|  |
| --- |
| **SUPPLY CHAIN****ENQ-COR-CS-FOR-00001**  |
| **THIS DOCUMENT IS CLASSIFIED AS NON-CRITICAL**  |
| **Supplier Self-Assessment Questionnaire**  |
|  **APPLICABILITY:**  |
| **Document Owner** | Supply Chain Manager |
| **Legacy Number** |  |
| **Revision** | C5 | **Issue Date** | 20/07/2022 | **Next Review Date** | N/A |

**EnQuest, Annan House, Palmerston Road, Aberdeen, AB11 5QP, Tel: 01224 975000**

**Revision History**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Rev** | **Reason for Issue** | **Created By**  | **Job Title** | **DD** | **MM** | **YYYY** |
| C1 | First issue on BMS | C. Taylor | Supply Chain Analyst | 08 | 01 | 2018 |
| C2 | Updated to give credit for key certifications | C. Taylor | Business Services Coordinator | 04 | 05 | 2021 |
| C3 | Updated to include sections on D&I and GDPR | C. Taylor | Business Services Coordinator | 02 | 02 | 2022 |
| C4 | Updated to include Cyber security question set | C. Taylor | Business Services Coordinator | 05 | 07 | 2022 |
| C5 | Updated HSEA Section | C. Taylor | Business Services Coordinator | 20 | 07 | 2022 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Revision Change Notices**

|  |  |  |
| --- | --- | --- |
| **Rev** | **Location of Changes** | **Brief Description of Changes** |
| **C2**  | **Throughout**  | **Tidy up and reduced input if suppliers has key ISO certifications** |
| **C3** | **Section 19****Section 20** | **Addition of GDPR section****Addition of equality, diversity, inclusion and wellbeing section** |
| **C4** | **Section 21** | **Addition of cyber security questions**  |
| **C5** | **Section 3** | **HSEA** |

**CONTENTS**

1.0 Company Information 4

2.0 Management System Registration 4

3.0 Health, Safety, Environment and Assurance 5

4.0 HSE&A Responsibility and Authority 10

5.0 Contract Review 10

6.0 Internal Audits and Control of Records 10

7.0 Document Control 10

8.0 Competency and Training 11

9.0 Contract and Order Review 11

10.0 Maintenance 12

11.0 Inspection, Testing and Verification 12

12.0 Customer Owned Property 12

13.0 Non-Conformances 13

14.0 Remedial and Preventive Action 13

15.0 Supplier Management 13

16.0 Warehouse, Packaging and Delivery 14

17.0 Anti-Corruption and Bribery 14

18.0 Compliance with Modern Slavery Legislation 14

19.0 GDPR 15

20.0 Equality, Diversity, Inclusion and Well Being 16

21.0 Cyber Security 17

**22.0 Required Documents…………………………………………………………..…21**

Decision 23

1. Company Information

|  |
| --- |
| Company name:  |
| Company address:  |
|  |
|  |
| Number of years in business:  | Number of employees: |
| Contact phone number:  | Contact email contact:  |
|  |  |
| Name EnQuest Account Representative:  | Title:  |
| Survey completed by: | Title:  |
| Describe the Products or Services provided to EnQuest:  |

1. Management System Registration

|  |
| --- |
| Is your management system certified? If so please provide details below. Yes [ ]  No [ ]  (Attach any certificate with the submission)  |
| System: | Certification No. | Expiration date:  |
| System: | Certification No. | Expiration date: |
| System: | Certification No. | Expiration date: |
|  |  |  |

|  |
| --- |
| Comments, including scope of certification: |

1. Health, Safety, Environment and Assurance

If you are certified to ISO 45001, 14001 & 9001 please go directly and complete from section 16 onwards.

|  |
| --- |
| **Leadership & Management** |
|  | Does your company have a documented HSEA Policy?  | Yes [ ]  No [ ]  |
|  | Is the HSEA Policy owned & approved by the company Board? | Yes [ ]  No [ ]  |
|  | Has the HSEA policy been communicated to all employees? | Yes [ ]  No [ ]  |
|  | Is an organisational chart or other means of defining and communicating authority and responsibility within the organisation available? | Yes [ ]  No [ ]  |
|  | Are HSEA roles and responsibilities defined within employee job descriptions? | Yes [ ]  No [ ]  |
|  | Is there a management representative for HSEA issues?Name: Title: | Yes [ ]  No [ ]  |
|  | Do you have a Safety & Environmental Management System detailing Health, Safety, Environmental and Audit processes? | Yes [ ]  No [ ]  |
|  | Has the Management System been audited and approved by an independent body within the past 2 years e.g., to meet a recognised standard such as ISO45001? | Yes [ ]  No [ ]  |
| If yes, please provide details i.e., name company, date and standard: |
|  | Does the Management System address the management of sub-contractors? | Yes [ ]  No [ ]  |
|  | Does the Management System address the requirement for Health Surveillance of your workforce? | Yes [ ]  No [ ]  |
|  | Are management reviews of the Management System held and records maintained? | Yes [ ]  No [ ]  |
|  | Are formal corrective actions defined, and reviewed following Management Review? | Yes [ ]  No [ ]  |
|  | Does your company have a HSE Management Interface Document with EnQuest?  | Yes [ ]  No [ ]  |
| If so, does it address any specialist action that needs to be taken in an emergency? | Yes [ ]  No [ ]  |
| How has this this been communicated to your workforce? |
|  | Do you have defined HSEA performance metrics i.e., annual KPIs? | Yes [ ]  No [ ]  |
|  | Has your company suffered any statutory notifiable incidents in the past year?  | Yes [ ]  No [ ]  |
| If so, please provide details: |
|  | Do you have a process for learning from incidents and sharing HSE information? | Yes [ ]  No [ ]  |
|  | Do you compare your HSE performance with others in your sector / beyond? | Yes [ ]  No [ ]  |
|  | Are you a member of any industry or trade bodies, e.g. OEUK, Step Change in Safety?  |  |

|  |
| --- |
| **Workforce Engagement** |
| **3.19** | Do you have a Safety Committee with workforces Safety / Trade Union Representatives? | Yes [ ]  No [ ]  |
| **3.20** | Does the Safety Committee meet regularly with the Management team? | Yes [ ]  No [ ]  |
| **3.21** | Do you provide resources, including access to HSE specific training for these representatives? | Yes [ ]  No [ ]  |
| **3.22** | Do you have a Welfare Committee and/or Wellness programmes? | Yes [ ]  No [ ]  |
| **3.23** | Do you have a means for recording risk assessments relevant to the work you are undertaking? | Yes [ ]  No [ ]  |
| **3.24** | Are employees knowledgeable about the task involved in creating and reviewing these risk assessments? | Yes [ ]  No [ ]  |
| **3.25** | Do personnel have the authority to ‘stop the job’ if they believe it to be unsafe? | Yes [ ]  No [ ]  |
| **3.26** | Do employees have a means to feedback on HSE or QA/QC concerns? | Yes [ ]  No [ ]  |
| **Competency** |
| 3.27 | Have minimum competency requirements for your workforce been established? | Yes [ ]  No [ ]  |
| 3.28 | Is training, education and work experience for personnel documented? | Yes [ ]  No [ ]  |
| 3.29 | Does this extent to contractors / sub-contractors? | Yes [ ]  No [ ]  |
| 3.30 | Are there formal training programmes, including refresher training, in place for individuals whose work has a direct effect on HSE and/or QA/QC? | Yes [ ]  No [ ]  |
| 3.31 | How are the training requirements identified?* Training Matrix
 | Yes [ ]  No [ ]  |
| 3.32 | How does an individual identify their training requirements?* Training matrix
 | Yes [ ]  No [ ]  |
| 3.33 | How is refresher training identified, individual informed, recorded/completed?* Is there a formalised notification process
 | Yes [ ]  No [ ]  |
| 3.34 | Individual competence records accurately reflect the current legislative and operational requirements of the job role (as per Oil and Gas UK Guidelines) and are made available to appropriate company representatives as required.* Each individual working on a EnQuest location has the required operations competence and understanding of current legislative requirements relating to a specific job role.

Have you provided evidence of such assessments as an attachment? | Yes [ ]  No [ ]  |
|  | Comments: |
| 3.35 | How do you ensure competency and training are up to date and meet the required standard? *Please add the detailed explanation as an attachment, where necessary.* | Yes [ ]  No [ ]  |
| 3.36 | Please also provide a copy of the competency matrix (record) for personnel deployed at EnQuest Assets / Sites or Offices. Have you provided the copy as an attachment? | Yes [ ]  No [ ]  |
| 3.37 | Do you have enough competent personnel to cover absences? | Yes [ ]  No [ ]  |
| 3.38 | Do you align your working processes with human performance incl. fatigue management and safety critical task guidance? | Yes [ ]  No [ ]  |
| 3.39 | What formalised competency strategy/framework/process documents are in place?* Is there anything formalised to ensure consistency and to establish guidelines?
 | Yes [ ]  No [ ]  |
| 3.40 | What KPI’s are in place to measure performance/progress? | Yes [ ]  No [ ]  |
| 3.41 | How are competency assurance processes internally assessed?* Client feedback, audits, systems, processes
* Routine internal and external audits
 | Yes [ ]  No [ ]  |
| 3.42 | Competence assessment* Are a variety of assessment methods used? – direct observation, information gathering, written and verbal questioning
* Are there different levels of competency used? i.e. awareness, perform under supervision, perform unsupervised, expert
 | Yes [ ]  No [ ]  |
| 3.43 | How would new roles which may not presently be included in the competence system be developed and implemented?* Training matrix/job description
 | Yes [ ]  No [ ]  |
| **Environment** |
| 3.44 | Do you have environmental specific objectives? | Yes [ ]  No [ ]  |
| If so, do these go beyond Environmental Legal Compliance (e.g. the minimum requirements)? | Yes [ ]  No [ ]  |
| 3.45 | Has your company been responsible for or played a part in any statutory notifiable environmental incidents in the past year? | Yes [ ]  No [ ]  |
| If so, please provide details, e.g. Pon1, Non-Compliance, SEPA Notification: |  |
| 3.46 | Do you have Environmentally Critical Elements/Equipment (ECE’s)? | Yes [ ]  No [ ]  |
| If so, do you have a process to identify, inspect and maintain ECE’s? | Yes [ ]  No [ ]  |
| 3.47 | Is your Environmental Management System independently verified or certified? | Yes [ ]  No [ ]  |
| If so please provide details, e.g. date, verification body, verified with comments etc.: |  |
| 3.48 | Do you have a process for maintaining your Environmental Management System (EMS) documentation? | Yes [ ]  No [ ]  |
| 3.49 | Do you have site specific Waste Management Plans? | Yes [ ]  No [ ]  |
| 3.50 | Do you have an Aspects & Impacts Register? | Yes [ ]  No [ ]  |
| 3.51 | Do you have a sustainability plan? | Yes [ ]  No [ ]  |
| 3.52 | Do you monitor and report atmospheric emissions?  | Yes [ ]  No [ ]  |
| Are your atmospheric emissions independently verified? | Yes [ ]  No [ ]  |
| If so, please provide details, e.g. types of emissions monitored, verification body: |  |
| 3.53 | Have you set emissions reduction targets? | Yes [ ]  No [ ]  |
| If so, provide details: |  |
| 3.54 | Do you have an Emissions Reduction Action Plan (or similar)? | Yes [ ]  No [ ]  |
| 3.55 | Are you investing in any new technologies/techniques (including studies into such) to improve environmental performance? | Yes [ ]  No [ ]  |
| If so, please provide details: |  |
| 3.56 | Are there any additional environmental initiatives or monitoring activities, not mentioned above, your company is doing? | Yes [ ]  No [ ]  |
| If so, please provide details: |  |
| **Quality & Assurance** |
| 3.57 | Does a defined system exist for communicating customer requirements between departments? | Yes [ ]  No [ ]  |
| 3.58 | Does the department responsible for Quality have the authority to control further processing and delivery of products and services until the unsatisfactory condition has been corrected? | Yes [ ]  No [ ]  |
| 3.59 | Does the organisation have a defined process to measure customer satisfaction?  | Yes [ ]  No [ ]  |
| 3.60 | Are internal audits or self-assessments performed with results documented and reported to management? | Yes [ ]  No [ ]  |
| 3.61 | Are records of internal audits kept? | Yes [ ]  No [ ]  |
| 3.62 | Are the retention periods of the records specified? | Yes [ ]  No [ ]  |
| 3.63 | Are records adequately protected against damage or accidental destruction? | Yes [ ]  No [ ]  |
| 3.64 | Are procedures defined to determine the responsibility for record disposition post retention period? | Yes [ ]  No [ ]  |
| 3.65 | Do you have a defined process for Managing Change? | Yes [ ]  No [ ]  |
| **Comments:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. HSE&A Responsibility and Authority

|  |  |  |
| --- | --- | --- |
| 4.1 | Does the department responsible for HSE&A report directly to the Head of organisation? | Yes [ ]  No [ ]  |
| 4.2 | Does the department responsible for Quality have the authority to control further processing and delivery of products and services until the unsatisfactory condition has been corrected? | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

 |

1. Contract Review

|  |  |  |
| --- | --- | --- |
| 5.1 | Are all customer contracts / purchase orders reviewed prior to start of work? | Yes [ ]  No [ ]  |
| 5.2 | Is the HSE & A department involved in this review? | Yes [ ]  No [ ]  |
| 5.3 | If a problem arises which may impact the quality, quantity, or delivery of the contract, is the customer notified? |  |
| Yes [ ]  No [ ]  |
| 5.4 | Are operations suspended until written response is obtained from customer? |  |
| Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

 |

1. Internal Audits and Control of Records

|  |  |  |  |
| --- | --- | --- | --- |
| 6.1 | Are internal audits or self-assessments performed with results documented and reported to management? |  |  |
| Yes [ ]  No [ ]  |  |
| 6.2 | Are records of internal audits kept? | Yes [ ]  No [ ]  |  |
| 6.3 | Are the retention periods of the records specified? | Yes [ ]  No [ ]  |  |
| 6.4 | Are records adequately protected against damage or accidental destruction? |  |  |
| Yes [ ]  No [ ]  |
| 6.5 | Are procedures defined to determine the responsibility for record disposition post retention period? |  |  |
| Yes [ ]  No [ ]  |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  |  |

1. Document Control

|  |  |  |
| --- | --- | --- |
| 7.1 | Is there a process related to the control of documents? | Yes [ ]  No [ ]  |
| 7.2 | Does this process contain facility for document review, update and approval? |  |
| Yes [ ]  No [ ]  |
| 7.3 | Is there a system in place for document revision identification? | Yes [ ]  No [ ]  |
| 7.4 | Is there a process in place to preclude the unintended use of obsolete documents? |  |
| Yes [ ]  No [ ]  |
| 7.5 | Is the distribution of documents of internal and external origin controlled? (Standards, customer drawings, etc.) |  |
| Yes [ ]  No [ ]  |
| 7.6 | Are external documents controlled?If so how is it ensured the latest revision is available? | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |

1. Competency and Training

|  |  |  |
| --- | --- | --- |
| 8.1 | Have minimum competency requirements been established? | Yes [ ]  No [ ]  |
| 8.2 | Is training, education and work experience for personnel documented? | Yes [ ]  No [ ]  |
| 8.3 | Are there formal training programs for individuals whose work has a direct effect on quality? | Yes [ ]  No [ ]  |
| 8.4 | For personnel provided in positions identified as minimum positions for Competency Assessments (as per Oil and Gas UK Guidelines).Have you provided evidence of such assessments as an attachment?  | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

 |
| 8.5 | Please also explain how you ensure competency and training are up to date and meet the required standard.Please add the detailed explanation as an attachment, where necessary. |
|

|  |
| --- |
| Explanation:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |
| 8.6 | Please also provide a copy of the competency matrix (record) for personnel deployed at EnQuest Assets / Sites or Offices. Have you provided the copy as an attachment? | Yes [ ]  No [ ]  |

1. Contract and Order Review

|  |  |  |
| --- | --- | --- |
| 9.1 | Is there a process in place for Purchase order and contract review to ensure customer requirements are met? | Yes [ ]  No [ ]  |
| 9.2 | Do this process include a clear means for communicating to the customer any build or specification issues? | Yes [ ]  No [ ]  |
| 9.4 | Are exceptions to contract requirements resolved before acceptance of a contract? | Yes [ ]  No [ ]  |
| 9.5 | Are order and contract reviews documented? | Yes [ ]  No [ ]  |
| 9.6 | Is there a process for communicating changes to a customer order among affected departments? | Yes [ ]  No [ ]  |
| 9.7 | Is there a process for communicating changes to the customer which may affect operation, obsolescence or safety? | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |

1. Maintenance

|  |  |  |
| --- | --- | --- |
| 10.1 | Are validation records for process or service provision available?  | Yes [ ]  No [ ]  |
| 10.2 | Is the organisation's production equipment on a scheduled maintenance program?  |  |
| Yes [ ]  No [ ]  |
| 10.3 | Are planned maintenance shutdowns addressed in production scheduling?  |  |
| Yes [ ]  No [ ]  |
| 10.4 | Is maintenance and repair work conducted in accordance with documented procedures?  |  |
| Yes [ ]  No [ ]  |
| 10.5 | Are maintenance and repair work documented and records up to date?  | Yes [ ]  No [ ]  |

1. Inspection, Testing and Verification

|  |  |  |
| --- | --- | --- |
| 11.1 | Do supplied materials and components undergo inspection, test or other means of verification upon receipt? | Yes [ ]  No [ ]  |
| 11.2 | Are processes defined and implemented for incoming materials inspections?  | Yes [ ]  No [ ]  |
| 11.3 | Does the process prevent uninspected materials being incorporated into equipment or processes?  | Yes [ ]  No [ ]  |
| 11.4 | Are inspection processes and test procedures defined clearly?  | Yes [ ]  No [ ]  |
| 11.5 | When required by contract, does the organisation control the implementation of customer's procedures?  | Yes [ ]  No [ ]  |
| 11.6 | Is the inspection status of the product readily apparent?  | Yes [ ]  No [ ]  |
| 11.7 | Has the organisation documented and implemented final test and inspection procedures?  | Yes [ ]  No [ ]  |
| 11.8 | Are all tests and inspections documented and records maintained, including results of non-conformance?  | Yes [ ]  No [ ]  |
| 11.9 | Does the business management system prevent the final release of un-inspected equipment or processes?  | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |

1. Customer Owned Property

|  |  |  |
| --- | --- | --- |
| 12.1 | Is there process in place to identify customer property?  | Yes [ ]  No [ ]  |
| 12.2 | Are there adequate facilities available to store and protect customer property?  |  |
| Yes [ ]  No [ ]  |
| 12.3 | Are records maintained of reporting lost, damaged or unacceptable materials to the customer who supplied them?  | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |

1. Non-Conformances

|  |  |  |
| --- | --- | --- |
| 13.1 | Is there a documented process for the control of non-conforming products?  | Yes [ ]  No [ ]  |
| 13.2 | Does the process require the identification, documentation, evaluation and handling of the non-conforming product?  | Yes [ ]  No [ ]  |
| 13.4 | Are instances of nonconforming product documented?  | Yes [ ]  No [ ]  |
| 13.5 | Are reworked items re-inspected and retested?  | Yes [ ]  No [ ]  |
| 13.6 | Are records of any re-inspection maintained and available? | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |

1. Remedial and Preventive Action

|  |  |  |
| --- | --- | --- |
| 14.1 | Is there a process for investigating and implementing corrective actions to prevent recurrence of non-conformance? | Yes [ ]  No [ ]  |
| 14.2 | Are all non-conformances subjected to this process? | Yes [ ]  No [ ]  |
| 14.3 | Are records of corrective actions maintained and shared? | Yes [ ]  No [ ]  |
| 14.4 | Are NCRs investigated and actions shared with customers?  | Yes [ ]  No [ ]  |
| 14.5 | Is the progress of corrective/preventive action monitored? | Yes [ ]  No [ ]  |
| 14.6 | Are corrective / preventive actions reviewed for effectiveness when completed? | Yes [ ]  No [ ]  |
| 14.7 | Are records of preventive actions available? | Yes [ ]  No [ ]  |
| 14.8 | Does the HSE & A department review all Corrective and Preventive actions including customer generated Non-Conformance Reports (NCRs)?  | Yes [ ]  No [ ]  |
| 14.9 | Does the organisation have an effective means of measuring continual improvement? | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |

1. Supplier Management

|  |  |  |
| --- | --- | --- |
| 15.1 | Do you have a documented process for selecting and evaluating suppliers? | Yes [ ]  No [ ]  |
| 15.2 | Are supplier assessments and reviews documented and records maintained? | Yes [ ]  No [ ]  |
| 15.3 | Is there a list of approved suppliers maintained and available? | Yes [ ]  No [ ]  |
| 15.4 | Are purchases only made from approved suppliers? | Yes [ ]  No [ ]  |
| 15.5 | Is supplier performance periodically re-evaluated? | Yes [ ]  No [ ]  |
| 15.6 | Do suppliers go through formal pre-qualification process before placement of contracts or orders? | Yes [ ]  No [ ]  |
| 15.7 | Do you have a process for regular supplier audits and performance management? | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

 |

1. Warehouse, Packaging and Delivery

|  |  |  |
| --- | --- | --- |
| 16.1 | Are there processes in place for handling, storing, packaging and protecting the product?  | Yes [ ]  No [ ]  |
| 16.2 | Are materials handled in accordance with documented procedures?  | Yes [ ]  No [ ]  |
| 16.3 | Are the procedures designed to protect the integrity of the handled material as well as personnel?  | Yes [ ]  No [ ]  |
| 16.4 | Is appropriate handling equipment available as and when needed?  | Yes [ ]  No [ ]  |
| 16.5 | Are storage areas and conditions appropriate to the nature of the goods held in them?  |  |
| Yes [ ]  No [ ]  |
| 16.6 | Are inward and outward movements from warehouse areas controlled and properly authorized?  | Yes [ ]  No [ ]  |
| 16.7 | Are components with limited shelf life audited and evaluated routinely?  | Yes [ ]  No [ ]  |
| 16.8 | Are records of these audits maintained and available?  | Yes [ ]  No [ ]  |
| 16.9 | Are customer requirements for packaging reviewed and evaluated for adequacy?  | Yes [ ]  No [ ]  |
| 16.10 | Does packaging, including identification, comply with all relevant statutory requirements?  | Yes [ ]  No [ ]  |
| 16.11 | Are delivery methods evaluated to ensure that they preserve the quality of the supplied items?  | Yes [ ]  No [ ]  |
| 16.12 | Is product quality preserved between final test and inspection and acceptance by the customer?  | Yes [ ]  No [ ]  |
|

|  |
| --- |
| Comments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. Anti-Corruption and Bribery

|  |  |  |
| --- | --- | --- |
| 17.1 | Does your company have a regularly monitored anti-corruption code of conduct documenting your anti-corruption and bribery policies and procedures? | Yes [ ]  No [ ]  |
| 17.2 | Is this anti-corruption code of conduct known and acted upon by all employees of your company? | Yes [ ]  No [ ]  |
| 17.3 | Is this anti-corruption code of conduct publicised internally and externally? | Yes [ ]  No [ ]  |
| 17.4 | Does your company carry out documented risk assessments of its potential exposure to corruption and bribery? | Yes [ ]  No [ ]  |
| 17.5 | Does your company apply due diligence procedures for persons who perform or will perform services for or on behalf of the organisation, to mitigate identified bribery risks? | Yes [ ]  No [ ]  |

|  |
| --- |
| Comments:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. Compliance with Modern Slavery Legislation

|  |  |  |
| --- | --- | --- |
| 18.1 | Is your company required by section 54 of the Modern Slavery Act to produce an annual statement setting out the steps that have been taken to ensure your company and supply chains are slavery free? | Yes [ ]  No [ ]  |
| 18.2 | Does your company have a policy on modern slavery and human trafficking? (this may form part of your company’s wider CSR policy) | Yes [ ]  No [ ]  |
| 18.3 | Does your company carry out documented risk assessments of its business and supply chain to ensure continuous compliance with relevant statutory requirements? | Yes [ ]  No [ ]  |

|  |
| --- |
| Comments:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. GDPR

|  |  |  |
| --- | --- | --- |
| 19.1 | Please confirm that you hold or process data of any kind on behalf of the Data Controller. | Yes [ ]  No [ ]  |
| 19.2 | Are you required to maintain documented records for processing activities you carry out?This includes back-up and retained data | Yes [ ]  No [ ]  |
| 19.3 | Do you maintain documented records for processing activities you carry out? Do you (or any sub-processors) process data on behalf of the Data Controller anywhere outside the EU/EEA? | Yes [ ]  No [ ]  |
| 19.4 | Do you have any relevant security certifications that your organisation holds?If Yes, submit copies of the certificate. | Yes [ ]  No [ ]  |
| 19.5 | Do you have a Data Protection policy in place to mitigate risks to personal data? | Yes [ ]  No [ ]  |
| 19.6 | When personal data is no longer required for processing, do you delete or return all personal data? | Yes [ ]  No [ ]  |
| 19.7 | Do you collect personal data from the data subjects on behalf of the Data Controller?When collecting data from the data subjects, do you ensure that there is an appropriate legal basis for collection?Appropriate lawful bases for data collection are: consent, contractual agreement, legal obligation, vital interests, public interest, or legitimate interest. See ICO's guidance on lawful basis for processing. | Yes [ ]  No [ ]  |
| 19.8 | Do you have a process for: erasing personal data when requested by the Data Subject? | Yes [ ]  No [ ]  |
| 19.9 | Do you inform all EU based citizens when collecting their personal data? (i.e. via website, privacy notice, statement, etc). | Yes [ ]  No [ ]  |
| 19.10 | Does your organisation have a tested and documented incident response plan and breach notification that meets the GDPR's 72-hour notification requirement? | Yes [ ]  No [ ]  |
| 19.11 | Does your organisation have offices outside the EU/EEA? | Yes [ ]  No [ ]  |
| 19.12 | Does your organisation have a Data Protection Officer (DPO)?A DPO is required for organisations in the following cases:- You are a public authority or body- Your primary business activities consist of processing activities, which, by virtue of their nature, scope and/or their purposes, require the regular and systematic monitoring of individuals on a large scale (e.g. tracking/ profiling/behavioural advertising)- Your primary business activities consist of processing on a large scale of special category data, or data relating to criminal convictions and offences | Yes [ ]  No [ ]  |

1. Equality, Diversity, Inclusion and Well Being

20.1 Do you have a corporate Diversity & Inclusion Policy and / or Strategy or similar? If so please provide

20.2 Provide information on most recent gender pay gap data, and a plan to reduce if a gap does exist?

20.3 Is your organisation a member of any groups that promote diversity and inclusion practises – such as AXIS Network, AFBE (Association for Black and Ethnic Minority Engineers)?

20.4 Does your company have any Employee Resources Groups (ERGs) that support the workforce in specific areas – wellbeing, diversity and inclusion etc if so please provide an overview.

20.5 What benefits does your company provide employees to help with their overall well being? For example – private health car, employee assistance program, mindfulness sessions etc.

20.6 Do you have a names Diversity and Inclusion Leader for your company?

20.7 Do you have a non-discrimination or equal opportunity statement in your organisation?

20.8 Do you have any corporate goals and metrics on diversity hiring?

20.9 Do you have any corporate goals and metrics in promotion and executive appointments?

20.10 Please provide the gender and ethnicity split of your board of directors

20.11 Please provide the gender and ethnicity split of your management

20.12 Please provide the gender and ethnicity split of your overall employees

20.13 Do you provide any diversity, equality and inclusion training programs to your employees?

20.14 Have you received any industry awards, or recognition in the last 5 years for diversity and inclusion, or work place engagement?

20.15 Are you a certified diverse-owned enterprise?

1. Cyber Security

21.1 Governance and Risk Management

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. How does your company manage and govern cyber risk at the level of strategy and policy/standards?
 | *Describe how your company’s cyber risk strategy/policy is:**- Created, - Approved, - Delivered, - Measured and reported, - Directed, - And how deviations are escalated.**Please include details of at which organisational level each of these is completed.* |
| 1. How do you assess and communicate the respective security responsibilities between you and your customers?
 | *As part of contracting how do you define security responsibilities for yourselves and your customers? Please share an illustrative example if you have one.* |
| 1. When engaging with a customer what processes do you operate to understand the cyber risks they face and the implications this has for what you need to do?
 | *Please describe any process you use pre- and post-contract to identify and agree the security requirements of the customer. What do you do to reflect security requirements arising from and any broader legal, regulatory, or national Critical National Infrastructure (CNI) implications?* |

21.2 Cyber Security Capability and Competence

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. Please describe how cyber security responsibilities are defined and supported for key delivery roles which are not full-time security jobs (such as for engineers or general IT professionals)?
 | *What security responsibilities are formally defined in roles and responsibilities and is there any training or certification? If you have a relevant competency model, please describe this.* |
| 1. Please describe the general organisation for any full-time cyber security professionals and the reporting line of the most senior cyber security professional.
 | *An organisation chart or description of reporting line would be helpful together with any certifications held. Use job titles or roles rather than naming individuals.* |
| 1. If you use external cyber security expertise (such as consultants or security services) what type of tasks do they perform?
 | *For example, managed security service providers, consultancies, penetration testing companies. You need not name the specific company unless you wish to.* *What certifications do they have?* |

21.3 Frameworks, Policies and Targets

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. What industry cyber security frameworks/series of standards do you use to measure your security activity and how do you define your goals and internal standards against these?
 | *Examples might be the NIST Cyber Security Framework, ISO 27001, the UK NCSC Cyber Assurance Framework and/or the UK HSE OG86 guidance. You should state which security framework(s)/standard(s) you have chosen and how you measure your activity using them.* |
| 1. What cyber security certifications do you hold for your company and what scope of coverage/applicability do they cover?
 | *Provide details of any relevant certification the relevant part of your business has obtained and provide the scope this covers? Examples could include ISO27001/2, Cyber Essentials or Cyber Essentials Plus.*  |
| 1. How do you keep up with legal and regulatory requirements for cyber security in the regions and countries in which you deliver your services/products?
 | *As well as describing any monitoring process, you may wish to reference any legal or regulatory compliance you measure yourself against (e.g. PCI-DSS, Smart Energy Code, NIS, Data Protection, controls on use of encryption etc.)* |
| 1. How do you learn about current and emerging cyber security threats to adjust your security goals?
 | *How do you keep up with changing threats (where do you get the information) and what do you do in response to any changes?* |

21.4 Culture, Training and Awareness

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. What background checks do you perform on employees and contractors and how often are these repeated?
 | *Background checks can start with simple thorough checking of references and go through to BS7858 criminal record and other vetting up to national security levels (SC, DV etc) provided for Critical National Infrastructure (CNI) roles.*  |
| 1. How do security requirements get included into employment contracts and made part of performance measures for staff and contractors?
 | *What security obligations are part of employment contracts for staff and contractors? How do security actions and behaviours get included in staff appraisals or objective setting?* |
| 1. How do you provide cyber security guidance and supporting training and awareness for staff and contractors? How do you assess the effectiveness of this?
 | *What security training do you require for general staff to ensure security competency in their role and how do you measure outcomes? What do you do for special or ‘privileged’ roles?* |
| 1. What actions do executives and managers take to set the tone to encourage a positive security culture?
 | *Please give illustrations of any of the things your leadership do collectively and/or individually to promote positive cyber security behaviours.* |

21.5 Detection, Logging, Event Analysis and Alerting

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. How do you monitor attempted unauthorised access to your information systems?
 | *What dedicated cyber security control(s) do you operate to monitor access logs on a regular basis?* |
| 1. How are cyber security events logged and correlated/analysed to identify incidents and then escalated for action?
 | *What type of events do you record and collate for analysis, either to trigger alerts or to use during investigations? In general terms please describe the process for how a technical alert or a concern raised gets handled as an incident.* |
| 1. What capabilities do you have to detect anomalous activities which could indicate a security incident?
 | *Please describe in general terms any capabilities that you have to see deviations from normal activity worthy of further investigation.* |

21.6 Managing Incidents, Vulnerabilities and Response

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. What is your response process for cyber security incidents and events and under what criteria would you expect to report to customers?
 | *Confirmation of the procedure used to identify and remediate security incidents (e.g., in line with the cyber kill chain) and what customers can expect on how an incident is communicated and within what timeframe.* |
| 1. How do you learn of vulnerabilities, including those discovered by third parties?
 | *Please describe any responsible disclosure process you operate to receive, act on and report on any vulnerabilities.* |
| 1. What is your process for supporting customers who have experienced a security incident involving your services or products?
 | *Please describe how you collaborate during an incident.* |
| 1. Have you been obliged to report a cyber security incident to a legislator or regulator in the past 12 months?
 | *Confirmation of a security incident when reported to legislative or regulatory entity. (For example: ICO, Smart Energy Code or the FCA.)* |

* 1. Managing Identity and Access

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. How do you manage how individuals are authorised and granted access to systems, networks and premises that you manage?
 | *Please describe your systems and processes used to ensure employees and contractors/third party staff, have their accounts or access updated in a timely manner on changing jobs.* |
| 1. How do you ensure customer policies and processes to control access to their systems/premises are complied with if you have personnel changes?
 | *How do your internal processes work to alert customers of personnel changes and how do you know this is working?* |
| 1. How do you minimise the number of individuals with privileged/administrative access to systems including end user PCs and what additional steps do you take to manage the security of privileged access?
 | *What is you approach to privilege management? What processes and/or sets of tools do you have to help you in this? How is administration of end user systems performed?* |

21.8 Protecting Sensitive Data

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. How is data protected when held outside of the corporate network such as on mobile devices, cloud services or removable media?
 | *How is removable media (such as disk or tape backups) stored securely – for example using encryption. What controls are used for customer data held on company (or personal) mobile devices, email or cloud services?* |
| 1. How is data protected when sent by email or when sent by network connection?
 | *The approach used to protect individual messages and/or messaging system and network connection should be described.* |
| 1. How are paper records destroyed or data destroyed when a digital device or medium is disposed of or reused?
 | *The process for paper destruction and secure wipe/disposal should be described as well as if it meets any formal security standard.* |
| 1. If you have any processes in place to detect unauthorised or unusual transfers of data from your systems/network, could you please describe them?
 | *Examples could include Data Leakage Protection (DLP) network monitoring or simple NetFlow analysis. Your approach can be described in generic terms.* |

21.9 Protecting the Network

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. What approach do you take for corporate network boundary defence/network segmentation, particularly in connecting to untrusted networks such as the Internet?
 | *A general description should be given of where firewalls are used and also any strategies for separating networks and/or administrative domains used for different purposes Where cloud services are used what are they and how are they managed?* |
| 1. What approach do you take to secure remote access to your systems and network and how are remote users authenticated for that access?
 | *Authentication examples include the use of passwords or multi-factor-authentication.* |
| 1. If you allow personal devices to access corporate networks what security do you use to protect other systems on the network?
 | *If unauthorised personal devices were to be attached to the network could this be detected? Would something limit what they had access to?* |

21.10 Physical Security

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. What is your approach for the physical protection of systems and data?
 | *Describe types of electronic access control, CCTV, alarm systems (intruder, fire/heat), security response, fire protection, security patrol, window protection or any additional facility hardening. What approved secure method is employed when moving computer assets outside of a secured company area?* |

21.11 Asset Management, Control Monitoring and Testing

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. What steps do you take to determine which systems are the most critical and how do you maintain current lists of hardware and software of those critical systems? How are changes to systems managed?
 | *Describe the processes you operate to determine system criticality and how you keep system registers up to date. How do you record change and also assure that the reported information is correct?* |
| 1. Do you perform automated control and/or vulnerability monitoring? If so, what type of things do you monitor and what is the frequency of reporting?
 | *Examples of this could include vulnerability and configuration security scanning, automated penetration tests or even more sophisticated control analysis such as on time of connection.* |
| 1. How do you ensure that all key systems are updated to the current version of software and what approach is taken for any exceptions?
 | *How are networked and mobile computer assets patched to the latest maintenance level and how do you manage exceptions including obsolescence? What mitigation approaches do you use for unpatched devices. How do you do this for components you obtain from 3rd parties?* |
| 1. Do you carry out red team exercises or penetration testing? If so, who conducts the tests and to what frequency?
 | *Tests to find security weaknesses or vulnerabilities might be conducted by internal staff or third parties (these need not be named).* |
| 1. What audit and review processes of cyber risk management do you perform? What organisation/company function does these reviews and what is the frequency?
 | *What internal audit programme of work and/or third-party reviews are performed and how do these report any discovered defects to controls and/or processes for corrective action?*  |

21.12 Business Continuity and Backup

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. Do you have a business continuity plan and when was it last tested?
 | *Confirmation of business continuity and disaster recovery planning, restoration of backups, including stating when tested (evidence may be asked for at some point). Some may wish to say more and discuss approaches to resilience.* |
| 1. What approach have you adopted to backup data from accidental and malicious data loss (such as ransomware)?
 | *Outline your backup approach including how you manage risks to attached backup storage for your own and customer data.* |

21.13 Supply Chain Cyber Assurance

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. What processes do you use to assure the cyber security capability of the suppliers who support you in your business activities?
 | *Describe any processes and activities which you or retained third3rd parties perform to assess the cyber security of your own suppliers.* |
| 1. What processes do you use to assure the cyber security integrity of third-party products/services used to form part of a product or service you will deliver to a customer?
 | *For products and services which you integrate into your solutions please describe any assurance processes used such as penetration testing, or lab testing performed? What assurances are you able to get about patch levels? What is you approach to the integrity of open-source software?* |

21.14 Operating Outside of the UK

|  |  |
| --- | --- |
| **Security question** | **Guidance on answering** |
| 1. Please name any countries you propose operating from where UK customer data or processing outside of the UK might be hosted.
 | *Please state the countries you are proposing, and if there are options available for hosting or support locations which can be specified by the customer please say this too.* |
| 1. Please describe any technical, security or support roles outside of the UK who might have access to critical customer systems or information.
 | *In general terms describe the main country locations where development activity is performed. Please also say where support staff will be located, particularly where support staff may have access to customer systems.* |

1. Required Documents

|  |  |  |
| --- | --- | --- |
|  |  | See Appendix |
| Attached details of any legal or regulatory notifiable events, including Health and Safety prohibition, improvement notices or Environmental events in the past five years. | [ ]  |  |
| Copy of any relevant certifications (e.g. ISO 45001, 9001, 14001 etc.) | [ ]  |  |
| Copy of your HSE & Q Policy | [ ]  |  |
| Key HSE&A statistics for last 5 years. | [ ]  |  |
| Provide details of each of your HSEA objectives. Including any plans to improve Environmental performance and progress for zero carbon |  |  |
| Copy of company organisation chart, showing key contract contacts | [ ]  |  |
| Copy of your training, qualification and work experience for key contract personnel  | [ ]  |  |
| Copy of the competency matrix (record) for personnel to be deployed at EnQuest Assets, Sites or offices. | [ ]  |  |
| Copy of your documented procedures for investigations, corrective action, non-conformance and risk management | [ ]  |  |
| Copy of your anti-corruption code of conduct | [ ]  |  |
| Copy of your statement complying with section 54 of the Modern Slavery Act 2015, if applicable  | [ ]  |  |
| Copy of relevant data relevant security certifications | [ ]  |  |
| Copy of Diversity and Inclusion Policy and / or Strategy | [ ]  |  |

Decision

|  |
| --- |
| **This area is for EnQuest internal use only.**Reviewed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Reviewed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Reviewed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Status**APPROVED\_\_\_\_\_\_\_\_\_CONDITIONALLY APPROVED\_\_\_\_\_\_\_\_CORRECTIVE ACTION REQUESTED\_\_\_\_\_\_NOT-APPROVED\_\_\_\_\_\_\_\_\_ | **Completion Date**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Attachments**Yes [ ]  No [ ] Yes [ ]  No [ ] Yes [ ]  No [ ] Yes [ ]  No [ ]  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Is an Interface Document required?If required, justify here:  | Yes [ ]  No [ ]  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |