（参考Ⅱ）

個人情報管理状況　検査シート

実　施　日	令和　年　月　日
実　施　者	群馬県　県土整備部　監理課
受　託　者	
業　務　名	登記事務委託

◆実施方法

（1）各項目について、業務委託契約に係る個人情報の安全管理措置等を評価し、「結果」欄に、「○（適切に実施している）」、「△（一部実施している）」、「×（全く実施していない）」「－（該当がない）」のいずれかの符号を記載してください。

※各項目について、「考え方」の欄を参考に評価をしてください。

（2）「詳細」欄に、「結果」欄で回答したことについて、その内容や理由を具体的に記載してください。

（3）表中「甲」は県の機関を指し、「乙」は委託先事業者を指します。

大項目	中項目	No.	小項目	考え方	結果	詳　細
保有個人情報の取扱	秘密の保持	1	知ることができた個人情報をみだりに他に知らせていないか。	・従事者に対し、個人情報をみだりに他に知らせないよう指導しているか。 ・委託契約が終了し、又は解除された後も同様としているか。		
	取得の制限	2	個人情報を取得するときは、事務の目的を明確にするとともに、事務の目的を達成するために必要な範囲内で、適法かつ公正な手続により行われているか。	・委託事務の目的を明確にしている。 ・取得する個人情報は、委託事務を処理するため、必要最低限とする。		
	利用及び提供の制限	3	甲の指示があるときを除き、委託事務に関して知り得た個人情報を契約の目的以外の目的のために利用し、又は甲の承諾なしに第三者へ提供していないか。	・契約の目的以外の目的のために個人情報を利用していない。 ・個人情報を第三者へ提供する場合、甲に承諾を得ている。		
	複写又は複製の禁止	4	個人情報が記載された資料を甲の承諾なしに複写又は複製していないか。	複写又は複製する場合、甲に承諾を得ている。		
再委託の禁止	再委託の禁止	5	甲の許諾なしに委託事務に係る個人情報を取り扱う事務を第三者に委託していないか。	第三者に委託する場合、甲に承諾を得ている。	－	
		6	再委託先の個人情報の取扱に関する監督を行っているか。	乙が行う委託事務に係る個人情報の取扱と同様の取扱を再委託先でも行うよう再委託先に対する指示や再委託先の報告を受けているか。	－	

大項目	中項目	No.	小項目	考え方	結果	詳　細
組織的安全管理措置	組織体制の確認	7	責任者が設置されているか。	・委託事務に係る責任者が設置されており、従事者に周知されている。 ・責任者に変更があった場合、甲にその旨を報告しているか。		
		8	委託事務に係る従事者が明確にされているか。	委託事務に係る従事者が明確にされており、従事者でない者が個人情報を取り扱うことがないようにしている。		
		9	特定個人情報を取り扱うことができる従事者及びその権限を明確にした上で、甲へ報告しているか。	個人番号利用事務等の委託を受けている場合、特定個人情報を取り扱うことができる従事者及びその権限をあらかじめ明確にした上で、甲へ書面により報告している。	―	
		10	漏えい等事案発生時の報告ルートが明確になっているか。	・漏えい等事案発生時、甲に対し報告するルートが明確になっている。 ・報告ルートが従事者に周知されている。		
		11	個人情報の漏えい等が発生した場合、甲に報告しているか。	個人情報の漏えい等が発生した場合、甲に報告している(再委託先における事案を含む。)。	―	
		12	労働者派遣契約書に、秘密保持義務等個人情報の取扱いに関する事項を明記しているか。	乙は、委託事務を派遣労働者に行わせる場合、当該労働者との労働者派遣契約書に、秘密保持義務等個人情報の取扱いに関する事項を明記している。	―	

大項目	中項目	No.	小項目	考え方	結果	詳　細
人的安全管理措置	従事者への監督	13	責任者は、従事者が適正に個人情報を取り扱うよう必要かつ適切な監督を行っているか。	取り扱う個人情報の適切な管理が図られるよう、必要かつ適切な監督を行っている。		
	従事者への監督・教育	14	責任者は、特定個人情報を取り扱うことができる従事者に対して監督・教育を行っているか。	個人番号利用事務等の委託を受けている場合、番号法・ガイドラインその他の規定により義務付けられている安全管理措置を図るため、従事者に対する監督・教育を行っている。	ー	
物理的安全管理措置	作業場所の特定	15	委託事務に係る個人情報は、●●事務所●●室で扱っているか。	個人情報は、個人情報取扱特記事項で定めた●●事務所●●室でのみ扱っている。	ー	
		16	委託事務に係る個人情報の作業場所を変更する場合は、甲から承諾を得ているか。	個人情報の作業場所を変更する際は、甲から承諾を得て変更した。	ー	
	機器及び電子媒体等の盗難等の防止	17	個人情報を取り扱う機器、電子媒体及び書類等を、施錠できる執務室、金庫等に保管しているか。	・個人情報を取り扱う電子媒体及び書類等は、施錠できる執務室、金庫等で保管する。		
		18	ロッカー、金庫等の鍵について、適切に管理しているか。	責任者や特定の従事者のみが管理し、容易にその所在が判明しないようにする。		
		19	個人情報を持ち運ぶ場合、漏えい等しないような措置を講じているか。	個人情報が記録された電子媒体や書類を持ち運ぶ場合は、パスワードの設定、封筒に封入し鞄に入れる等している。		
		20	個人情報の誤送付・誤送信等が発生しないよう適切な措置を講じているか。	・書類を発送する場合は、複数名で確認する体制を築く。 ・外部にメールを送信する場合は、「BCC」を使用するよう周知している。		
	資料等の廃棄等	21	個人情報が記録されてる資料等を削除又は廃棄する場合には、資料の溶解等復元できない手段で確実に廃棄等しているか。	・廃棄等する場合は、焼却、溶解又はシュレッダーによる裁断等の復元不可能な手段による。 ・機器及び電子媒体等を溶解する場合は、データ削除ソフトウェアの利用又は物理的な破壊等による		

大項目	中項目	No.	小項目	考え方	結果	詳　細
※　以下の項目は、個人情報をPC等の電子機器で取り扱う場合のみ対象です。						
技術的安全管理措置	アクセス制御	22	使用するPCや情報システムにおいて、適切なアクセス権限を付与された者のみがアクセスできるようアクセス制御しているのか。	・アクセス権限を付与すべき者を最小化する。 ・アクセス権限のない職員がシステムにアクセスできないように制限する。		
	アクセス者の識別と認証	23	使用するPCや情報システムは、利用者が正当なアクセス権を有する者であることを識別した上で、認証しているか。	・ユーザーID、パスワード、磁気・ICカード、生態情報等により識別する。		
	不正アクセス等による被害の防止等	24	使用するPCや情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入し、適切に運用しているか。	・外部ネットワーク等との接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 ・セキュリティ対策ソフトウェア等を導入し、不正ソフトウェアの有無を認証する。 ・セキュリティ対策ソフトウェア等のパターンファイルは常に最新の状態にする。		
	情報漏えい等の防止	25	個人情報を機器又は電子媒体等に保存する必要がある場合に、暗号化又はパスワードにより秘匿しているか。	個人情報を暗号化して管理し、暗号化に用いた暗号鍵及び暗号化された情報は別々に保管する等適切に管理する。		