別紙１

石川県情報セキュリティ対策要領（外部委託業者）

（趣旨）

第１　この要領は、石川県情報セキュリティポリシーに基づき、外部委託業者が遵守すべき項目を定めるものとする。

（適用資産）

第２　この要領の適用範囲は、情報セキュリティポリシー基本方針第４条に定める適用資産のうち、委託対象のものとする。

（外部記憶媒体の管理）

第３　外部委託業者は、資格のない者による不正利用や情報漏えいを防止するため、県の情報を外部記憶媒体（ＵＳＢメモリ、フロッピーディスク、ＣＤ、ＭＯ、磁気テープ等）に記憶してはならない。

２　前項の規定にかかわらず、県の許可を得た場合は、外部記憶媒体を使用できるものとする。この場合において、外部委託業者は、次に掲げる項目を守らなければならない。

(1) 県の重要な情報を記録した外部記憶媒体の使用者を、あらかじめ必要のある者に限定すること。

(2) 県の重要な情報を記録した外部記憶媒体の複写、送付、持出し及び廃棄する場合は、外部委託業者の責任範囲及び手順を明確にし、県の許可を取得すること。

(3) 県の重要な情報を記録した外部記憶媒体を保管する場合は、外部委託業者の責任範囲及び手順を明確にし、パスワードを設定する等情報の漏えいの防止対策を講じるとともに、施錠できるキャビネット等に保管すること。

(4) 県の重要な情報を記録した外部記憶媒体を送付する場合は、親展の表示、手渡し又は暗号化等の情報漏えい対策を講ずること。

(5) 県の重要な情報を記録した外部記憶媒体の運送を行う場合は、外部委託業者の責任範囲及び手順を県へ報告すること。

(6) 県の重要な情報を記録した外部記憶媒体を廃棄する場合は、県の立会いのもと、情報を電磁的に消去（データ消去プログラムなどで情報を復元できなくすることをいう。）又は裁断する等の物理的な破壊を行うこと。

(7) 県の重要な情報を記録した外部記憶媒体をこれまでの使用目的と違う用途で再利用する場合は、県の立会いのもと、情報を電磁的に消去すること。

(8) 外部記憶媒体の放置を禁止すること。

(9) 外部記憶媒体によって、情報を県に提供する場合は、当該外部記憶媒体について最新のウイルス対策ソフトにより検査を行わなければならない。

（情報の持出し等の禁止）

第４　外部委託業者は、県の庁舎又は外部委託業者等の施設において、委託業務の必要上県の情

報を持出す場合は、県の許可を取得しなければならない。

（情報機器の管理）

第５　外部委託業者は、委託対象の情報機器（情報システムを構成する機器をいう。以下同じ。）の盗難、破壊及び使用資格のない者による保存情報の不正利用を防止するため、次に掲げる項目を守らなければならない。

(1) 外部委託業者は、県の情報を記録した情報機器の存在を定期的に確認すること。

(2) 県が管理する情報機器又は県の情報を記録した情報機器を持出す場合は、県の許可を取得すること。

２　外部委託業者は、外部委託業者等の施設に設置する情報機器に関して、次に掲げる項目を守らなければならない。

(1) 管理体制及び責任範囲を県へ提出すること。

(2) 施錠できる部屋又はラックに格納する等の物理的な保護措置を取ること。

(3) 障害発生時の連絡先を事前に関係者へ周知すること。

(4) 設定変更を行う場合は、県の許可を取得すること。

（情報機器の保守）

第６　保守を行う外部委託業者は、機器の故障を早期に発見又は予防するため、重要な情報を扱う情報機器に対し、保守に関する作業の記録及び保管を行わなければならない。

（情報機器の廃棄及びリース返却）

第７　外部委託業者は、情報機器を廃棄及びリース返却する場合には、情報機器からの情報漏えいを防止するため、委託契約の内容に応じ、以下の項目を守らなければならない。

(1) 情報を電磁的に消去又は記憶媒体を物理的に破壊すること。

(2) 県が所有するソフトウェアのアンインストールすること。

(3) 情報機器の廃棄及びリース返却の記録及び保管すること。

（外部委託業者の持込機器）

第８　外部委託業者は、持ち込んだ情報機器による情報漏えい、ウイルス感染を防止するため、持ち込んだ情報機器をネットワークに接続する場合は、次に掲げる項目を守らなければならない。

(1) 県の許可を得ること。

(2) 必要な情報セキュリティ対策（ウイルス対策ソフトの導入、必要なセキュリティパッチの適用、及びその他必要な情報セキュリティ対策）を実施し、実施状況を確認すること。

(3) 個人所有の情報機器は使用しないこと。

（外部委託業者の義務）

第９　外部委託業者は、情報セキュリティ事故を防止するため、次に掲げる項目を守らなければならない。

(1) 管理体制を明確にして、県に提示すること。
(2) 名札又は身分証明書を着用すること。

(設計開発基準)

第１０　情報システムの設計及び開発を行う外部委託業者は、情報セキュリティ事故発生の防止及び発見を可能とするため、次に掲げる項目を守らなければならない。

(1) 業務で実際に使用しているデータをテストデータとして使用しないこと。ただし、業務上やむを得ず使用する場合は、利用範囲及び利用目的を限定して、県の許可を得た上で必要な保護対策を実施すること。
(2) 開発及び運用で使用する媒体及び資料は、利用する資格のない者が利用できないよう施錠できる部屋又はキャビネット等に保管すること。
(3) 開発した情報システムのテスト計画を作成し、セキュリティ機能の正常動作を確認すること。
(4) 開発した情報システムの導入により、既存システムに影響を及ぼさないことを確認すること。
(5) 設計及び開発する情報システムには、次に掲げる機能を持たせること。
ア　利用者識別子（以下「ユーザＩＤ」という。）により、利用者を個別に識別できる機能。
イ　非表示又は伏せ字などの、入力したパスワードを画面上に表示しない機能。
ウ　情報システム管理者が、ユーザＩＤ及びパスワードを設定及び削除できる機能。
エ　利用者自身でパスワードを変更できる機能。
オ　重要な情報を扱う情報システムの場合には、利用者認証の履歴を収集し保管できる機能。
カ　重要な情報をネットワーク上に送信する場合には、暗号化等の情報漏えいを防ぐ機能。
キ　重要な情報を扱うシステムは、情報の秘匿性等その内容に応じて、暗号化を行う機能。
ク　重要な情報の処理を行う端末を限定する機能。

(アクセス制限)

第１１　利用者管理を行う外部委託業者は、情報システムの利用者を明確にすることによって、不正接続による情報の改ざん、破壊、漏えい又は業務の妨害を防止するため、委託契約の内容に応じて、次に掲げる項目を守らなければならない。

(1) 利用者の登録、変更及び削除の手順を含んだ運用手順を遵守すること。
(2) 重要なシステムのユーザＩＤは、各利用者にそれぞれ割り当てるよう努めること。
(3) 利用者登録は、情報システム管理者が許可した利用者に対してのみ行うこと。
(4) 不要となったユーザＩＤは、速やかに削除すること。
(5) 利用者の登録状況を定期的に確認すること。
(6) 管理者の接続履歴は、不正な利用がされていないか定期的に検査すること。
(7) 発行されたユーザＩＤには、必ずパスワードを設定すること。
(8) パスワードは、類推が困難なものにさせること。
(9) 利用者が管理するパスワードは、定期的に変更させること。
(10) 情報の秘匿性等その内容に応じて、当該情報にアクセスする権限を有する者をその利用目的を達成するために必要最小限の利用者に限ること。

２　アクセスする権限のない外部委託業者は、重要な情報にアクセスしてはならない。

3　外部委託業者は、アクセス権限を有する場合であっても、業務上の目的以外の目的で重要な情報にアクセスしてはならない。

（外部とのデータ交換セキュリティ管理）

第１２　ネットワークを利用して外部とのデータ交換を行う外部委託業者は、県の了解を得ないデータの盗難、改ざん又は誤用を防止するため、次に掲げる項目を守らなければならない。

(1) 使用する回線及び通信方法等の外部とのデータ交換に関する手順を遵守すること。

(2) データ交換は、決められた保存領域で行い、別の領域を使用しないこと。

(3) データ交換後は、保存領域にデータが残らないよう削除すること。

(4) データ交換後には、ファイルサイズ又はデータの一部を交換前のデータと比較する等の確認をすること。

(5) データ交換の接続に先立って交換日程を定めること。

(6) データ交換時には、交換相手、交換日時、交換方法、交換データの内容等について記録すること。

(7) 重要な情報を外部に提供する場合は、県の了解を得ること。

（コンピュータウイルス対策）

第１３　外部委託業者は委託契約の内容に応じ、コンピュータウイルスの感染を防止し、かつ、コンピュータウイルスが発生した場合の被害の拡散を防止するために、次に掲げる項目を守らなければならない。

(1) コンピュータウイルスの予防及び検出のために必要な対策を行うこと。

(2) インターネットを利用するパソコン及びサーバにコンピュータウイルス対策ソフトウェア又はインターネットとの通信を経由する情報機器にコンピュータウイルス対策ソフトウェアを導入すること。

(3) コンピュータウイルス対策ソフトウェアのパターンファイルは、最新の状態に保つこと。

(4) 最新のパターンファイルを利用して、定期的にコンピュータウイルスの検査を行うこと。

(5) 必要なセキュリティパッチをパソコン及びサーバに適用すること。

（ソフトウェア管理）

第１４　外部委託業者は、ソフトウェアのライセンス契約違反を防止し、かつ、不正なソフトウェアの導入によるセキュリティ事故の発生を防止するため、委託契約の内容に応じ、次に掲げる措置を講じなければならない。

(1) ソフトウェアの使用許諾契約に従い、海賊版や偽造品を使用しないこと。

(2) ファイル交換ソフトその他業務上必要のないソフトウェアを使用しないこと。

（ネットワーク管理）

第１５　ネットワークを管理する外部委託業者は、ネットワークの可用性の確保及びネットワークを利用した不正アクセスを防止するため、委託契約の内容に応じ、次に掲げる項目を守らなければならない。

(1) ネットワーク管理に関して、次に掲げる管理資料を作成すること。

ア　ネットワークの構成図

イ　ネットワークの運用管理方法

ウ　ネットワーク接続基準

エ　ネットワーク障害時の対応方法

(2) ネットワーク管理に関する管理資料に不備及び変更がある場合は修正すること。

(3) 重要なネットワーク回線及びネットワーク機器は、障害発生を想定し、必要に応じて二重化等を行うこと。

(4) 総合行政ネットワーク等の外部機関が管理するネットワークとの接続を行う場合は、そのネットワーク接続仕様に従った対策を行うこと。

(5) インターネット等外部のネットワークを経由した接続については、ファイアウォールを構築し、管理するネットワークを保護すること。

(6) 外部のネットワークを経由した接続については、必要に応じてパスワード等による利用者の認識の対策を行うこと。

(7) インターネット利用については、利用者の手順を作成し、セキュリティ事故を未然に防ぐこと。

(8) メールサーバにおいて、メールの送信元、受信先を含めた履歴を取得すること。

(9) ファイアウォール及びルータにおいて、次に掲げる内容を明確に定めること。

ア　通過させるポート番号、通信の方向及び通過させる理由

イ　通信元及び通信先

(10) ファイアウォールを通過させるポート番号は、必要最小限とすること。

(11) ファイアウォールの不正アクセスの履歴を記録すること。

(12) ファイアウォールの設定内容は、外部に公開しないこと。

(外部接続管理)

第１６　外部接続を行っている情報システムを運用する外部委託業者は、外部接続における情報セキュリティ事故の発生を防止するため、委託契約の内容に応じ、次に掲げる項目を守らなければならない。

(1) 外部接続を行う利用者の管理担当者を指定し、利用者を管理すること。

(2) 外部接続を行う利用者を限定すること。

(3) 専用線でない場合は、コールバック（公衆回線で一旦通信を切断し、受信側から登録された送信側へかけなおす方式をいう。）又は発信番号確認等の認証を行うよう努めること。

(4) 外部接続時の接続履歴を取得し、不正アクセスの兆候を発見するよう努めること。

(5) 次に掲げる点を考慮し、外部接続の利用者に関する手順を作成すること。

ア　パスワード等の認証情報の紛失時の再発行手続

イ　利用する際の情報セキュリティの注意点

ウ　電話番号の適切な管理

(6) 異動・退職等の理由により外部接続の必要が無くなった場合は、速やかにユーザＩＤを削除すること。

（情報システム運用手順）

第１７　情報システムを運用する外部委託業者は、情報システム運用の管理及び操作の手順を明確にし、適切で安全な運用を保証するため、委託契約の内容に応じ、次に掲げる項目を守らなければならない。

(1) 情報システム運用手順を作成すること。

ア　運用スケジュール

イ　他の情報システムとの接続

ウ　ソフトウェアの利用制限

エ　重要なデータのバックアップ

オ　接続履歴の記録取得

カ　異常検出時の対処方法

(2) ＯＳ等のうち必要のない機能は停止し、必要のないソフトウェアは削除すること。

(3) 情報システム変更後は、正常動作を確認すること。

(4) 情報システム変更に関わる操作について、操作履歴、情報システム設定値の変更を記録し、保管すること。

(5) 情報システム変更によって、運用方法、操作手順等が変わる場合は、教育計画の作成及び職員への教育を行うこと。

(6) 担当者を変更する場合は、十分な引継資料作成及び引継を行うこと。

(7) セキュリティ事故発生時の連絡体制及び責任について明確にすること。

(8) 重要な情報の記録媒体、処理経路、保管方法について、必要に応じて点検を行うこと。

(9) 重要な情報の内容に誤り等を発見した場合には、県へ報告すること。

（複製等の制限）

第１８　外部委託業者は、情報漏えい、改ざんを防止するため、次に掲げる行為を行う場合は、県の許可を取得しなければならない。

(1)　重要な情報の複製

(2)　重要な情報の送信

(3)　その他重要な情報の適切な管理に支障を及ぼすおそれのある行為

（情報システム安全確保）

第１９　外部委託業者は、情報システムの安全性を確保するため、委託契約の内容に応じ、次に掲げる項目を守らなければならない。

(1) 重要な情報を扱うシステムは、情報の秘匿性等その内容に応じて、当該情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期に又は随時に分析を行うこと。

(2) アクセス記録の改ざん、窃取又は不正な消去の防止を行うこと。

(3) 外部委託業者は、情報システムで取り扱う情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該情報の内容の確認、既存の情報との照合等を行わなければなら

ない。

(4) 外部委託業者は、端末の使用に当たっては、第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行わなければならない。

(5) 重要な情報の改ざん、漏えい、窃取又は不正な消去の防止を行うこと。

(情報セキュリティ事故時の対応)

第２０　外部委託業者は、情報セキュリティ事故の発生時に迅速に対応し、被害の拡大を防止するとともに再発を防止するため、委託契約の内容に応じ、次に掲げる項目を守らなければならない。

(1) 情報セキュリティ事故の発生により、情報システムに影響があった場合は、速やかに県に報告し、回復処置を講じること。

(2) 情報セキュリティ事故発生を想定し、次に掲げる項目についての対応手順を事前に作成すること。

ア　原因の究明

イ　履歴及びそれに該当する証拠物件の収集及び保管

ウ　システム回復手順

(3) 情報セキュリティ事故の対応に関する手順書を必要に応じて見直すこと。

(4) 情報セキュリティ事故からの回復後に、情報システムの正常動作を確認し、県へ原因の調査結果、回復方法及び再発防止策について報告すること。

(情報セキュリティ監査)

第２１　外部委託業者は、情報セキュリティ監査に協力しなければならない。

(その他)

第２２　外部委託業者は、この要領に定めるものの他に、業務内容に応じて、適切な情報セキュリティ対策を実施しなければならない。

(損害の義務)

第２３　外部委託業者の当該要領規定違反により損害が発生した場合、その責めは外部委託業者が負うものとし、県は外部委託業者に対し、その損害の賠償を請求することができるものとする。

附　則

この要領は、平成１８年７月１日から施行する。

附　則

この要領は、平成２０年４月１日から施行する。