NATIONAL NUCLEAR LABORATORY

NNL SECURITY POLICY

NNL recognise that secure operations are dependent upon employee participation, commitment and accountability. NNL will maintain the highest appropriate levels of security for our offices, projects and sites to prevent unauthorised access to all protected assets whilst allowing authorised persons to go about their business.

This policy will be enacted by:

What you can expect from us:	What we expect from you:
• As dutyholder for security, NNL will establish and comply with ONR approved Nuclear Site Security Plans (NSSP) for any site that handles nuclear material and Sensitive Nuclear Information (SNI) to prevent the unauthorised access, removal (theft) of nuclear material or SNI, or the sabotage of nuclear premises and nuclear material transit. • NNL will ensure that NSSPs, procedures and instructions are in place to protect nuclear assets.	• Employees will ensure they adhere to security procedures and instructions that flow down from any Nuclear Site Security Plan (NSSP).
• NNL will develop a robust cyber security and information assurance plan to mitigate risks to systems and information in accordance with ISO27001 standards, Cabinet Office requirements for Protectively Marked Information (PMI) and ONR's requirements for Sensitive Nuclear Information.	• Employees will ensure adherence to NNL's information and cyber security standards, procedures and instructions.
• NNL will promote security awareness across all NNL employees and contractors via security educational courses, periodic communications encouraging healthy security culture and Learning from Experience (LfE) messages.	• Employees should undertake all mandatory security awareness courses and apply learning from these and any LfE broadcast.
• NNL will benchmark performance and culture against industry standards and certifications, such as the CPNI SeCuRE tool and comparing results to similar national infrastructure industries.	• Employees will investigate and rectify all incidents and known vulnerabilities wherever possible.
• NNL will develop and implement a security culture to reduce the likelihood of security incidents occurring.	• Employees with specific security roles will lead by example, carry out monitoring at all times and all employees will remain vigilant and report any suspected security incidents.
• NNL will ensure that NNL remains compliant with all relevant nuclear and general security legislation, including but not limited to the Official Secrets Acts, the Nuclear Industry Security Regulations, The Nuclear Safeguards Act, The Cabinet Office Security Policy Framework and the Data Protection Regulations.	• Employees will adhere to all relevant security procedures and instructions that flow down from legislation and approved security plans.
• NNL will provide a facility to report any non-compliances with this policy.	• Employees will report any suspected non-compliance though the correct channels as soon as practicable.
• NNL will provide the necessary tools, equipment, information and resources to employees to enable secure access to facilities, material or information and provide a secure working environment.	• Employees will demonstrate diligence in the protection of any asset afforded by NNL and return any such items as soon as practicably possible when requested to do so.
• NNL will take reasonable steps to protect staff, contractors and visitors from the effects of any security incident including malicious attacks.	• Employees will report any suspicious activity or behaviours and adhere to any security procedure or instruction that protects their safety and security.
• NNL will ensure effective emergency arrangements are in place, planning and testing these to ensure continuous improvement.	• Employees will participate in security drills as required and comply with emergency arrangements.

Review/measurement:

This Policy will be reviewed regularly and updated as required to ensure it is effective and reflects the business needs.

NNL expects all to operate in accordance with NNL's values and behaviours, and adhere to this policy.

The implementation of this Security Policy and key monitoring activities will be detailed in the EHSS&Q and Delivery Operations Policy Implementation Matrix - IMS-EHSS&Q-DO-PIM.

Signed:  Date: 27/03/2023

Paul Howarth CEO