福井県特別職向け情報セキュリティポリシー

1. 目的

本ポリシーは、福井県特別職の職員が取り扱う行政情報・住民情報・政策情報を、機密性・完全性・可用性の観点から保護し、組織の信用・法令順守・行政の継続性を確保することを目的とする。

2. 対象となる特別職の範囲

知事、副知事および福井県教育長とする。

3. 規範遵守

（1）義務

特別職は、県の情報セキュリティ対策を推進する模範となり、組織文化の醸成に責任を負う。

（2）CISO への協力

特別職は、福井県 IT 推進要綱第3条の2で定める CISO（最高情報セキュリティ責任者）が主導する情報セキュリティ対策等を尊重し、全庁的なセキュリティ確保に協力する。

4. 情報資産の取扱い

（1）機密保持の徹底

特別職は、職務上知り得た未公開情報（政策決定過程、個人情報、企業の秘密情報等）について、在任中および退任後も第三者に漏洩してはならない。

（2）ソーシャルメディアサービス・メディア対応

特別職は、公務に関する情報を個人のソーシャルメディアサービス、ブログで、またはメディアに対して発信する際は、個人の見解と組織の公式見解を明確に区別しなければならない。

（3）情報の持ち出し制限

特別職は、機密性の高い文書やデータが格納された USB メモリ等を許可なく組織外へ持ち出してはならない。

5. 物理的・技術的セキュリティ

（1）端末管理

特別職は、組織から貸与された端末（PC、スマートフォン等）に最新のセキュリティアップデートを適用し、強固なパスワード等を設定しなければならない。

（2）個人所有端末等の制限

特別職は、原則として、個人所有端末や個人で契約するサービス（例：特別職が個人で契約するクラウドサービス・メッセージサービス・ファイル共有サービス・AI サービス・アプリ）等を業務で使用してはならない。

（3）公共の場での注意

特別職は、飲食店等、公共交通機関、出張先での覗き見（ショルダーハッキング）や、フリーWi-Fi の利用による情報漏洩に細心の注意を払わなければならない。

6. 外部接触に関するリスク管理

（1）外部の者との接触時の遵守事項

特別職は、外部の者との接触の際は、情報収集を目的としたアプローチ（ソーシャルエンジニアリング）に警戒し、情報の流出を防がなければならない。

（2）退任時の手続き

特別職は、退任時には、貸与された全ての端末および物理データ・電子データを速やかに返却しなければならない。

7. 事故発生時の対応

特別職は、端末の紛失、サイバー攻撃の疑い、情報漏洩の可能性を認識した場合は、直ちに CISO へ報告しなければならない。

8. その他

その他本ポリシーに定めのないことは、福井県情報セキュリティポリシー基本方針および対策基準に準ずる。

附則　このポリシーは、令和 8 年 2 月 16 日から施行する。