Information Security Policy (SAR 02)

1. Introduction

Security is critical to the success of INS's strategy. It is much more than a simple enabler and is considered to be a unique selling point for the organisation.

The nature of our business requires the processing of a range of information (sensitive, personal, commercial etc.). This information, if lost or compromised, could impact our reputation, the delivery of our strategy, our employees, customers and stakeholders.

For this reason, good information security and information risk management arrangements are essential to ensure that information is appropriately protected and represent a fundamental enabler in helping the business achieve its strategic aims.

2. Purpose and Scope

The purpose of this policy is to outline INS's intent and approach to information and cyber security and information risk management (IRM) within INS.

This policy applies to all INS staff and contractors (agency-supplied workers, secondees etc.), underpins the overarching INS Security Policy and supports the INS corporate risk management arrangements.

3. Commitments

INS will:

- adopt an integrated, proportionate and risk-based approach to information security;
- undertake information risk management within the context of its approved risk appetite
- In applying these arrangements, INS will ensure compliance with the following (not exhaustive):
  - All applicable legislation and regulation;
  - Its customers', stakeholders' and owners' expectations and requirements;
  - UK Nuclear Cyber Security strategy and relevant derivatives of it;
  - INS's own cyber security and business strategy, including the Risk Appetite Statement

To achieve this, INS will:

With Regards to Personnel

- Deliver strong, business-focussed information security leadership and governance;
- Provide strategic level governance and review of information risks;
- Appoint subject matter experts and suitably qualified and experienced individuals to deliver this policy and provide security advice.

This includes:

  - A Senior Information Risk Owner (SIRO), who will own and manage risk governance and provide strategic direction;
  - A Chief Information Security Officer (CISO), who will ensure that cyber and information security risks are appropriately identified and managed;
  - A Security Director accountable for setting and assuring compliance with corporate security policy

With Regards to Process

- Identify and manage information risks that may represent a threat to the INS mission;
- Articulate its information risk appetite and take risk-based decisions in line with this;
- Ensure information risk appetite remains fit for purpose and current in the context of changing threats, vulnerabilities and business or cyber strategies;
- Ensure that, where required, INS computer systems are formally accredited for use, using a recognised risk management process;
- Provide guidance on information security and IRM;
- Ensure there is an appropriate training & awareness programme to support implementation of this policy;
- Communicate effectively with stakeholders about relevant information security and IRM matters and incidents;
- Conduct effective information security oversight of our supply chain;
- Undertake activities to validate compliance with this policy.

25 September 2019