# INS Security Policy

*International Nuclear Service (INS) believes that its effective management and delivery of security is central to the success of the business.*

## 1. Scope

This policy applies to International Nuclear Services Limited (INS) staff and contractors and covers all aspects of personnel, physical, information, cyber and operational security. Security training; the reporting of incidents; and the performance testing of arrangements, are an integral part of the policy requirements. This policy is supported by the:

- INS Information Security Policy (SAR 02);
- INS Security Breaches Policy (SAR 03);
- INS Clear Desk Policy (SAR 04);
- INS IT Policy;
- INS Security Marking Guide (INS/PROM/057.10); and
- INS Disciplinary Procedure*.

## 2. Requirements

INS will apply the requirements of the Nuclear Industry Security Regulations (2003), as amended; the Port Security Regulations (2009); the Ship & Port Facility (Security) Regulations (2004); the Anti-Terrorism, Crime & Security Act 2001 and the UK Government Security Policy Framework (SPF). Where security controls are not mandatory, INS will take a risk based approach utilising threats and vulnerabilities to determine effective and economic mitigation actions or measures.

In applying the above requirements, INS aims to protect against the:

- sabotage of nuclear material in transit;
- unauthorised removal or access to nuclear material or other assets; and
- loss, theft or compromise of commercial information, SNI or cryptographic material.

To support this policy, INS will:

- inform, instruct, train and develop the people who work for us;
- appoint suitably qualified & experienced personnel to provide competent security advice;
- maintain an excellent security awareness culture;
- work with our regulators, government stakeholders, the rest of our industry, customers and contractors to ensure effective and appropriate security standards;
- establish and comply with approved security statements and plans;
- comply with the statutory, or other reporting requirements, of any non-compliances or incident identified;

- ensure that all personnel shall be security cleared to an appropriate level;
- use information and cyber security to provide a framework so that INS and the NDA are able to minimise the risk to the Confidentiality, Integrity and Availability of our sensitive information; and
- comply with relevant legislation, regulatory requirements, contractual and other standards for sensitive information.

* The INS Disciplinary Procedures do not apply to Contractors. Any disciplinary issues Involving a contractor will be raised with their employer or agency.

**Mark C Jervis**
Managing Director
International Nuclear Services

**Ben Whittard**
Head of Security & Resilience
International Nuclear Services

15th September 2016