竹富町議会情報セキュリティ基本方針

１．目的

本方針は、竹富町議会（以下「議会」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、情報セキュリティ対策の基本事項を定めることを目的とします。これにより、円滑な議会運営と町民の信頼確保を図ります。

２．用語の定義

情報資産：議会活動で使用するデータ、情報システム、ネットワーク、電子機器（タブレット等）を指します。

機密性：許可された人だけが情報にアクセスできること。

完全性：情報が破壊や改ざんをされず、正しい状態であること。

可用性：必要な時にいつでも情報が利用できること。

３．適用範囲

この方針は、議会が保有・管理する情報資産、及びそれを取り扱うすべての議員に適用します。 ※議会事務局職員については、竹富町情報セキュリティポリシーを適用します。

４．管理体制

最高責任者：議長を最高情報セキュリティ責任者とし、議会における最終決定権限と責任を負います。

事務局の役割：議会事務局長は、議長を補佐し、具体的な対策の運用や教育、事故発生時の連絡調整を行います。

５．議員の遵守義務

議員は、情報セキュリティの重要性を認識し、以下の事項を守らなければなりません。

1. ID やパスワードを適切に管理し、他人に教えないこと。
2. 貸与された端末を紛失・盗難から守るため、適切に保管すること。
3. ウイルス感染や情報漏えいの疑いがある場合は、直ちに議長（事務局）へ報告すること。

６．情報セキュリティ対策

議会は、脅威から情報資産を守るために以下の対策を講じます。

人的対策：セキュリティ意識向上のため、議員への教育・研修を定期的に行います。

技術的対策：不正アクセスやウイルス感染を防ぐため、端末の制限設定や最新ソフトの利用、通信の暗号化等を行います。

物理的対策：端末の紛失・盗難防止のための措置を講じます。

７．事故発生時の対応

情報漏えいなどの事故（インシデント）が発生した場合は、被害の拡大防止を最優先とし、速やかに原因調査と再発防止策を講じます。また、必要に応じて町本（執行機関）と連携します。

８．点検・見直し

議会は、本方針が守られているか定期的に自己点検を行い、社会情勢や技術の変化に合わせて内容を適宜見直します。