INS Information 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 information and cyber security. This policy underpins the INS Security Policy (SAR 01) and is supported by the:

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

2. Requirements

To protect the Confidentiality, Integrity and Availability (CIA) of all Sensitive Nuclear Information (SNI) and assets INS will apply the requirements of the:

- Nuclear Industry Security Regulations (2003),as amended;
- Anti-Terrorism Crime and Security Act (2001);
- Data Protection Act (1998);
- Freedom of Information Act (2000);
- Regulation of Investigatory Powers Act (2000); and
- UK Government Security Policy Framework.

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:

- unauthorised removal or access to SNI 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 information security advice;
- ensure that all personnel shall be security cleared to an appropriate level;
- apply the fundamental security principle that all staff must have a legitimate 'Need to Know' the details of the SNI or assets, to which they are permitted access;
- maintain an excellent security awareness culture covering all aspects of information security;
- work with our regulators, government stakeholders, the rest of our industry, customers and contractors to ensure effective and appropriate information security standards;

- comply with the statutory, or other reporting requirements, of any information security non compliances or incident identified;
- use information and cyber security to provide a framework so that INS and the NDA are able to minimise the risk to the CIA of our SNI and assets; and
- comply with relevant legislation, regulatory requirements, contractual and other standards for SNI and assets.
- appoint a Company Security Officer (CSO), a Senior Information Risk Owner (SIRO), an Information Governance Officer (IGO) and a Chief Information Security Officer (CISO) to lead and manage the company's strategic approach to managing information risks;
- appoint Information Asset Owners (IAO) to manage all key information, systems and assets; ,
- where possible, produced, maintained and validated Business Continuity Plans (BCP) to ensure that information, assets and vital services are available to users; and
- reserve the right to pursue through legal means any individual who is suspected of unauthorised or reckless disclosure of SNI, sensitive nuclear assets, commercial information or intellectual property.

3. Definition and Guidance

For the purposes of this policy and the supporting policies, the following terms will be used to describe the 'Need to Know Principle' and all material that is Commercially Sensitive or classified as SNI.

3.1 'Need to Know Principle'

The 'Need to Know Principle' is a fundamental building block of security, which requires that knowledge or possession of SNI should be strictly limited to those members of staff, or trusted third parties, who have the appropriate security vetting and can clearly evidence a need to have it. It is a key principle that needs to be applied when decisions are being made about how SNI is classified when it is produced or shared.

3.2 'Commercial Sensitive Information'

Commercially Sensitive Information can be described as information which, if it were to be disclosed improperly, may cause concern for the INS, NDA and / or other parties (such as UK Government, Regulators, Customers, Site Licensing Companies, other stakeholders,

INS staff and their families or the wider public) including but not limited to; embarrassment, an increased risk to the security of persons or property, a security risk to Nuclear Material or an increased risk of litigation.

3.3 'Classified Information' and 'Sensitive Nuclear Information' (SNI)

Classified Information and SNI can be described as information which has an intrinsic value to UK Government and therefore must be protected appropriately under the Government Classification Scheme (GSC) which consists of three security markings, OFFICIAL (including OFFICIAL-SENSITIVE), SECRET and TOP SECRET.

Further guidance is available in the mandatory INS Security Marking-Guide (INS/PROM/057.10) or from the Security & Resilience Directorate.

* 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