情報セキュリティ監査業務委託仕様書

１　業務名

情報セキュリティ監査業務委託

２　目的

本業務は、最新のセキュリティ情報及び専門的知識を有する第三者により、県の情報システムについて情報セキュリティ監査を実施するものである。

また、その結果を踏まえ、監査対象課所等に対しては、問題点の確認、改善方法等についての検討、助言を行う。

これにより、庁内の情報セキュリティ対策の向上を図る。

３　期間

契約日から令和８年３月２５日（水）まで

４　履行場所

埼玉県企画財政部情報システム戦略課が指定する場所

５　委託内容

⑴　発注者が提示する情報システムを対象として、各情報システムの運用形態に応じた情報セキュリティ対策の妥当性に関する検証・評価及び改善に向けた助言型監査を実施する。

⑵　情報セキュリティ監査終了後、対象となったシステムの管理者に対し、監査内容や監査結果等について説明、助言等を行う監査結果報告会を実施する。

⑶　明らかになった脆弱性に対して、実現可能な具体的な対策案を提示し、次年度以降に対応できるよう業務を補佐する。

６　実施方法

別紙「情報セキュリティ監査実施方法」のとおり。

７　適用基準

⑴　必須とする基準等

ア　埼玉県情報セキュリティポリシー

イ　情報セキュリティ共通実施手順

ウ　県庁LANセキュリティ個別実施手順（運用管理編・利用者編）

エ　監査対象システムに関する基本情報（設計書・運用手順書等）

⑵　参考とする基準

ア　個人情報の保護に関する法律（平成１５年法律第５７号）

イ　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（令和７年３月版、総務省）

ウ　地方公共団体における情報セキュリティ監査に関するガイドライン（令和７年３月版、総務省）
エ　α’／β／β’モデル採用地方公共団体における外部監査の実施及び監査報告書の提出について（令和６年１２月１６日総務省自治行政局住民制度課デジタル基盤推進室長ほか通知）
オ　上記のほか委託期間において情報セキュリティに関し有用な基準等で、発注者と協議して採用するもの

８　要件

⑴　監査責任者、監査人、監査補助者、アドバイザー等で構成される監査チームを編成すること。
⑵　監査の品質の保持のため監査品質管理責任者、監査品質管理者等の監査品質管理体制をつくること。
⑶　監査チームには、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者が１人以上含まれていること。
ア　システム監査技術者
イ　ＩＳＭＳ主任審査員
ウ　ＩＳＭＳ審査員
エ　公認システム監査人
オ　公認情報システム監査人（ＣＩＳＡ）
カ　公認情報セキュリティ主任監査人
キ　公認情報セキュリティ監査人
⑷　監査チームには、監査の効率と品質の保持のため次の実績（実務経験）を有する専門家が１人以上含まれていること。
ア　情報システム又はサーバの運用管理経験
イ　情報セキュリティに関するコンサルティング
ウ　情報セキュリティポリシーの作成に関するコンサルティング（支援を含む）

９　成果物

以下の成果物について、それぞれの提出期限までに提出し、発注者の確認を得ること。
最終納品期限は、令和８年３月２５日（水）とし、電子データ一式を納品すること。
なお、電子データについては、最新のMicrosoft Officeで閲覧及び編集できる形式とする。
また、事前調査、ヒアリング及び現地調査で作成した資料についても、必要に応じて添付する。

納品物	提出期限
打合せ議事録（ヒアリング及び報告会含む）	打合せ終了後１週間以内
情報セキュリティ監査実施計画書	キックオフ会議開催前日
監査対象システムに対する事前調査表	キックオフ会議において協議した日程
情報セキュリティ監査結果報告書	キックオフ会議において協議した日程

10　成果物の納入場所

埼玉県企画財政部情報システム戦略課
（埼玉県さいたま市浦和区高砂三丁目１５－１）

11　成果物の帰属

成果物及びこれに付随する資料は、全て発注者に帰属するものとし、書面による発注者の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。

ただし、成果物及びこれに付随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、発注者は、本業務の目的の範囲内で自由に利用できるものとする。

12　委託業務における留意事項

業務の実施にあたっては、以下の事項に留意する。

⑴　業務実施計画書の提出

契約締結後、受注者は発注者と協議し、委託業務内容及び各業務の実施時期に係る業務実施計画書を提出するものとする。

⑵　資料の提供等

本業務の実施に当たり、発注者が妥当と判断する範囲内資料及び情報を提供する。

なお、受注者は、発注者から提供された資料は適切に保管し、特に個人情報に係るもの及び情報システムのセキュリティに係るものの保管は厳格に行うものとする。

また、契約終了後は本業務に当たり受注者が収集又は作成した一切の資料を破棄し、「廃棄破棄証明書」（様式任意）を提出すること。

⑶　技術的検証

技術的検証については、監査対象システム及び県庁ＬＡＮ/ＷＡＮの運用に対し、支障及び損害を与えないように実施するものとする。

⑷　再委託

受託者は、本業務の実施にあたり他の業者に再委託することを原則、禁止する。再委託が必要な場合は、発注者と協議の上、事前に書面により発注者の承認を得ること。

⑸　関係法令の遵守

受託者は、業務の実施にあたり、知り得た情報及び成果品の内容を正当な理由なく他に開示し又は自らの利益のために利用してはならない。これは、契約終了後又は契約解除後においても同様とする。

⑹　報告等

受注者は作業スケジュールに十分配慮し、発注者と密接に連絡を取り、業務の進捗状況を報告するものとする。遅延している場合は、遅延の回復対策を内容とした文書を作成し、報告すること。

13　その他

本業務の実施にあたり、本仕様書に記載のない事項については発注者と協議の上決定するものとする。

情報セキュリティ特記仕様書

1　実施計画書の提出

(1) 乙は、本件業務を行うに先立って、実施体制、責任者、実施方法、作業場所、スケジュール等を記した実施計画書を作成し、甲に提出し、甲の承認を得なければならない。実施計画書を変更する場合も同様とする。

(2) 甲は、乙から提出された実施計画書に対して必要な指示をすることができる。

2　外部委託先に関するセキュリティ要件のチェックシートの提出

(1) 乙は、本件業務を行うに先立って、別紙「外部委託先に関するセキュリティ要件のチェックシート」の各項目を確認し、チェック欄にチェックを付した上で甲に提出し、甲の承認を得なければならない。

(2) 甲は、乙から提出された「外部委託先に関するセキュリティ要件のチェックシート」の内容に不備がある場合、必要な指示をすることができる。

3　従事者の監督

乙は、本件業務に関わる実施体制（連絡体制を含む。）及び要員の一覧表を甲に提出し、甲の承認を得なければならない。要員に変更があった場合も同様とする。

4　状況報告書の提出

(1) 乙は、甲、乙双方の合意に基づき定めた期間、方法及び内容等で本件業務の作業状況等について、甲が認めた場合を除き書面により報告しなければならない。

(2) 前項の規定にかかわらず、乙は、甲から本件業務の作業状況等について報告を求められたときは、甲が指示する方法及び内容等により、これを報告しなければならない。

(3) 甲は、状況報告に対して必要な指示をすることができる。

5　本件業務を行うために甲から提供された情報（以下「情報」）が記録された資料（以下「資料」）等の管理

(1) 乙は、資料等の一覧表を作成しなければならない。

(2) 乙は、資料等の複製、提供、業務作業場所以外への持ち出し、送信その他個人情報を含めて適切な管理に支障を及ぼすおそれのある行為をしてはならない。ただし、あらかじめ甲の承諾を受けたときは、この限りではない。

(3) 乙は、資料等、作業中のデータ及び甲に帰属した成果物を、甲の承諾を得ずに、甲の指示する目的以外に使用及び第三者への提供をしてはならない。

(4) 乙は、甲の承諾を得ずに、資料等、作業中のデータ及び甲に帰属した成果物を作業場所から持ち出してはならない。

(5) 乙は、資料等及び作業中のデータをその貸与目的を達したとき又は契約終了時に返却、廃棄又は消去しなければならない。複製物及び貸与された資料をもとに変更したものも同様とする。

(6) 乙は、資料等を甲の承認を得て破壊した場合、確実に破壊した旨の証明を書面で

甲に提出しなければならない。

(7) 乙は、資料等及び作業中のデータの保護・管理に必要な手続きを作成し、資料等を閲覧できる者や方法の制限等を行わなければならない。

(8) 乙は、提供された資料等の内容については、公知の事実となるまで契約終了後も他言してはならない。

6　本人確認

乙は、本件業務の履行に関わる要員が納入場所等に立ち入る場合名札を着用させるとともに、乙の要員であること、要員本人であることを証するものを携帯させなければならない。

7　安全確保上の問題への対応

(1) 乙は、本件業務の遂行に支障が生じるおそれのある事故の発生を知り得たときは、直ちにその旨を甲に報告し、遅延なくその措置状況を書面により報告しなければならない。

(2) 甲は、前項の規定により報告を受けたときは、乙に対し、被害の拡大の防止又は復旧のために必要な措置に関する指示を行い、乙は当該指示に従わなければならない。

(3) 乙は、事案の内容、影響等に応じて、その事実関係及び再発防止策の公表等の措置を甲と協力して講じなければならない。

8　要員の教育

(1) 乙は、本件業務にかかわる全要員に対して、本件業務を遂行するために必要な教育を行わなければならない。

(2) 乙は、教育に関する計画及び実施実績について甲に報告しなければならない。

(3) 乙が行う教育には、ドキュメントの取扱方法、個人識別情報の取扱方法、データの取扱方法、事故時の連絡体制、個人情報の取扱方法を含まなければならない。

(4) 甲は、乙の提出した教育に関する計画及び実施実績について必要な指示をすることができる。

9　作業上の権限

(1) 乙は、本件業務の実施において、情報へのアクセス制御を設け、要員に対し、必要なアクセス権のみを付与するものとする。

(2) 乙は、甲の情報をシステムで操作する場合操作記録を作成すること。（ログを保存すること。）

(3) 乙は、甲の要求があったとき、操作記録（ログ）を甲に提示しなければならない。

10　機器の管理

(1) 乙は、本件業務の実施に使用するコンピュータ機器等を限定しなければならない。ただし、甲の承認を得た場合はこの限りではない。

(2) 乙は、前号の機器等の盗難、破壊等の防止策を講じなければならない。

(3) 乙は、甲から貸与された機器等についても同様の措置をとらなければならない。

11　機器及び納品物のウイルスチェック

(1) 乙は、本件業務を履行するために使用するコンピュータ等の機器に対してウィルス対策ソフトを導入する等のコンピュータウイルス感染防止策を講じなければならない。

(2) 乙は、甲に対して納品する電子データがコンピュータウイルスに感染していないことを甲の指定する方法で保障しなければならない。

(3) 乙は、甲から貸与された機器に対しても(1)の措置を行うものとする。

12　テストの実施方法

(1) テストに際しては、乙は、テストスケジュール、テスト内容、テストデータ内容等を記したテスト計画を作成し、甲の承認を得なければならない。

(2) 乙は、テストの実施後、テスト内容、テスト結果、改善スケジュール等を記したテスト報告書を提出し、甲の承認を得なければならない。

(3) 乙は、県庁ＬＡＮ等の共用情報資産に影響を与えないことが確認できた後でなければ、県庁ＬＡＮ等の共用情報資源を利用したテストを実施してはならない。

13　管理規定

(1) 乙は、本件業務の実施について以下の規定を定めなければならない。

ア　セキュリティ事故の場合の連絡体制

イ　甲から提供された資料等の保管方法と責任者

ウ　甲から提供された資料等にアクセスできる者の名簿、管理責任者

エ　甲から提供された資料等のアクセス記録の管理方法

オ　本件業務の実施において作成された資料等（データ、ドキュメント、出力帳票、入力帳票、プログラム、設定ファイル、ログ等）にアクセスできる者の名簿、管理責任者

カ　本件業務の実施において作成された資料等のアクセス記録の管理方法と管理責任者

キ　甲から提供された資料等及び本件業務の実施において作成された資料等の返却または破壊方法と返却・破壊管理者

ク　コンピュータ等の機器の管理方法と責任者

ケ　コンピュータウイルス対策

(2) 乙は、甲からの請求があった場合、前号の規定により作成されたドキュメントを速やかに提示しなければならない。

14　検査権

(1) 甲は、乙が行う本件業務に関して、口頭、書面及び立入りにより検査を行うことができる。

(2) 甲は、乙に対し、必要な指示を出すことができる。

(3) 乙は、甲からの検査要求及び甲からの指示に対して誠実に協力しなければならない。

15　協力会社等に対する責任

(1) 乙は、本件業務を実施するに際して自社以外の企業、個人（以下「協力会社等」という。）を利用する場合、協力会社等に対して本契約の定めを周知・指導しなければならない。

(2) 協力会社等の行為は、乙の行為とみなす。

16　その他

乙は、本件業務の実施について本契約書、仕様書及び甲から提出された資料等に明記されていない事態が発生した場合、速やかに甲に報告し、甲の指示を仰がなければならない。

外部委託先に関するセキュリティ要件のチェックシート

項目	確認事項	チェック欄
1.基本事項	契約に係るデータ及び知り得た秘密等の取扱いについて、その重要性を認識し、適切に取り扱う。	□
2.法令等遵守	個人情報の保護に関する法令等を遵守する。	□
3.秘密の保持	契約の履行に際して知り得た秘密を他に漏らさない。	□
	契約の終了後、解除後及び職を退いた場合においても同様とする。	□
4.目的外使用及び第三者への提供禁止	契約に係るデータを委託者が指示する目的以外に使用し、第三者に提供しない。	□
5.データの受領	委託者からデータ等の提供を受けた場合は、データ等の受領証を作成し、委託者に提出する。	□
6.データの持ち出し	委託者の環境からデータを持ち出す場合は、持ち出す目的、データの内容及び暗号化等の対策を記し、委託者から承認を受ける。	□
	委託者の環境から業務システムで利用している本番データ（住民情報が含まれるデータ）を持ち出すことを禁止する。業務委託契約において本番データの持ち出しが認められている場合は、都度申請し、委託者から承認を受ける。	□
7.複写及び複製の禁止	本契約に係るデータを委託者の承認なく、用紙、記録媒体等に複写し、又は複製しない。	□
8.パソコン及びデータの持ち込み	委託者の環境にパソコン及びデータを持ち込み、作業を行う場合は、委託者からパソコン及びデータ持ち込みに係る承認を受ける。	□
9.安全管理義務	契約に係るデータの管理責任者を定め、業務の従事者を限定する。	□
	契約に係るデータを取り扱う場所を特定する。	□
	データの無断持ち出し禁止を周知徹底し、やむを得ず、持ち出す場合は、委託者の承認を得たうえで、管理簿等に記録する。	□
	紛失、損傷、焼失等の事故が生じないよう安全かつ適切な管理体制を整備する。	□
	パソコンやデータを持ち込む場合、最新のウイルス対策ソフト等を使用していることや不正なプログラムが書かれていないことを確認する。	□
10.データの返却・消去	委託者から借用したデータは、速やかに返却する。借用したデータを複製・保存した場合は消去し、消去したことが分かる書類を委託者に提出する。	□
11.記録媒体の廃棄	契約の履行上、委託者から廃棄指示がある場合の記録媒体等は、確実に物理的破壊し、又は全ての記録を復元不可能な状態に消去した後に廃棄し、廃棄したことが分かる書類を委託者に提出する。	□
12.監督及び監査	委託者が、契約の履行に関し必要があるときは、受託者及び再委託先に対して報告を求め、監査を行い、又は監査に立会うことができるように、体制等を整備する。	□
13.教育	従業者に対して、データの保護及び秘密の保持等データの取扱いに関し履行すべき責務について十分な教育を行う。	□
	教育の実施状況を記録する。	□
14.事故発生の報告義務	安全管理措置等が履行できない場合及び情報漏えい等の事故が発生した場合等に備え、直ちに委託者へ通知、報告できる体制を整備する。	□
15.再委託の禁止	委託者の承諾なしに、業務を第三者に委託し又は請け負わせない。	□
	委託者の承諾を受けて再委託した場合は、再委託者に本契約の規定を遵守させる。	□

提出日：令和　　年　　月　　日

記入者：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿