仕様書

1　適用範囲

本仕様書は、札幌市が実施する「令和２年度　札幌市情報セキュリティ内部監査業務（以下「本業務」という。）」に適用する。

2　業務の目的

本市は、情報セキュリティの対策を整備した「札幌市情報セキュリティポリシー（以下「ポリシー」という。）」を策定し、運用している。

本業務は、本市における情報セキュリティの維持を目的とし、ポリシーの遵守状況を確認する等の情報セキュリティ内部監査（以下「内部監査」という。）を行うものである。

3　履行場所

納品や打合せ等は「札幌市白石区菊水１条３丁目 1-5（札幌市菊水分庁舎）」とする。また、実地検査（ヒアリング）等は本市が別に認めた場所（札幌市内）で行うものとする。

来庁又は本市職員の立会を要しない作業の実施場所は、受託者の責において任意とする。

4　履行期間

契約書に示す委託期間の初日から令和３年３月 19 日まで

5　業務委託内容

内部監査を支援するため、次の各号に掲げる内容を実施すること。

⑴　内部監査実施手順書の作成

別紙「情報セキュリティ内部監査実施要領」の「２　実施概要」に掲げる⑴～⑶の項目について、具体的な手順を著した実施手順書を作成する。

実施手順書は内部監査の全ての対象者に配布するため、情報セキュリティに明るくない職員が使用することを想定し、平易かつ詳細に記載すること。

また、Microsoft 社の Word 形式で作成すること。

なお、実施手順書の作成に当たっては、作成案をもって本市と協議を行い、承認を得るものとする。

⑵　内部監査調査票の作成

別紙「情報セキュリティ内部監査実施要領」の「２　実施概要」に掲げる⑴～⑶を実施するための調査票及び同票記入要領を作成する。

調査票の回答方法は、原則として選択式を採用すること。

また、Microsoft 社の Excel 形式で作成し、集計機能を設けること。集計にはマクロ機能を用いても構わない。

なお、調査票の作成に当たっては、作成案をもって本市と協議を行い、承認を得るものとする。

⑶　ヒアリングの実施

本市が選定する部署及びシステムに対し、現地へ訪問して実地検査（ヒアリング）を実施する。

ヒアリングの主体は受託者とし、本市職員が立会のもと実施すること。

⑷　報告書の作成

内部監査実施結果の集計及び分析を行い、報告書としてまとめる。

また、報告書には分析内容に基づく改善の提案を盛り込むこと。

⑸　説明会の実施

⑷で取りまとめた報告書について、本市の指定する場所（菊水分庁舎会議室を予定）にて情報システム部を対象とした説明会を１回実施すること。

⑹　進捗報告

業務の進捗状況について、本市から問い合わせがあった時は、その都度報告すること。また、業務内容について、本市の目的に合致しているか、その都度確認すること。

６　対象範囲

内部監査のうち、自己点検及び相互点検は、本市における全ての所属（課等）、職員及びシステムを対象に実施する。ただし、実地検査の対象となるものは相互点検を省略する。

実地検査は、所属及びシステムのうち一部を抽出して実施する。

各数量は概ね次に掲げるとおりである。

⑴　所属数　約 400

⑵　職員数　約 13,000

⑶　システム数　約 300

⑷　実地検査の実施数　約 30

7　作業日時

原則として土、日、祝日を除く 8:45～17:15 とする。ただし、来庁又は本市職員の立会を要しない作業については、この限りではない。

8　業務責任者の要件

本業務を履行するに当たっては、⑴及び⑵に掲げる条件を共に満たす業務責任者を選任すること。

⑴　ア～ケに掲げる資格のいずれかを有すること

ア　システム監査技術者

イ　公認情報システム監査人（CISA）

ウ　公認システム監査人

エ　ISMS 主任審査員

オ　ISMS 審査員

カ　情報処理安全確保支援士

キ　情報セキュリティスペシャリスト（情報セキュリティアドミニストレータ）

ク　公認情報セキュリティ主任監査人

ケ　公認情報セキュリティ監査人

⑵　自社（派遣労働者である場合は派遣先）以外の法人に対し、対象者本人が監査人として監査を実施した経験が、直近 5 年間で 2 回以上あること。なお、監査人の経験には、自社に所属する以前のものも含めることができる。

9　提出書類

本業務に係る提出書類は、次に掲げるとおりとする。

⑴　業務着手時

ア　業務責任者指定通知書（様式１）　１部

「８　業務責任者の要件」を満たすことが確認できる書類の写しを添付すること。また、業務期間中に業務責任者を変更するときも、速やかに届け出ること。

イ　履行管理体制図（任意様式）　１部

業務期間中に履行管理体制を変更するときも、速やかに届け出ること。

⑵　業務完了時

ア　完了届（様式２）　１部

イ　内部監査自己点検結果の集計及び実施報告書（任意様式）　１部

ウ　実施報告書のダイジェスト版（任意様式）　１部

エ　本件業務で使用した資料、書類、議事録等　１部

オ　その他、本市が別に必要と定めるもの　必要部数

カ　イ～オの電子データ（CD-R 又は DVD-R）　１部

電子データは、Microsoft Word、Microsoft Excel、Microsoft PowerPoint 及び PDF を基本とする。

10　環境に対する配慮

受託者は、本市の環境マネジメントシステムに準じ、環境負荷低減に努めること。

⑴　電気、水道、油、ガス等の使用にあたっては、極力節約に努めること。

⑵　ごみ減量及びリサイクルに努めること。

⑶　両面コピーの徹底やミスコピーを減らすことで、紙の使用量を減らすよう努めること。

⑷　自動車等を使用する場合は、できるだけ環境負荷の少ない車両を使用し、アイドリングストップの実施など環境に配慮した運転を心がけること。

⑸　業務に係る用品等は、札幌市グリーン購入ガイドラインに従い、極力ガイドライン指定品を使用すること。

11　再委託の禁止

原則として、本業務の全部又は一部を第三者に委託（以下「再委託」という。）してはならない。止むを得ず再委託を行う場合は理由及び範囲を明確にし、事前に本市の

承認を得ること。

12　秘密保持義務

本業務で知り得た情報及び入手したデータは、本契約の履行期間及び履行後においては第三者に漏らしてはならず、本業務に関わる従業員その他関係者にも周知徹底しなければならない。

データを取り扱うときは、これを流出させないように留意しなければならない。特に、次に掲げる各号を遵守すること。

⑴　本市の情報を目的外に使用しないこと。

⑵　本市の情報を複写、複製する場合には本市の許可を事前に得ること。

⑶　本市の情報を外部記憶媒体等で持ち出す場合は、紛失及び盗難を避けるため厳重に保管すること。また、データは必ず暗号化をすること。

⑷　本市の情報を取り扱う際は、のぞき見等への対策を行い、関係者以外に情報が知れ渡らないようにすること。

13　その他特記事項

⑴　交通費その他諸経費は本業務による費用に含まれており、別途支給することはないので注意すること。

⑵　ISMS、関連情報の最新動向、コンサルティングのノウハウを活用し、企画・提案を行うこと。

⑶　成果物の納入後、その内容が要求品質を満たしていないものについては、受託者の責任において関連する項目を再検査し、当該個所の修正を行うこと。

⑷　本契約を履行する過程で生じた納入成果物に関し、著作権法第 27 条及び第 28 条に定める権利を含むすべての著作権は、札幌市に帰属するものとする。ただし、受託者は、本契約履行過程で生じた納入成果物に関し、著作権を自ら使用又は第三者に使用させる場合には、札幌市と別途協議することとする。なお、受託者は、札幌市に対し、一切著作人格権を行使しないこととし、また、第三者をして行使させないものとする。

⑸　契約図書に定めのない事項及び疑義が生じた場合は、業務担当者と協議をするものとし、その内容を記載した議事録を提出すること。

14　業務担当課

総務局情報システム部システム調整課

（仕様書 様式 1）

業務責任者指定通知書

令和　　年　　月　　日

（あて先）札幌市長

受託者（住所）

（氏名）　　㊞

件　　名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

上記業務に係る業務責任者等について、次のとおり定めたので通知します。

区分	氏名	備考（資格等）
業務責任者		

備考　この様式により難い時は、この様式に準じた別の様式を使用することができる。

役務－第９号様式　完了届　　（仕様書 様式2）

完　了　届

年　　月　　日

（あて先）札幌市長

住　　所
商号又は名称
職　・　氏　名　　印

名　称

上記役務は，　　年　　月　　日に完了したのでお届けします。
（なお，完了した役務の内容は，作業日誌等にて逐次報告したとおりです。）

受付	年　　月　　日	完了を確認した職員	印

課　長	係　長	係

年　月　日上記のとおり完了届の提出があったので，この役務の履行検査に係る検査員及び立会人については次の者に命じ、　　年　月　日に検査を実施してよろしいか。

検査員　　職　　氏　名

立会人　　職　　氏　名

（仕様書 別紙）

情報セキュリティ内部監査実施要領

1　実施方針

内部監査の実施方針は以下の３点とし、助言型監査とする。

⑴　ポリシーに基づく対策の実施状況の確認

ポリシーに規定される各項目が遵守されているかをチェックし、必要に応じて改善提案を行う。

⑵　情報資産の取扱状況の確認

情報資産（個人情報、機密情報等）の取扱状況の実態（一覧の作成状況等）をチェックし、必要に応じて改善提案を行う。

⑶　緊急時の連絡・報告体制の整備状況の確認

情報システムを利用する業務において、緊急時の連絡・報告体制等の必要資料が整備されているかをチェックし、必要に応じて改善提案を行う。

2　実施概要

各所属は、配布される内部監査実施手順書等に従い、内部監査を実施する。

内部監査の実施項目は以下の３点とする。

⑴　自己点検

「１　実施方針」に掲げる⑴～⑶の状況について、各所属が自身で確認を行い、その結果を 3 種類の調査票（所属、職員及びシステム）に記入する。

確認は、所属、職員及びシステムの各単位で行う。

⑵　相互点検

「１　実施方針」に掲げる⑴～⑶の状況を客観的に評価するため、自己点検で作成した調査票を基に所属相互で点検を行う。

原則として同一部内の課単位で実施する。ただし、事務室の都合等により実施が困難な場合は、係単位等での実施を可能とする。

⑶　実地検査（ヒアリング）

「１　実施方針」に掲げる⑴～⑶の状況を客観的に評価するため、情報システム部が外部委託する監査人によるヒアリングを受ける。実地検査では、自己点検で作成した調査票を基に詳細の聞き取り及び必要に応じて改善提案が行われる。