NO MARKING REQUIRED

This Sellafield Ltd Policy is approved by the SL Board; it represents the SL Board's direction to the business on this topic. Compliance with this policy is mandatory through aligning Sellafield Ltd Management System processes and people behaviours to the commitments below.

Information Management Policy

Policy Statement

Sellafield Ltd regards information and knowledge as valuable assets critical to delivering its mission. We shall provide robust information management arrangements, including all aspects of information risk and security, to ensure information (in all its forms; including records, data, documents or of any media type) and all forms of knowledge is identified, valued, secured, preserved, easily retrieved and reused for the Company and its stakeholders.

We shall establish and maintain suitable means of storing information for re-use at the point of work whilst also protecting information and associated technology to ensure the Company meets its legal and proliferation-sensitive obligations. Any known loss of information shall be reported and investigated accordingly.

Commitments

We shall be a company that;

- Has in place a risk based approach to the management of information throughout its lifecycle and in accordance with quality and value added to the Company.
- Ensures information management arrangements give due attention to security, protection, usability, retrievability, preservation, environmental and cost issues in order to make the right information available through a knowledge sharing and learning culture.
- Ensures compliance with all legal and regulatory requirements relating to the retention of information including long term preservation (physical and digital).
- Maintains a business ownership model for all information assets, with clearly defined roles and accountabilities, to ensure critical information assets are effectively controlled, leveraged, and optimised for the benefit of the Company.
- Promotes an effective information management culture, including information security, through the continued delivery of awareness and training.
- Supports the move from systems and processes primarily underpinned by paper to a compliant electronic environment in accordance with BS 10008 (Evidential Weight and Legal Admissibility of Electronic Information).
- Ensures that information management principles are incorporated in the design of new or upgraded processes and systems utilising appropriate automation of workflows to provide a timely and accurate single source of data.
- Rationalises and optimises information systems to a strategic enterprise level blueprint based on an integrated set of best-in-class (functional capability) systems and sourced, where possible, from industry standard packaged solutions.

NO MARKING REQUIRED

- Treats personal information lawfully and correctly, in particular adhering to the Eight Principles of Data Protection, contained in the Data Protection Act 1998.
- Ensures arrangements are in place to monitor and protect the confidentiality, integrity and availability of the Company's information assets from all known threats, whether internal or external, deliberate or accidental in accordance with NISR (2003 as amended), the Security Policy Framework (SPF) and Civil Nuclear Security Standards (CNSS).
- Has in place suitable arrangements for the monitoring of activity on Company information systems to prevent or detect actual or potential security breaches and take appropriate action in response.
- Ensures that Intellectual Property (IP) is managed in a manner that meets all legal and contractual obligations and requirements.