情報セキュリティ外部監査及び要領等再構築業務調達仕様書

１　業務名

情報セキュリティ外部監査及び要領等再構築業務

２　目的

（１） 情報セキュリティ外部監査

本市では令和５年４月１日現在、88 に及ぶ情報システムを運用しており、毎年内部組織による情報セキュリティ監査（内部監査）を実施しているが、監査のペースがシステム増加に追い付いておらず、網羅的に監査を実施する必要に迫られている。また、同時に内部監査については監査側の業務負担も大きく、限られた人的リソースで対応を迫られているところである。

これらを踏まえ、外部の専門家による客観的な視点から主要な監査対象システムに対し網羅的に監査を実施するとともに、外部の専門的な知見の活用によりセキュリティを担保することを目的とする。

（２） 情報セキュリティに係る要領等再構築

総務省発行の「地方公共団体における情報セキュリティポリシーに関するガイドライン（以下「ガイドライン」という。）」に基づき、各自治体が情報セキュリティポリシー（以下「ポリシー」という。）を定めているところである。本市でも、ガイドラインに基づき、ポリシー及び関連要領等（以下「要領等」という。）の改正を行っているが、現状にあわせるだけで、将来の外部環境の変化を含めた規定になっていない状況である。また、要領等を都度改正していることから、体系的に整理されておらず、網羅的に考慮が及んでいない場合があり、応急処置的に対応せざるを得ないこともある。

これらを踏まえ、要領等の再構築を行い、体系的に整理するとともに、外部の専門的な知見を各規定に反映することにより、将来に向けてセキュリティの担保を図ることを目的とする。

３　発注部署

吹田市行政経営部情報政策室

４　契約期間

令和５年８月１日から令和８年３月 31 日まで

５　業務概要

（１）情報セキュリティ外部監査

本市が運用する情報システムに対し情報セキュリティ監査を実施することで、本市情報セキュリティポリシーに基づき適切に管理及び運用されているかどうかを点検し、セキュリティの向上を図る助言型の情報セキュリティ監査とする。

本市が所管するシステムは住民情報系、内部事務系、独自事務系を合わせ令和５年４月１日時点で88システムあり、今後も新規導入により増え続けていく見込みである。

本業務では、それらの中の主要なシステムに対し、年間10～15システムの監査を実施することとする。なお、各年度の監査対象システムについては当該年度の当初(令和５年度にあっては契約締結後速やか)に過去の監査実績やその他本市セキュリティに係る事情等を考慮して決定するものとする。

想定する監査システム数は以下のとおりとする。

・令和５年度　10システム
・令和６年度　15システム
・令和７年度　15システム

（２）情報セキュリティに係る要領等再構築

以下に示す要領等の再構築を行う。なお、情報セキュリティポリシーの改定作業は含まない（別事業で実施）が、互いに整合性を保つようにする等、協力し合うこと。
※その他、必要となる要領等については、別途協議の上、改定または作成することがある。

No	名称	説明
1	吹田市情報システム等管理運営要領	本市の情報システム及び情報処理機器等の適正な管理運営に関し必要な事項を定めたもの
2	吹田市情報化推進本部設置要領	情報化推進本部、PMO、情報セキュリティ部会等の内部組織の設置に関し必要な事項を定めたもの
3	吹田市庁内ネットワーク取扱手順	「吹田市情報セキュリティポリシー　Ⅱ　情報セキュリティ対策基準」に基づき、ネットワークの利用に必要な手順を定めたもの
4	事務なび管理運営要領	本市のLGWAN接続系ネットワーク及び事務なび（本市庁内グループウェア）の適正な管理運営を図るため、必要な事項を定めたもの
5	インターネット利用ルール運用基準	インターネットによる情報の受発信を行うため、本市に設置する情報通信機器等の適正な管理・運用及び個人情報の保護を図るため、必要な事項を定めたもの

6	吹田市電子メール利用基準	「吹田市情報セキュリティポリシー」「インターネット利用ルール運用基準」、「吹田市庁内ネットワーク取扱手順」 に基づき、電子メールによる情報交換に関し、本市職員が守るべき基準の詳細を定めたもの
7	吹田市情報セキュリティ管理基準	情報セキュリティ監査において、吹田市が運用する電算システムが適切に管理、運用されているかどうかを点検する指標
8	情報セキュリティ実施手順（ひな型）	吹田市情報セキュリティポリシーの規定に基づき、各室課が所掌するシステムについて具体的な遵守事項を定めたもの（ひな型）
9	保有個人情報取扱いに係る特記事項（ひな型）	外部業者と個人情報を含む委託契約を締結する際に、受注者が遵守すべき事項等を定めたもの
10	吹田市情報システム化に関する要領	情報システムの導入、変更又は廃止の手続等を定めたもの
11	システムマネージャの手引き	各業務所管に配置するシステムマネージャの所掌事項等について定めたもの
12	一般ユーザの手引き	本市職員が本市ネットワーク及び情報機器等を利用するうえで必要となる事項をポリシーから抜粋しまとめたもの
13	在宅勤務実施にあたっての対象業務選定に関するガイドライン	テレワーク等で扱うことができる情報資産やテレワーク実施時の情報セキュリティ対策についての規則
14	重要性区分Ⅰ又はⅡの情報資産を外部で処理する場合における安全管理措置	情報資産を外部で処理する場合における安全管理措置を定めたもの
15	外部サービスの利用に関する規程	取扱う情報資産の重要性区分に応じた外部サービスの利用判断基準や選定基準、ライフサイクル毎の手続きを示したもの
16	Web 会議を適切に利用するための利用手順	以下のシステムの情報セキュリティ実施手順 ・インターネット会議システム(LFV) ・インターネット会議システム(Zoom) ・庁内テレビ会議システム
17	その他規定等	その他、ポリシーで定めることとされている規定について新規で作成する必要があるもの

６　情報セキュリティ外部監査業務の詳細

当該業務の詳細を以下に示す。

（１） 監査手順

ア　監査計画

当該年度の監査対象システムを決定し、実施計画を策定する。その後、本市内部組織である情報セキュリティ部会において承認を受ける。

イ　監査準備

監査を受ける部署とのスケジュール調整を行い、事前アンケート（予備調査）を実施する。また、回答結果から監査項目を決定しヒアリングシートを作成する。

ウ　監査実施

現地調査及びミーティングを行う。

監査結果に基づきフォローアップを行う。

エ　監査報告

監査報告書を作成し、セキュリティ部会に報告する。

（２）委託内容

ア　監査計画

・監査対象システム選定に係る支援

・実施計画書の作成

イ　監査準備

・事前アンケート項目の作成

・事前アンケート回答結果の集計

・ヒアリング項目の決定及びヒアリングシートの作成

ウ　監査実施

・現地調査及びミーティングの実施

・監査結果に基づくフォローアップ

エ　監査報告

・監査報告書の作成及びセキュリティ部会への報告

オ　情報政策室職員への監査実施に係る教育、ノウハウ共有等

・職員の ICT 教育の一環として非常に重要視している。本業務終了後も職員が独力で監査ができるように支援すること

カ　その他

・本市との協議参加

・その他本業務における手法、改善等にかかる提案

・その他類似監査業務との役割整理、改善等にかかる提案

・前年度に改善事項があったシステムについての後追い

（３）納品物

以下に該当する者をそれぞれ書面及びデータで納品すること。なお、アの監査報告書本体は、詳細版と概要版とに分けて作成すること。また、納品する成果物に関する権利は、本市に帰属するものとする。

ア　監査報告書

イ　脆弱性検出一覧

調査結果から運用管理上の脆弱点となる事項を取りまとめたものであること。

ウ　改善方法一覧

脆弱点と判断された項目について、採るべき改善策を取りまとめたものであること。

エ　手順書等

今後、内部監査を容易に実施することを可能とするための手順書、様式等

７　情報セキュリティに係る要領等再構築業務の詳細

当該業務の詳細を以下に示す。

（１）再構築の実施手順

ア　現状分析

要領等の規定事項や本市における実運用を整理し、重複、不足及び実態との乖離を把握する。

イ　要領等の構成策定

要領等の構成を検討し、体系図を作成する。

ウ　要領等の改正

要領等を作成、改正または削除する。

エ　情報セキュリティ部会報告資料の作成及び出席

各年度末の情報セキュリティ部会での報告資料を作成する。また、同部会に出席及び報告を求める場合がある。

オ　全庁宛通知

作成または改正された要領等を全庁宛に通知する。

（２）委託内容

ア　要領等の再構築

（ア）現状分析

現状分析資料の作成

（イ）要領等の構成策定

体系図の作成

（ウ）要領等の改正

要領等の作成、改正または削除（決裁手続きは除く）

（エ）次期調達に向けた助言

本業務の課題等を整理し、次期調達に向けた助言を行う

イ　情報政策室職員への情報セキュリティに係る教育、ノウハウ共有等

職員の ICT 教育の一環として非常に重要視している。本業務終了後も職員が独力で要領等の制定・改正ができるように支援すること

ウ　その他

・本市との協議参加及び議事録作成

・その他本業務における手法、改善等にかかる提案

（３）納品物

以下の物をそれぞれ書面及びデータで納品すること。また、納品する成果物に関する権利は、本市に帰属するものとする。

ア　要領等の現状分析資料

イ　要領等体系図

ウ　各要領等

エ　セキュリティ部会報告資料

オ　議事録

８　監査人要件

情報セキュリティ外部監査に係る監査人要件として、次の（１）から（３）の要件をすべて満たしていること。

（１）監査は、監査責任者（1 名)、監査人（数名）による監査チームを編成し実施すること。

（２）監査チームには、以下に定める資格又は同等のものを有している者が、1 名以上含まれていること。

ア　公認情報セキュリティ監査人

イ　公認システム監査人

ウ　CISA: Certified Information System Auditor

エ　システム監査技術者試験に合格

（３）監査チームには、情報セキュリティ監査、システム監査、情報セキュリティコンサルティング、情報セキュリティポリシー作成支援のうちのいずれかの実務経験を有する者が、1 名以上含まれていること。