においては、書込禁止を措置すること。

・利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合においては、自然災害を被る可能性が低い地域への保管をすること。

・自治体機密性２以上、自治体完全性２又は自治体可用性２の情報を記録した電磁的記録媒体を保管する場合においては、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所への保管をすること。

⑤情報の送信

電子メール等により自治体機密性２以上の情報を送信する者は、必要に応じ、暗号化又はパスワード設定を行わなければならない。

⑥情報資産の運搬

車両等により自治体機密性２以上の情報資産を運搬する者は、情報資産の不正利用を防止するための措置を講じなければならない。

⑦情報資産の提供

・自治体機密性２以上の情報資産を原則、外部に提供してはならない。

・管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑧情報資産の廃棄等

情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

３．情報システム全体の強靭性の向上

情報のアクセス対策として、情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証(多要素認証)の利用に努める。

４．物理的セキュリティ

管理者は、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、次のとおりとする。

①タブレット端末等の保管に関し、盗難防止のため、施錠管理等の物理的措置を講じなければならない。

②情報システムへのログインに際し、パスワード等の認証情報の入力を必要とするように設定しなければならない。

５．人的セキュリティ

（1）議員の遵守事項

議員は、人的セキュリティ対策のため、次の事項を遵守するものとする。

①情報セキュリティポリシー等の遵守

情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに責任者に相談し、指示を仰がなければならない。

②職務以外の目的での使用の禁止

職務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセスを行ってはならない。

③タブレット端末等の持ち出しの届出

タブレット端末等、情報資産を外部に持ち出す場合には、責任者に届け出なければならない。管理者は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の職務利用

支給以外のパソコン、モバイル端末及び電磁的記録媒体等を会議等で利用してはならない。ただし、支給以外の端末利用の可否判断を責任者が行った場合にはその限りでない。また、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、安全管理措置に関する規定を遵守しなければならない。

⑤タブレット端末等におけるセキュリティ設定変更の禁止

タブレット端末等のソフトウェアに関するセキュリティ機能の設定を責任者の許可なく変更してはならない。

⑥退職時等の遵守事項

退職した場合には、速やかに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情報を漏らしてはならない。

（2）研修の実施

責任者は、必要に応じて議員に対する情報セキュリティに関する研修計画を策定し、情報セキュリティに関する理解度等に応じた研修の実施に努めるものとする。

（3）緊急時対応訓練の実施

責任者は、必要に応じて、緊急時対応を想定した訓練計画を策定し、定期的な実施に努めるものとする。

（4）研修・訓練への参加

議員は、定められた研修・訓練に参加しなければならない。

（5）情報セキュリティインシデントの報告

①議員は、議会が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、議員自ら認知した場合、又は住民等外部から報告を受けた場合は、速やかに管理者に報告しなければならない。

②管理者は、情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて議会運営委員会及び茨城町情報セキュリティ総括責任者へ報告し、住民等外部から報告を受けるための窓口を議会事務局内に設置するとともに、当該窓口への連絡手段を公表しなければならない。

６．技術的セキュリティ

６－１．コンピュータ及びネットワークの管理

（1）バックアップの実施

①管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、必要に応じて定期的にバックアップを実施しなければならない。

②管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

（２）システム管理記録及び作業の確認

①管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。また、作業記録は、詐取、改ざん等をされないように適切に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

②管理者、担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

（３）情報システム仕様書等の管理

管理者は、ネットワーク構成図、情報システム仕様書を記録媒体にかかわらず、業務上必要とする者以外の者の閲覧や紛失等がないよう、適切に管理しなければならない。

（４）障害記録

管理者は、議員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（５）ネットワークの接続制御、経路制御等

管理者は、ネットワークの接続制御、経路制御等に関し、次のとおり行うものとする。

①フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

③保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。

（６）IoT 機器を含む特定用途機器のセキュリティ管理

管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（７）無線 LAN のセキュリティ対策及びネットワークの盗聴対策

管理者は、無線 LAN のセキュリティ対策及びネットワークの盗聴対策について、次のとおり対策を講じるものとする。

①無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（８）電子メールの利用制限

議員は、タブレット端末等を用いて電子メールを送信するときは、次の事項を遵守するものとする。

①自動転送機能を用いて、電子メールの転送をしてはならない。

②職務上必要のない送信先への電子メールを送信してはならない。

③複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④重要な電子メールを誤送信した場合は、管理者に報告しなければならない。

（9）無許可ソフトウェアの導入等の禁止

①議員は、タブレット端末等に無断でソフトウェアを導入してはならない。

②管理者は、議員の職務上の必要がある場合に限り、タブレット端末等に責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、管理者は、ソフトウェアのライセンスを管理しなければならない。

（１０）機器構成の変更の制限

議員は、タブレット端末等に対し、機器の改造及び増設・交換を行ってはならない。

（１１）管理外ネットワークへの接続

①議員は、タブレット端末等を、やむを得ず議会のネットワークと異なる外部のネットワークに接続するときは、そのネットワークが安全である旨を確認した上で接続しなければならない。

②管理者は、タブレット端末等について、端末に搭載されたＯＳ（operating system）のポリシー設定等により、端末を異なるネットワークに自動で接続できないよう技術的に制限することが望ましい。

（１２）職務以外の目的でのウェブ閲覧の禁止

①議員は、タブレット端末等を用いて、職務以外の目的でウェブを閲覧してはならない。

②管理者は、議員のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、責任者に通知し適切な措置を求めなければならない。

（１３）ソーシャルメディアサービスの利用

①管理者は、議員に発信する文書について、責任者が指定するソーシャルメディアサービスを利用しなければならない。

②ソーシャルメディアサービスの不正アクセスやアカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

（１４）ペーパーレス会議システムの利用

①管理者は、会議に用いる資料について、タブレット端末等により、責任者が指定するペーパーレス会議システムを利用しなければならない。

②議員は、ペーパーレス会議システムを、タブレット端末等の他、管理者が許可した議員が所有するスマートフォン又はパーソナルコンピューターにより、利用することができる。

③管理者は、ペーパーレス会議システムにおいて、機密情報の流出を防ぐため、掲出されたファイルがみだりにダウンロードできないようしなければならない。ただし、公開されている資料又は責任者が認めたときはこの限りではない。

６－２．アクセス制御等

（1）アクセス制御

管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない者がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

（2）利用者ＩＤの取扱い

管理者は、利用者の登録、変更、抹消等の情報管理、退任に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

（３）特権を付与されたＩＤの管理等

管理者は、特権を付与されたＩＤの管理等について、次の対策を講じるものとする。

①管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理すること。

②管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じること。

③特権を付与されたＩＤ及びパスワードの変更は、委託事業者に行わせないこと。

④特権を付与されたＩＤ及びパスワードについて、議員に変更等があった際のパスワードの変更、入力回数制限等のセキュリティ機能を強化すること。

⑤特権を付与されたＩＤを初期設定以外のものに変更すること。

（４）自動識別の設定

管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

６－３．システムの導入、保守等

（１）機器等の調達に係る運用規程の整備

管理者は、機器等の調達において、次の対策を講じるものとする。

①機器等の選定基準を運用規程として整備すること。また、必要に応じて、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じること。

②情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を行うこと。

（２）機器等の導入、保守及び情報システムの調達

管理者は、機器等の導入、保守及び情報システムの調達において、次のことを行うものとする。

①機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認すること。

②情報システムの導入、保守等に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記し、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載すること。

（３）情報システムの導入

管理者は、情報システムの導入において、次の事項を確認しなければならない。

①機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていること。

②情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていること。

（4）情報システムの管理又はソフトウェア導入時の対策

管理者は、情報システムの管理又はソフトウェアを導入する端末、通信回線装置等及びソフトウェア自体に情報を保護するための措置を講じなければならない。また、利用するソフトウェアの特性を踏まえ、次の実施手順を整備しなければならない。

①情報システムの管理又はソフトウェアの情報セキュリティ水準の維持に関する手順

②情報システムの管理又はソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

（5）システムの保守に関連する資料等の整備・保管

管理者は、システムの保守に関連する資料及び関連文書を適切に整備・保管しなければならない。

（6）情報システムにおける脆弱性対策の確認等

管理者は、運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

（7）保守用のソフトウェアの更新等

管理者は、保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（8）システム更新又は統合時の検証等

管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（9）情報システムについての対策の見直し

管理者は、必要に応じて情報システムの情報セキュリティ対策を適切に見直さなければならない。

６－４．不正プログラム対策

（1）管理者の措置事項

管理者は、不正プログラム対策として、次の事項を措置しなければならない。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ議員に対して注意喚起しなければならない。

（2）管理者の措置事項

管理者は、不正プログラム対策に関するセキュリティ性を確保するため、タブレット端末等のＯＳ（operating system）を常に最新の状態に保たなければならない。

（３）議員の遵守事項

議員は、タブレット端末等の不正プログラム対策に関し、次の事項を遵守しなければならない。

①ＯＳ（operating system）の設定をみだりに変更しないこと。

②外部からデータを取り入れる場合には、不正プログラム対策ソフトウェア等によるチェックを行うこと。

③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除すること。

④管理者が提供するウイルス情報を、常に確認しなければならない。

⑤コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、速やかに使用を中止し、管理者に報告すること。

（４）専門家の支援体制

管理者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、専門家の支援を受けられるようにしておかなければならない。

６－５．不正アクセス対策

（１）責任者の措置事項

責任者は、不正アクセス対策として、次の事項を措置しなければならない。

①不要なサービスについて、機能を削除又は停止しなければならない。

②不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、管理者へ通報するよう、設定しなければならない。

③責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

（２）攻撃への対処

責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

（３）記録の保存

責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（４）内部からの攻撃

管理者は、議員及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５）議員による不正アクセス

管理者は、議員による不正アクセスを発見した場合は、適切な処置をしなければならない。

（６）サービス不能攻撃

管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(7)標的型攻撃

管理者は、標的型攻撃による組織内部への侵入を低減する対策(入口対策)や内部に侵入した攻撃を早期検知して対処する対策、侵入範囲の拡大の困難度を上げる対策、外部との不正通信を検知して対処する対策(内部対策及び出口対策)を講じなければならない。

６－６．セキュリティ情報の収集

(1)セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

管理者は、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(2)不正プログラム等のセキュリティ情報の収集・周知

責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、議員に周知しなければならない。

(3)情報セキュリティに関する情報の収集及び共有

管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

７．運用

７－１．情報システムの運用・保守時の対策

管理者は、情報システムの運用・保守時の対策として、次の事項を行う。

①情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じること。

②重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をすること。

７－２．情報セキュリティポリシーの遵守状況の確認

(1)遵守状況の確認及び対処

情報セキュリティポリシーの遵守状況の確認及び対処については、次のとおりとする。

①管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やか責任者に報告しなければならない。

②責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

③管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

(2)タブレット端末等の利用状況調査

責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、議員が使用しているタブレット端末等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３）議員の報告義務

議員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに管理者に報告を行わなければならない。

７－３．侵害時の対応等

（１）緊急時対応計画の策定

責任者は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅かつ適切に実施するため、緊急時対応計画を策定する。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めるものとする。

①関係者の連絡先

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

（３）緊急時対応計画の見直し

責任者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直すことができる。

７－４．例外措置

（１）例外措置の許可

管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適切な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、責任者の許可を得て、例外措置を講じることができる。

（２）緊急時の例外措置

管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後、速やかに責任者に報告しなければならない。

（３）例外措置の申請書の管理

責任者は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

７－５．法令遵守

議員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか、関係法令を遵守し、これに従わなければならない。

①地方公務員法(昭和 25 年法律第 261 号)

②著作権法(昭和 45 年法律第 48 号)

③不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)

④個人情報の保護に関する法律(平成 15 年法律第 57 号)
⑤行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号)
⑥サイバーセキュリティ基本法(平成 26 年法律第 104 号)
⑦茨城町議会の個人情報の保護に関する条例(令和 5 年条例第 1 号)
⑧茨城町個人情報保護条例(平成 17 年条例第 1 号)

７－６．違反時の対応

議員の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

①責任者が違反を確認した場合は、速やかに管理者に連絡し、当該議員に対して、注意、指導等、適切な措置を取らなければならない。

②管理者が違反を確認した場合は、責任者に報告し、責任者より、当該議員に対する注意、指導等、適切な措置を求めなければならない。

③責任者の注意、指導によっても改善されない場合、責任者は、当該ネットワーク又は情報システムを使用する権利を停止あるいは剥奪し、議会運営委員会において、当該議員に対する措置を諮らなければならない。

８．外部サービス(クラウドサービス)の利用

議員は、タブレット端末等において、責任者が指定したアプリケーション以外の外部クラウドサービスの利用をしてはならない。

９．自己点検・見直し

(1)実施方法

管理者は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施するものとする。

(2)報告

管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、責任者に報告しなければならない。

(3)自己点検結果の活用

責任者は、自己点検の結果を受け、必要に応じて情報セキュリティポリシー及び関係規定等の見直しを行うものとする。