Information and Cyber Security Policy

Purpose:

This policy supports the delivery of the HS2 Information & Cyber Security Strategy, providing the authority required to the broader Information & Cyber Security Control Framework.

The objective of this policy is to outline how HS2, the HS2 Project, and the wider supporting supply chain (where applicable) can meet statutory, regulatory, contractual, and development agreement obligations concerning Information and Cyber Security.

Principles

- Establish a top-down security culture aligned with HS2 corporate values, ensuring that Information and Cyber Security (ICS) roles, responsibilities, and requirements are clearly communicated to HS2 personnel and relevant external parties.

- Raise awareness and ownership of ICS risks at the board and executive levels, and throughout HS2 and its supply chain. Risks should be identified and managed in line with the HMG Security Policy Framework and ISO/IEC 27001:2022, integrating with wider governance, risk, and assurance processes at HS2.

- Clearly define roles and responsibilities for information and cyber security across HS2. Ensure a single point of contact is accountable for enabling and driving ICS initiatives within HS2.

- Provide cyclical assurance of internal projects and third parties involved in the HS2 Project to ensure that minimum security requirements are consistently met.

- Prepare for a range of cyber threats by implementing and exercising ICS incident management processes, ensuring integration with existing incident management procedures at HS2.

- Engage with external stakeholders, including the Department for Transport (DfT), National Cyber Security Centre (NCSC), and National Protective Security Authority (NPSA), to ensure compliant delivery of ICS within HS2 and the Project.

- HS2 is committed to complying with all relevant laws, regulations, and standards concerning information and cyber security, including GDPR for data protection. Adherence to these obligations is essential to maintain trust and protect the integrity of HS2's operations.

- HS2 will adopt a proactive approach to risk management, including the regular assessment of information and cyber security risks. These risks will be prioritised and mitigated through the implementation of appropriate controls, aligned with the HMG Security Policy Framework and ISO/IEC 27001:2022.

- Regular and mandatory ICS training will be provided to all HS2 staff, contractors, and third parties. This training is critical to ensure that all personnel are aware of their responsibilities and are up to date with the latest security practices.

- All identified risks must be systematically assessed, monitored, and mitigated through HS2's established Risk Management Framework. This framework serves as the foundation for decision-making and ensures that risks are handled in a structured and comprehensive manner, minimising potential negative impacts on the organisation's objectives.

- The identification of risks is a collective responsibility that extends across all levels of the organisation. Every employee, contractor, and stakeholders are required to actively engage in the process of identifying potential risks within their areas of operation.

- All risks related to information and cyber security will be managed and controlled in accordance with HS2's Information and Cyber Security Control Framework.

- HS2 reserves the right to monitor usage and compliance with this control framework.

- Governance of information and cyber security will be overseen through the established governance process, with regular review and oversight by the Cyber Governance Group.

- We will embed security into the design and development of systems, applications, and processes. Security considerations are integral to the planning and execution phases of all projects, ensuring that risks are addressed from the outset.

- We will adopt a Zero Trust security framework which is predicated on the principle that trust is never assumed, irrespective of where the request originates from. This framework has 3 principles: Explicit verification, least-privilege, and assume breach.

- We will anticipate and pre-empt security threats, implementing measures that not only react to incidents but also predict and prevent potential threats.

- We will ensure that effective risk management is employed in decision making, ensuring the following traits are present in our risk management: Dynamic, Defensible, Data-Driven, and Decision-Enabling.

Applicability, implementation and resources

This policy applies to all;

- Persons working on the HS2 programme, including but not limited to, permanent staff, contractors, suppliers, consultants.
- Information stored, processed and managed by HS2*. and

- Any other interested parties handling or accessing HS2 information, such as Regulatory bodies, Joint Ventures and other authorised third parties.

*Operational and Engineering Technologies (OT and ET) are out of scope for this policy.

The Senior Information Risk Owner (SIRO) is member of the HS2 Board and will provide support and authorisation to the Head of Cyber Security for the implementation of the strategy, and the development, upkeep, and implementation of the Information & Cyber Security Control Framework.

Executive Owner:

The Chief Financial Officer, as Senior Information Risk Owner, is the Executive Owner of this policy and is responsible for maintaining the accuracy and relevance of its contents and for periodic review and update to reflect changing circumstances.

[redacted]

Approved on:
18/06/25

Mark Wild
Chief Executive Office
HS2 Ltd