|  |
| --- |
|  |
| Nuclear Industry Security Regulations  Regulation 22 Dutyholder – Evidencing Expectations  Facility Question Set |



|  |
| --- |
| April 2023 |
| **Nuclear Industry Security Regulations**  **Regulation 22 Dutyholder – Evidencing Expectations**  **Facility Question Set** |
|  |
| 2023/25876 |

**Fundamental Security Principle (FSyP) 1 - Leadership and Management for Security**

Dutyholders must implement and maintain organisational security capability, underpinned by strong leadership, robust governance, an adequate management and accountability of security arrangements incorporating internal and independent evidence-based assurance processes.

|  | **Risk Profile Levels and Question Set Alignment: FSyP1 – Leadership and Management for Security** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (5 Questions)** | **Low (1 Questions)** | **Moderate (3 Questions)** | **High (0 Questions)** |
| SyDP 1: Security Governance and Leadership | FVL1.1: Describe how staff at the facility are informed of the security governance and leadership arrangements for the organisation. | FL1.1: Are staff at the facility routinely consulted on security issues? | FM1.1: Describe how staff at the facility are kept aware of the Board's/Senior Leadership's approach to the effective delivery of security for the organisation. |  |
| SyDP 1.2: Organisational Security Capability | FVL1.2: Describe your competence management system for effectively identifying training requirements for all security related roles at the facility. |  | FM1.2: Describe how organisational arrangements for security knowledge transfer are implemented at the facility and how managers are involved.  FM1.3: Describe how security related roles are performance managed, to ensure that responsibilities are being fully delivered at the facility. |  |
| SyDP 1.3: Security Decision Making | FVL1.3: Describe how organisational arrangements for security decision making are implemented at the facility, and what authority is delegated to staff to take timely decisions in the interests of security. |  |  |  |
| SyDP 1.4: Organisational Learning for Security | FVL1.4: What policy mechanisms are in place for systematically identifying and correcting deficiencies in security and describe how staff are encouraged to report them at the facility? |  |  |  |
| SyDP 1.5: Security Assurance Processes | FVL1.5: What CS&IA assurance activities are in place to ensure compliance with relevant security policies within the facility? |  |  |  |

**FSyP 2 - Organisational Culture**

Dutyholders must encourage and embed an organisational culture that recognises and promotes the importance of security.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 2 - Security Organisational Culture** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (2 Questions)** | **Low (0 Questions)** | **Moderate (1 Question)** | **High (1 Question)** |
| SyDP 2.1: Maintenance of a Robust Security Culture | FVL2.1: Describe how CS&IA policies, procedures and guidance are made available to staff at the facility and how changes are communicated.  FVL2.2: Describe your CS&IA awareness and training programme for new and existing employees, and how this takes account of the threat to the civil nuclear industry within the facility. |  | FM2.1: How are cultural initiatives identified and improvements made across the facility? | FH2.1: Describe any arrangements in place to maintain continual assurance of a robust security culture, including any arrangements for addressing any findings. |

**FSyP 3 – Management of Human Performance**

Dutyholders must implement and maintain effective arrangements to ensure the human contribution to delivery of security is understood and appropriately designed (to include tasks, competence staffing, workspace, equipment and administrative control), implemented and resourced.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 3 – Management of Human Performance** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (2 Questions)** | **Low (0 Questions)** | **Moderate**  **(0 Questions)** | **High**  **(0 Questions)** |
| SyDP 3.1: Identification and Analysis of Security Tasks and Roles | VL3.1: Describe the facility's approach to identify the tasks and roles relevant to security.  FVL3.2: Describe how training needs for security specific roles at the facility are assessed and addressed. |  |  |  |

**FSyP 7 - Cyber Security and Information Assurance**

Dutyholders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 7 - Cyber Security and Information Assurance** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (16 Questions)** | **Low (0 Questions)** | **Moderate (0 Questions)** | **High (3 Questions)** |
| SyDP 7.1: Effective Cyber and Information Risk Management | **Scope and Business Objectives** | | | |
| FVL7.1: Describe how staff at the facility are made aware of the organisations business objectives for cyber and information risk management, and the relationship to relevant legislation and regulation. |  |  |  |
| **CS&IA Risk Governance Structure** | | | |
| FVL7.2: Who holds responsibility for CS&IA risk management? Clearly identify any key roles and responsibilities for delivery and accountability concerning the facility. |  |  |  |
| **CS&IA Residual Risk Management** | | | |
| FVL7.3: Describe how risk managers at the facility understand their role in the governance structure, are empowered appropriately and own, report and/or escalate risk through the life of information assets. |  |  |  |
| SyDP 7.2: Information Security | **CS&IA Policy and Standards** | | | |
| FVL7.4: Describe the structure of the facility's CS&IA policies, procedures and guidance, providing references to key documents as required.  FVL7.5: Describe how the facility uses organisational processes in identifying and managing SNI and associated assets, including the arrangements to maintain and audit SNI and associated equipment, applications and software. |  |  |  |
| **Data Classification and Sensitivities** | | | |
| FVL7.6: What arrangements does your facility have in place to classify and control SNI? |  |  |  |
| **Identification of Classified Subcontracts** | | | |
| FVL7.7: Describe briefly any classified contracts involving SNI that your facility is currently undertaking.  FVL7.8: Describe the facility's mechanisms for assuring classified contracts to ensure that suitable security controls are implemented and maintained. |  |  |  |
| **End of Contract** | | | |
| FVL7.9: Describe the facility's processes to manage the closure of classified contracts with third party companies involving SNI and associated assets. |  |  |  |
| SyDP 7.4: Physical Protection of Information | **Physical Security Risk Assessment** | | | |
| FVL7.10: Describe the process used to determine the facility's physical security measures.  FVL7.11: Describe how the physical security measures are part of a layered approach based upon a risk assessment. |  |  |  |
| **Physical Security Control Measures** | | | |
| FVL7.12: Describe the physical security control measures in place that protect SNI and associated assets at your facility. |  |  | FH7.1: Describe how TEMPEST has been considered as part of the physical security risk assessment of the facility, if SNI is processed electronically.  FH7.2: Describe the facility arrangements in ensuring that the alarm response force is trained and resourced adequately, to respond to physical security events that affect SNI. |
| **Assurance of Physical Security Measures** | | | |
| FVL7.13: What assurance activities are undertaken to assess the effectiveness of physical security measures at the facility? Detail any supporting processes and procedures as appropriate. |  |  | FH7.3: Describe the facility's processes in place to identify emerging and changing threats, and how physical security control measures are adaptive to respond to such changes. |
| SyDP 7.5: Preparation and Response to Cyber Security Incidents | FVL7.14: Describe how the facility identifies and manages all types of security incidents. Include brief details of how incidents are logged, reported (to internal and external stakeholders) and any lessons learned processes.  FVL7.15: Describe your process for reporting security incidents and matters of interest in compliance with the Nuclear Industry Security Regulations 2003.  FVL7.16: Describe your processes to test and exercise your security incident management arrangements, relating to SNI. |  |  |  |

**FSyP 8 - Workforce Trustworthiness**

Dutyholders must implement and maintain a regime of workforce trust to reduce the risks posed by insider activity.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 8 – Workforce Trustworthiness** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (3 Questions)** | **Low (1 Question)** | **Moderate (0 Questions)** | **High (1 Question)** |
| SyDP 8.1: Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security | FVL8.1: Describe how the facility implements and maintains on-going personnel security management to remain assured about your employees and contractors; and to mitigate the risks from insiders. |  |  |  |
| SyDP 8.2: Pre-employment Screening and National Security Vetting | FVL8.2: Describe any processes used to determine the level of NSV clearance required for the facility and access to SNI (where required). |  |  |  |
| SyDP 8.3: Ongoing Personnel Security | FVL8.3: Describe how the facility promotes and aligns to corporate processes to support employees when dealing with personal challenges that may have an impact on security. | FL8.1: Describe what processes and procedures exist, regarding security risks associated with visitors and how such access is managed by the facility. |  | FH8.1: If applicable, describe any processes for when facility staff are carrying out activities under duress e.g. duress code and describe how is this communicated to staff so that they are always aware of how to enact it. |

|  |
| --- |
|  |