|  |  |  |  |
| --- | --- | --- | --- |
| The author/owner of this document is: | This document has been approved for issue by: | Date of issue: | Review date: |
| **Ross Hiddlestone, Nick Boyns** | **Chief Information Security Officer** | **2018** | **2019** |

Contents

[1. Overview 2](#_Toc523430601)

[2. Purpose 2](#_Toc523430602)

[3. Third Party Information Security Pre-Qualification Questionnaire (PQQ) 2](#_Toc523430603)

[4. Contact Information 7](#_Toc523430604)

# Overview

SSE is a leading energy company, operating critical national infrastructure and delivering a number of services to millions of customers. It is reliant on many third parties that provide IT solutions, people, application development, support services, hardware and software products. SSE relies on the integrity and accuracy of its third parties in order to carry out its business obligations to its customers. It is therefore essential that its assets are secured in accordance with its security policies, standards, and its legislative and regulatory obligations, in order to maintain the confidentiality, integrity and availability of its services to its customers. SSE contracts with its third parties must incorporate SSE security policies, Standards and any legislative and regulatory requirements when required.

# Purpose

The purpose of the PQQ (PQQ) is to provide the CRIS Representative and the Procurement Representative and Business Representative with a bank of questions purposed to identify the best third party supplier(s) for the business requirement.

# Third Party Information Security Pre-Qualification Questionnaire (PQQ)

The third party supplier should answer one or more of the questions below, as picked-out by the CRIS Representative in liaison with the Procurement Representative and Business Representative. This will allow an evaluation, leading to the selection of the best third party supplier(s) for the business requirement.

**Please answer the following questions**

**Information Security Questions**

1. **Please indicate the information security standards that your organisation meets. Any response must be applicable to the specific part(s) of the organisation that would supply the services proposed under this PQQ. For example, ISF's Standard of Good Practice for Information Security, ISO-27001, NIST SP-800 Series, COBIT, HIPAA, PCI DSS. Please provide details of certification and audit where applicable. If you apply other controls of your own selection, please explain.**

|  |  |  |
| --- | --- | --- |
| Internationally recognised standard | Compliant since | Date last audited |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Do you currently have the following governance functions? If so, please provide a brief overview how the governance function is managed and maintained.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Governance Function | Overview | Weight | Score | Max Marks |
| There is a corporate information security policy. |  |  |  |  |
| There is a corporate information security management system. |  |  |  |  |
| There are information security functions/roles. |  |  |  |  |
| There are information owners for critical and sensitive data. |  |  |  |  |
| There is a corporate information risk management process. |  |  |  |  |
| Business continuity is assured for critical information functions. |  |  |  |  |
| There is a corporate information security policy. |  |  |  |  |

1. **Do you currently have corporate security policies and/or implement specific security controls to achieve the following? If so, please indicate the method/product/service you use and whether the mechanism meets a recognised standard. Please also provide a reference for your relevant corporate policy document.**

|  |  |  |  |
| --- | --- | --- | --- |
| Security controls and corresponding security policies | Overview | Weight | Score |
| All users must be authenticated to access corporate IT systems. |  |  |  |
| Remote users of IT systems require 2-factor authentication. |  |  |  |
| Only known devices can connect to the corporate network. |  |  |  |
| Password complexity and expiry are prescribed by policy. Those rules are enforced and compliance is monitored. |  |  |  |
| Staff are subject to background screening according to their role. |  |  |  |
| Data on mobile devices is protected in the event of physical loss. |  |  |  |
| All IT systems have specific malware protection. |  |  |  |
| Employees use their own devices safely to access and process company data or they are prohibited from doing so. |  |  |  |
| Systems are patched promptly; exceptions are known and scrutinised by a recognised management process. |  |  |  |
| Data is reliably deleted from obsolete equipment. |  |  |  |
| All cryptographic key material is protected. |  |  |  |
| Sensitive information is labelled consistently and properly . |  |  |  |
| Access to sensitive information is restricted according to need. |  |  |  |
| Important data is routinely backed up to a remote location. |  |  |  |
| Users only run approved applications on corporate IT systems. |  |  |  |
| Security is built in during the design of business applications. |  |  |  |
| There are regular independent security audits. |  |  |  |
| Access to sensitive data is monitored. |  |  |  |
| Security incidents are investigated and trends are reviewed by management. |  |  |  |
| Users’ understanding and adherence to company security policies is measured and reviewed by management. |  |  |  |

**Protection and Data Protection Questions**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Governance Function | Guidance | Answer | Weight | Score |
| Do you have a Data Protection policy? | Please indicate whether your organisation has a Data Protection policy and/or an Information Security policy and to what extent it addresses the following areas:  - Relevant to parts of the organisation that process personal data  - Approved and applied throughout your organisation  - Reviewed and updated on a regular basis  - Defines responsibilities and principles for Data Protection for staff and external parties (including potential consequences of non-compliance)  - Covers key areas of Data Protection (e.g. GDPR compliance)  - Includes appropriate use of electronic systems, such as email and the Internet  - Governs the secure exchange and transfer of personal data outside the organisation and/or overseas (e.g. outside the EEA)  - Communicated effectively to all staff and applicable external parties |  |  |  |
| Do you have a valid and up to date registration (if relevant) to process personal data as required under Data Protection Legislation? | Under applicable Data Protection Legislation there are local registration duties requiring a Data Controller (and in certain jurisdictions a Data Processor) to notify to the appropriate supervisory authorities (e.g. the UK Information Commissioner) details of their processing and disclosure of personal data. |  |  |  |
| Have you established responsibility for managing Data Protection within your organisation? | Please outline how responsibility for Data Protection has been allocated and communicated within your organisation, for example whether your organisation has an appointed Data Protection Officer, Data Protection Committee or similar governance function. |  |  |  |
| Are measures taken to safeguard SSE Personal Data that is transferred outside the organisation, including data transferred overseas? Please provide details. | Please describe how electronic and physical SSE data is protected when transferred outside of the organisation and overseas.  If data is transferred to other countries please list the countries that SSE data is transferred to and indicate how your organisation ensures that the destination country applies the appropriate mechanisms to protect SSE Personal Data, including whether you notify SSE prior to changes in how your organisation transfers SSE data outside the organisation.  Please indicate where your organisation utilises the following to protect data when being disclosed or transferred:  - Techniques to prevent unauthorised disclosure of SSE Personal Data, including use of encryption and password protected files  - Protection Shield (for US transfers)  - EU Approved Model Contractual Clauses  - Other forms of inter-group and third party agreements  - Consent of the Data Subject  Note: Your response should also include the controls applied to the exchange of data between your organisation and SSE. |  |  |  |
| Do you have an incident management process which applies to SSE Personal Data? | Where relevant, please indicate whether you have a process in place for dealing with complaints around inaccuracies of personal data and subject access requests and if so please indicate to what extent this process addresses the following (NB: The intent of this question is to understand about your process for handling queries regarding the accuracy of personal data, and not breaches of personal data).  - Identification and tracking of responses  - Logging of changes made to personal data  - Appropriate verification of complainant prior to disclosing or updating personal data  - Periodic data quality reviews and QA procedures around processes involving manual and automated updates and migration of data  - Root cause analysis and mitigation |  |  |  |
| Do your employment contracts or Terms and Conditions (T&Cs) specifically mention staff Data Protection responsibilities? | If your Data Protection responsibilities are included in employment contracts and T&Cs, to what extent have the following aspects been addressed for staff, agents and contractors that will have access to personal data:  - Data Protection responsibilities for all staff specified in job descriptions and T&Cs  - Data Protection responsibilities extend outside normal hours and beyond the duration of the contract, further explain employee’s legal responsibilities, and include appropriate non-disclosure/confidentiality clauses  - Staff required to sign contracts, and external personnel are required to sign non-disclosure/confidentiality agreements  - Communicated and documented disciplinary measures for data breaches caused by employees and contractors failings |  |  |  |
| Do you have security measures in place for SSE Personal Data that may be saved on physical media and transported outside the organisation's premises? | Please indicate whether physical media is used to transport SSE Personal Data. If so, please describe how the following areas are addressed:  - Govern physical media transport though formally defined policies and procedures for secure transfer and storage  - Protect physical media from being tampered with while transported  - Prevent physical media from being accessed or copied (e.g. encryption)  - Track of physical media from point of origin to destination, including controls for approved transfer, labelling, receipt confirmation, and completeness check  - Dedicated couriers for physical data with relevant confidential clauses in place |  |  |  |
| Do you have processes and procedures in place for the secure deletion and destruction of SSE Personal Data? | Please indicate if formalised processes and procedures are in place and if so to what extent they address the following areas:  - Decommissioning or reusing computer equipment within your organisation (e.g. secure deletion of hard drive data before it is sold, discarded or passed to a new user)  - Secure storage and disposal of confidential physical waste (e.g. requirements for the use of confidential waste bins, shredders and third party data disposal organisations) |  |  |  |
| Is there a process to govern the selection and management of your third parties handling SSE Personal Data? | Please confirm to what extent processes are formalised and followed for establishing and managing sub-contractor relationships including processes to:  - Select sub-contractors  - Evaluate risks to cover general and business specific issues, sensitive and critical environments, business and IT standards and practices for sub-contractor, interdependencies, and exit strategies  - Define and agree contracts (including Data Protection control requirements)  - Develop contingency arrangements  Please also outline any activities which are undertaken to establish the level of security within a selected sub-contractor (e.g. due diligence, regular security reviews etc.) and confirm to what extent these processes are formalised and documented.  If no sub-contractors are used to process personal data please enter "N/A" |  |  |  |
| Do you have contracts in place with sub-contractors working with SSE Personal Data? | Please indicate if there are any sub-contractor relationships which involve the processing or handling of personal data exchanged through your relationship with SSE and if so confirm whether appropriate contracts are in place in all such instances.  If no sub-contractors are used to process personal data please enter "N/A" |  |  |  |

# 4. Contact Information

For more information regarding this PQQ: or any policies or standards published by Cyber Risk & Information Security, please email information.security@sse.com.