「明石市住民基本台帳に関する事務全項目評価書(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「明石市住民基本台帳に関する事務全項目評価書(素案)」に関する意見募集の結果は、下記のとおりです。

No.	頁	記載箇所	意 見	回 答
1	17	Ⅱ 特定個人情報ファイルの概要 1 住民基本台帳ファイル 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	「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。 18 ページ 委託事項2の⑧ 19 ページ 委託事項 3 の⑧ 19 ページ 委託事項 4 の⑧ また、「2. 本人確認情報ファイル」の35 ページ 委託事項1の⑧ 「3 送付先情報ファイルの40 ページ 委託事項1の⑧も同様です。	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	45	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 1 住民基本台帳ファイル 3. 特定個人情報の使用 リスク2 アクセス権限の発効・失効の管理 具体的な管理方法	「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、「発行管理」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	46	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 1 住民基本台帳ファイル 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	「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。・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。 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。 54 ページの「2 本人確認情報ファイル」 61 ページの「3 送付先情報 ファイル」 の同項目の内容についての意見も同じです。	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。
4	46	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 1 住民基本台帳ファイル 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	「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。 54 ページの「2 本人確認情報ファイル」 61 ページの「3 送付先情報ファイル」の同項目の内容についての意見も同じです。	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。

No.	頁	記載箇所	意 見	回 答
5	46	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 1 住民基本台帳ファイル 4. 特定個人情報ファイルの取扱いの委託 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	「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。 54 ページの「2 本人確認情報ファイル」 61 ページの「3 送付先情報ファイル」の同項目の内容についての意見も同じです。	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もとづき、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、46ページに記載のとおりです。
6	50	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 1 住民基本台帳ファイル 7. 特定個人情報の保管・消去 リスク1 ⑤物理的対策 具体的な対策の内容	「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・入室管理されたデータセンター 」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。 57 ページの「2 本人確認情報ファイル」 64 ページの「3 送付先情報ファイル」の同項目の内容についての意見も同じです。	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。
7	53	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 2 本人確認情報ファイル 3. 特定個人情報の使用 リスク2 アクセス権限の発効・失効の管理 具体的な管理方法	「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、「発行管理」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)。 60 ページの「3 送付先情報ファイル」の同項目の内容についての意見も同じです。	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。

No.	頁	記載箇所	意 見	回 答
8	53	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 2 本人確認情報ファイル 3. 特定個人情報の使用 リスク2 アクセス権限の管理 具体的な管理方法	「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。 60 ページの「3 送付先情報ファイル」の同項目の内容についての意見も同じです。	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。
9	66	Ⅳ その他のリスク対策 1. 監査 ② 監査 具体的な内容	「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、66 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	66	Ⅳ その他のリスク対策 1. 監査 ② 監査 -	「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。