個人住民税課税に関する事務の特定個人情報保護評価書（全項目評価書）（素案）への意見募集の結果について

2022年(令和4年)6月1日から6月30日までの間に実施した「明石市　個人住民税課税に関する事務　全項目評価書(案)」に関する意見募集の結果は、下表のとおりです。

No	項	記載箇所	意見	回答
1	12	Ⅱ　特定個人情報ファイルの概要 ４．特定個人情報ファイルの取扱いの委託 委託事項１ ⑧再委託の許諾方法 （記載内容） ・委託先から再委託承諾申請書の提出があり、本市が再委託承諾書により承諾した場合に限る。 ・再委託先から従業者名簿及び再委託先の従業者から個人情報の取扱いに関する誓約書を提出させる。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「・評価実施機関が再委託を許諾する場合は、その判断基準について記載してください。」 とされており、貴市が「再委託承諾書」により承諾するための判断基準を記載されてはどうでしょうか。 下記の記載事項も同様です。 １３ページ 委託事項２の⑧ １５ページ 委託事項５の⑧ １６ページ 委託事項６の⑧	契約書上に、再委託する場合は、委託先と同様の個人情報保護の措置を実施しなければならない旨を規定しているため、再委託を承認する基準は、契約書に記載する個人情報保護措置条項となります。
2	32	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ３．特定個人情報の使用 リスク２：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発効・失効の管理 具体的な管理方法 （記載内容） ・人事異動や権限変更があった場合は、書面にて管理者が決裁し、システムに反映している。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、下記のとおりとなっており、「発効管理」と「失効管理」に分けてどのような手段でリスク対策を講じているかについて記載されてはどうでしょうか。 （１）発効管理：事務上必要なユーザについてのみ ID 等を発効するようにどのような手段を講じているか（権限発効のポリシー、申請・許可の流れ等を記載してください）。更新権限者を不必要に増やさないためにどのような手段を講じているか。 （２）失効管理：事務範囲の変更、異動、休職、退職など、事務上情報にアクセスする必要のなくなったユーザの権限を迅速に失効するためにどのような手段を講じているか（たとえば、権限失効の流れを記載してください）。	人事異動時に作成する書類は、「発効管理」及び「失効管理」を合わせて実施する様式としています。分かりにくい表現であったため、追記いたします。

3	32	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ３．特定個人情報の使用 リスク２：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法 （記載内容） ・端末操作資格者のアクセス可能機能の権限一覧表を作成している。 ・業務上アクセスが不要となった機能については、アクセス権限の変更または削除している。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「アクセス権限の発効・失効の管理を行う者による当該管理の適正性についてどのようにチェックをしているか（権限表の作成、定期的見直しなど）記載してください。」とされています。アクセス権限の管理については、左記に加えて、ユーザーIDやアクセス権について、事務担当部署や情報システム部署の管理者が定期的に確認し、その妥当性を検証し、アクセス権限の見直しにつなげるなどの対応を行っていれば、追記されてはどうでしょうか。	権限の変更は、業務の内容追加・変更がある都度見直しを実施しています。なお、システム利用の必要性を含め、権限の見直しは、年に一度実施しています。
4	32	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ３．特定個人情報の使用 リスク２：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な方法 （記載内容） ・端末から検索、更新した際のアクセスログを記録している。 ・処理日時、端末情報、部署情報、操作者情報、処理事由を記録している。 ・バックアップされたアクセスログは一定期間保管している。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「記録はどの程度の期間保管されるか」とされており、保管期間（たとえば７年間など）を明記されてはどうでしょうか。	業務により、保管期間は異なるため明記しませんが、業務としてログを参照する必要のある期間は、ログの保管をしています。

5	34	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ４．特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認 （記載内容） ＜システム運用・保守委託について＞ ・委託業者を選定する際、委託先の情報保護管理体制として、プライバシーマーク等の公共機関の認定・認証を取得していることを選定基準としている。 ・委託業者の選定及び契約締結の決裁を行うなかで、委託業者の社会的信用と能力を確認している。 ・委託業者の業者登録内容が有効か適時確認している。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「・委託先を決定する際に特定個人情報ファイルを適切に取り扱う委託先であることをどのように確認しているか、手続等について記載してください。」とあり、また、「委託先の決定後においても、特定個人情報ファイルの適切な取扱状況等を把握するために、必要に応じて実地の監査、調査等を行う等、契約締結後に情報保護管理体制の確認を行うこととしている場合は、その旨を記載することが考えられます」とされています。 「システム運用・保守委託」については、左記内容に加えて、委託先の決定後において、情報保護管理体制の確認を実施されていれば、追記されてはどうでしょうか。	ご指摘の箇所に記載しておりますように、委託業者の業者登録内容が有効か適宜確認しており、この登録内容には情報保護管理体制の確認も併せて実施しているところです。
6	34	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ４．特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録 具体的な方法 （記載内容） ・システム運用・保守委託、その他業務委託については、アクセスログまたは作業記録を残している。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「・記録を残している場合は、記録はどの程度の期間保存されるかを記載してください。」とされており、保管期間（たとえば７年間など）を明記されてはどうでしょうか。	業務により、保管期間は異なるため明記しませんが、業務としてログを参照する必要のある期間は、ログの保管をしています。

7	35	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ４．特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録 再委託先による特定個人情報ファイルの適切な取扱いの確保 具体的な方法 （記載内容） ・許可のない再委託は認めていない。 許可した場合でも通常の委託と同様の措置を適用している。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「特定個人情報ファイルの取扱いを再委託している場合には、再委託先での適正な取扱いの確保のために行っている措置について記載してください。例えば、再委託先における特定個人情報ファイルの管理状況を定期的に点検している場合は、実施頻度、点検方法（訪問確認、セルフチェック）、点検後の改善指示の実施有無、改善状況のモニタリングの実施有無等を記載してください。」とされています。 上記を踏まえ、「通常の委託と同様の措置の適用」の中身について、具体的に記載されてはどうでしょうか。	従来から、委託先及び再委託先には、明石市特定個人情報取扱基準及び要領に基づき、定期的に適正な特定個人情報の取扱いにかかる報告を提出させています。その旨を委託先への措置として追記します。 なお、再委託先において「通常の委託と同様の措置の適用」と記載している部分は、34 ページに記載のとおりです。
8	42	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ７．特定個人情報の保管・消去 リスク１：特定個人情報の漏えい・滅失・棄損リスク ⑤物理的対策 具体的な対策の内容 （記載内容） ＜明石市における措置＞ ・電子計算機、データを含んだ記録媒体の盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。 ・停電(落雷等)によるデータの消失を防ぐために、電子計算機に無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ・厳重に入館・入室管理されたデータセンターにサーバーを設置している。 ・システムのバックアップデータは媒体に格納し、遠隔地に保管している。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「・特定個人情報の漏えい・滅失・毀損を防ぐために、どのような物理的な対策を行っているかを記載してください。物理的な対策とは、例えば、特定個人情報が保有されているサーバの設置場所に監視カメラを設置するなどの方法により入退出者を管理することや、サーバ設置場所、端末設置場所、記録媒体・紙媒体の保管場所について施錠管理がなされていること、サーバ室等への電子記録媒体等の機器類の不要な持込みを制限していること等です。」とされています。 左記の「厳重に入館・入室管理された」とはどのような技術的対策がとられているかについて記載されるとともに、また上記記載要領にある「たとえば」の対策で実施されているものがあれば記載されてはどうでしょうか。	データセンターにおける入館・入室管理については、第三者の不法侵入を防ぐための措置を実施していますが、セキュリティの観点から詳細な記載はできません。なお、契約にあたり、データセンターのセキュリティ措置が、本市の求めるセキュリティ要件を満たしていることを確認しています。

9	44	Ⅳ　その他のリスク対策 １．監査 ②監査 具体的な内容 （記載内容） ＜明石市における措置＞ ・「明石市情報セキュリティ基本方針」及び「明石市特定個人情報等取扱基準」に基づき、年に１回、複数の所管課を対象として監査を行っている。	「特定個人情報保護評価書（全項目評価書）」の【記載要領】によれば、「・評価書に記載したとおりに運用がなされていることその他特定個人情報ファイルの取扱いの適正性について、どのように監査するか記載してください。 -監査を行うか否か -評価実施機関内の内部監査／外部の第三者による監査の別 -監査事項 -監査の頻度、方法 -監査責任者、監査実施体制 -監査の結果をどのように活用するか ・評価対象の事務において使用するシステムに関する監査を併せて実施している場合は、当該監査についても記載してください。」とされています。 左記の「明石市情報セキュリティ基本方針」及び「明石市特定個人情報等取扱基準」に基づく監査においては、当評価書に記載したとおりの運用がなされているかについての監査が実施されることになっているのでしょうか、そうなっているのであれば、そのことを追記されてはどうでしょうか。 また、44/47 頁「①自己点検」と同様に、どの部署が実施するかについて記載されてはどうでしょうか。 その場合、監査の独立性、客観性、監査人の専門性が担保されていることに留意されることが望ましいと考えられます。	情報セキュリティ監査の実施基準や監査報告等は、「明石市情報セキュリティ基本指針」に定めており、年に１回、２～３課を対象として実施しています。前年度の監査対象課及び情報セキュリティの担当課が当該監査を実施するため、監査箇所、指摘事項等においての客観性はあるものと考えます。

10	44	Ⅳ　その他のリスク対策 １．監査 ②監査 （記載内容） なし	「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４年３月版)（総務省）の「第 3 編 地方公共団体における情報セキュリティポリシー（解説)」の「第２章 情報セキュリティ対策基準（解説） ９ 評価・見直し ９．１ 監査」において、例文や解説が下記のとおりとされており、再委託先(再々委託先等更なる委託先を含む）を含む外部委託業者に対する監査も検討されてはどうでしょうか。 （例文） （４）委託事業者に対する監査 事業者に業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。 （解説） （４） 委託事業者に対する監査情報システムの運用、保守等を業務委託している場合は、情報資産の管理が契約に従い適正に実施されているかを点検、評価する必要がある。また、これによって、セキュリティ侵害行為に対する抑止効果も期待できる。	再委託先についても、本市が委託先に対して課している措置と同様の個人情報保護の措置を実施するよう契約書上に規定しています。また、再委託先に対しても、契約履行期間中の実施体制の報告により、適切な管理がされているかを確認しています。