別紙3

情報セキュリティ要件

受託者は（「情報セキュリティ要件」において「乙」という。以下同じ。）は、広島県(（「情報セキュリティ要件」において「甲」という。以下同じ。）)の定める個人情報保護条例，本特記仕様書「情報セキュリティ要件」に基づき、情報資産の取扱いに関する事項を遵守しなければならない。

また，乙は，セキュリティ管理態勢確認票（別記様式）で確認した項目を遵守しなければならない。

第１条（用語の定義）

本特記仕様書における「情報資産」とは，情報及び情報を管理する仕組み（情報システム並びに情報システムの開発，運用及び保守のための資料等を含む。）をいう。

第２条（責任体制の整備）

乙は、情報資産の安全管理について、内部における責任体制を構築し、その体制を維持しなければならない。

第３条（作業責任者等の届出）

1　乙は、情報資産の取扱いに係る作業責任者及び作業従事者を定めなければならない。
2　作業責任者は、特記仕様書に定める事項を適切に実施するよう作業従事者を監督しなければならない。
3　作業従事者は、作業責任者の指示に従い、特記仕様書に定める事項を遵守しなければならない。

第４条（作業場所の特定）

1　乙は、情報資産を取り扱う場所（以下「作業場所」という。）を定め、書面により甲に報告しなければならない。
2　乙は、作業場所を変更する場合は、書面により甲に報告しなければならない。
3　乙は、甲の事務所内に作業場所を設置する場合は、作業責任者及び作業従事者に対して、乙が発行する身分証明書を常時携帯させ、事業者名が分かるようにしなければならない。

第５条（教育の実施）

乙は、情報資産の保護、情報セキュリティに対する意識の向上、特記仕様書における作業従事者が遵守すべき事項その他本委託業務の適切な履行に必要な教育及び研修を、作業従事者全員に対して実施しなければならない。

第６条（守秘義務）

1　乙は、本委託業務の履行により直接又は間接に知り得た情報資産を第三者に漏らしてはならない。契約期間満了後又は契約解除後も同様とする。

第７条（再委託）

1　乙は、契約約款に基づき本委託業務の一部をやむを得ず再委託する必要がある場合は、再委託先の名称、再委託する理由、再委託して処理する内容、再委託先において取り扱う情報、再委託先における安全性及び信頼性を確保する対策並びに再委託先に対する管理及び監督の方法を明確にした上で、業務の着手前に、書面により再委託する旨を甲に申請し、その承認を得なければならない。
2　前項の場合、乙は、再委託先に本契約に基づく一切の義務を遵守させるとともに、甲に対して、再委託先の全ての行為及びその結果について責任を負うものとする。
3　乙は、再委託先との契約において、再委託先に対する管理及び監督の手続及び方法について具体的に規定しなければならない。
4　乙は、再委託先に対して本委託業務を委託した場合は、その履行状況を管理・監督するとともに、甲の求めに応じて、管理・監督の状況を甲に対して適宜報告しなければならない。

第８条（派遣労働者等の利用時の措置）

1　乙は、本委託業務を派遣労働者、契約社員その他の正社員以外の労働者に行わせる場合は、正社員以外の労働者に本契約に基づく一切の義務を遵守させなければならない。
2　乙は、甲に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

第９条（情報資産の管理）
　乙は、本委託業務において利用する情報資産を保持している間は、次の各号の定めるところにより、情報資産の管理を行わなければならない。
一　施錠が可能な保管庫又は施錠若しくは入退室管理の可能な保管室で厳重に情報資産を保管すること。
二　甲が指定した場所へ持ち出す場合を除き、情報資産を定められた場所から持ち出さないこと。
三　情報資産を電子データで持ち出す場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。
四　事前に甲の承認を受けて、業務を行う場所で、かつ業務に必要最小限の範囲で行う場合を除き、情報資産を複製又は複写しないこと。
五　情報資産を移送する場合、移送時の体制を明確にすること。
六　情報資産を電子データで保管する場合、当該データが記録された媒体及びそのバックアップの保管状況並びに記録されたデータの正確性について、定期的に点検すること。
七　情報資産を管理するための台帳を整備し、情報資産の利用者、保管場所その他の情報資産の取扱いの状況を当該台帳に記録すること。
八　情報資産の紛失、漏洩、改ざん、破損その他の事故（以下「情報資産の漏洩等の事故」という。）を防ぎ、真正性、見読性及び保存性の維持に責任を負うこと。
九　作業場所に、私用パソコン、私用外部記録媒体その他の私用物を持ち込んで、情報資産を扱う作業を行わせないこと。
十　情報資産を利用する作業を行うパソコンに、情報資産の漏洩につながると考えられる業務に関係のないアプリケーションをインストールしないこと。

第１０条（提供された情報資産の目的外利用及び第三者への提供の禁止）
　乙は、本委託業務において利用する情報資産について、本委託業務以外の目的で利用してはならない。また、甲に無断で第三者へ提供してはならない。

第１１条（情報資産の返還又は廃棄）
1　乙は、本委託業務の終了時に、本委託業務において利用する情報資産について、甲の指定した方法により、返還又は廃棄を実施しなければならない。
2　乙は、情報資産の消去又は廃棄に際し甲から立会いを求められた場合は、これに応じなければならない。
3　乙は、本委託業務において利用する情報資産を廃棄する場合は、当該情報が記録された電磁的記録媒体の物理的な破壊その他当該情報資産を判読不可能とするのに必要な措置を講じなければならない。
4　乙は、情報資産の消去又は廃棄を行った後、消去又は廃棄を行った日時、担当者名及び消去又は廃棄の内容を記録し、書面により甲に対して報告しなければならない。

第１２条（定期報告及び緊急時報告）
1　乙は、甲から、情報資産の取扱いの状況について報告を求められた場合は、直ちに報告しなければならない。
2　乙は、情報資産の取扱いの状況に関する定期報告及び緊急時報告の手順を定めなければならない。

第１３条（監査及び検査）
1　甲は、本委託業務に係る情報資産の取扱いについて、本契約の規定に基づき必要な措置が講じられているかどうか検証及び確認するため、乙及び再委託先に対して、監査又は検査を行うことができる。
2　甲は、前項の目的を達するため、乙に対して必要な情報を求め、又は本委託業務の処理に関して必要な指示をすることができる。

第１４条（事故時の対応）
1　乙は、本委託業務に関し情報資産の漏洩等の事故が発生した場合は、その事故の発生に係る帰責の有無に関わらず、直ちに甲に対して、当該事故に関わる情報資産の内容、件数、事故の発生場所、発生状況を書面により報告し、甲の指示に従わなければならない。
2　乙は、情報資産の漏洩等の事故が発生した場合に備え、甲その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

3　甲は、本委託業務に関し情報資産の漏洩等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。
4　受託者は，県から委託を受けた業務に関し，第三者からの苦情や問合せを受けた場合，その他これに関連した事故が発生した場合，又は発生する恐れがある場合，直ちにその旨を県に報告するものとする。
なお，第三者からの苦情や問合せについては，県の承諾なしにこれに回答してはならず，対応については県の指示に従う。

第１５条（契約解除）
1　甲は、乙が本特記事項に定める義務を履行しない場合は、本特記事項に関連する委託業務の全部又は一部を解除することができる。
2　乙は、前項の規定による契約の解除により損害を受けた場合においても、甲に対して、その損害の賠償を請求することはできないものとする。

第１６条（損害賠償）
乙の故意又は過失を問わず、乙が本特記事項の内容に違反し、又は怠ったことにより、甲に対する損害を発生させた場合は、乙は、甲に対して、その損害を賠償しなければならない。

別記様式

セキュリティ管理態勢確認票

委託業者名		確認者職指名	

1　認定資格取得状況

○プライバシーマーク取得状況
　□取得済み（許諾番号 ：　　，平成　 年　 月　 日まで有効）　　□取得していない
　□取得活動中（取得予定時期 ： 平成　 年　 月頃）
　□プライバシーマークに準じた運用を行っている
○ISMS取得状況
　□取得済み（許諾番号 ：　　，平成　 年　 月　 日まで有効）　　□取得していない
　□取得活動中（取得予定時期 ： 平成　 年　 月頃）
　□ISMSに準じた運用を行っている
○その他　□取得資格名（　　）

2　管理態勢

セキュリティ管理態勢		機密性	確　認　事　項	適・否
体制	組　織	3	経営者を責任者とし，当該業務の全従事者を含めたセキュリティ管理組織が定められているか	
	点検・監査・教育	3	セキュリティ体制の自己点検・監査を行い，問題点の是正や教育を繰り返し，継続的な改善が図られているか	
	従業員の義務	3	セキュリティ規定遵守の誓約書を取り付け，違反時には従業員規則などで罰則を科すこと，退職後も守秘義務があり違反時には損害賠償義務と法的罰があることが告知されているか	
	再委託先への義務	3	県から課せられたものと同等の守秘義務と責任を，再委託先にも課すことが契約書で明記されているか	
規定	セキュリティ	3	ISO27001の中から，当該業務に関係する事項に係る規定が設けられているか	
	個人情報保護	3	個人情報を取扱う場合には，個人情報保護法に準じた規定が定められているか	
	保　管	2	預かった書類の保管場所が制限されているか	
		3	預かった書類は保管責任者を定めて，施錠管理されているか	
取扱	取扱者	3	業務上必要な者だけに取扱者を限定し，アクセス制限手段が講じられているか	
	使用するコンピュータ	2	私物パソコンでの作業が禁止されているか	
	使用するネットワーク	2	信頼できるネットワーク回線の使用が義務付けられているか	
	外部媒体	3	保管場所や作業場所への必要以上の記憶媒体の持ち込みが禁止されているか	
	複製，廃棄	3	作業責任者の許可を得て複製・廃棄する場合は，作業責任者の許可を得て記録し，復元不可能な処理をして廃棄されているか	
	受渡し記録	3	定められた場所以外への持ち出しを行う際は，受渡し記録が付けられているか	
	搬　送	3	情報の送信，情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへ格納されているか	
アクセス制限	入退室制限	3	当該業務関係者以外が許可なく保管場所に立ち入れないようになっているか	
	コンピュータへのアクセス	3	当該業務従事者に限定し，ID・パスワードなどの認証が行われているか	
	安全管理措置	2	PC，サーバ使用時の安全管理措置（ウイルス対策，ネットワーク対策，授受制限等）が行われているか	