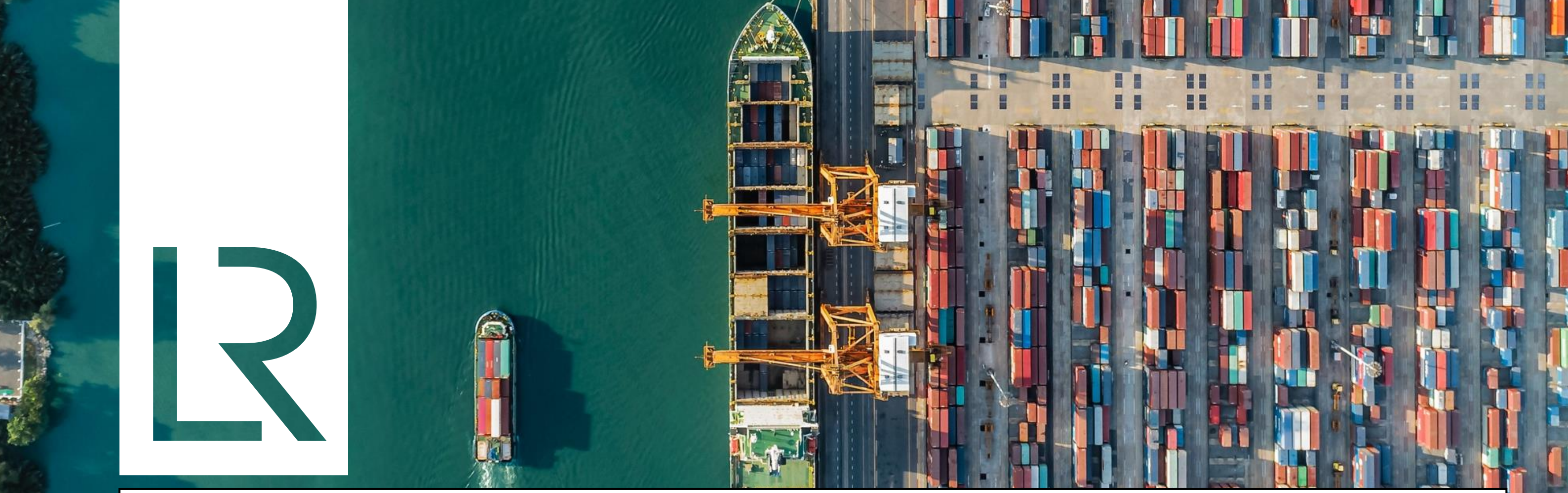

BMS2-712 Information Security Policy

1. Purpose

1.1 This policy supports GMS01-01 Health, Safety, Environment and Quality Policy which refers to the commitment to the protection, integrity and security of personal and business information.

1.2 Lloyd's Register Group (LR) takes seriously its responsibilities to protect the information entrusted to us by our clients and the information we generate and use in the provision of services to our clients and society.

1.3 We understand the importance of our contractual, legal, regulatory, compliance and business obligations. With this level of dependency on information it is vitally important that we have the right controls in place to ensure the confidentiality, integrity, availability, accountability and reliability of our information. We are also committed to ensuring that information is adequately protected from unauthorized use, modification, disclosure or destruction, whether accidental or intentional, and that information is used for approved purposes only.

1.4 Information security protects all important information, including intellectual property, compliance records, competitive information, research results, emails, personnel files and financial records, while also securing the systems, hardware and supporting processes that store and use the information.

1.5 This policy is designed to protect information, systems and employees. The policy protects LR's ability to offer information services to employees and to deliver effective client services. The policy is also designed to preserve LR's reputation.

2. Applicability

2.1 This policy is applicable to all LR personnel including (but not restricted to):

- LR employees (all employment types, including permanent, contract and temporary).
- Suppliers and vendors with authorised access to LR Group assets.
- Non-integrated business units (who must ensure that their information security controls at least meet the requirements of this policy).

2.2 The Director of each Business and Group Support function must ensure that people working under their control are aware of and comply with the controls set out in this policy.

3. Definitions

- **Information Security**: The preservation of confidentiality, integrity and availability of information. Additionally, information security refers to other properties, such as authenticity, accountability, non-repudiation, and reliability.
- **Confidentiality**: The prevention of the disclosure of information to unauthorized individuals, organisations or processes.
- **Integrity**: The safeguarding of the accuracy and completeness of information over its entire lifecycle.
- **Availability**: The accessibility and usability of information within an agreed timescale by an authorised organization

4. Information Security Objective

4.1 The objective of information security is to protect LR's business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity, and availability.

4.2 It is the intention of senior management to achieve and maintain compliance with information security best practice by doing the following:

- Demonstrate and maintain alignment to ISO27001 standard.
- Provide information security awareness training to all personnel.
- Manage incidents to minimise their impact and learn from them to prevent reoccurrence.
- Ensure Information is available promptly for authorized access when required.
- Establish an Audit schedule that meets the needs of the business.
- Ensure that the ISSB (Information Security Steering Board) meets regularly, at least every 6 months, to provide direction for the business and IS.

5. Information Security Principle

5.1 It is the policy of senior management that the principles below will be followed:

- Information security is managed using a formal, risk-based, LR-wide information security management system.
- Business need for information security is satisfied, balancing the freedom to conduct business with effective security.
- Comply with all relevant legislation, regulatory and contractual requirements while achieving standards of best practice.
- Provide supporting processes, procedures, standards, guidelines, and resources as necessary.
- Identify and manage risks to protect information throughout its lifecycle.
- Safeguard information whether belonging to LR, LR clients or suppliers against unauthorised modification, disclosure, loss, or theft.
- Ensure LR intellectual property rights (IPR) are protected.
- Ensure information is protected against unauthorised access, disclosure and modification in accordance with relevant business, contractual, legal, statutory and regulatory compliance obligations.
- Raise awareness of this policy and the need to adhere to it.
- Monitor, measure and improve information management practices to ensure effectiveness and adherence to policy, take corrective and preventive action to achieve continual improvement of the information security management system.

6. Roles and Responsibilities

6.1 Roles and responsibilities are documented and communicated to all users via BMS4-756 Governance Roles and Responsibilities Standard.

7. Compliance

7.1 All persons working for or on behalf of LR must comply with the LR information security policies, procedures, and standards.

7.2 The Head of IS Operations is ultimately responsible for ensuring the requirements of this policy are fulfilled and monitored to ensure continued compliance.

7.3 The Head of Group PMO is responsible for ensuring that the requirements of this policy are integrated in LR's project management framework.

7.4 The Head of Information Security is responsible for ensuring the requirements of this policy are integrated in the security risk assessment and risk treatment process.

7.5 Failure to comply with this policy will be taken seriously and may lead to disciplinary action dependent upon the nature and severity of the non-compliance in accordance with relevant HR policies.

7.6 Existing policies, procedures and standards that encompass and/or exceed LR Information Security policies may be accepted subject to review. If for any reason compliance is not possible, a deviation must be requested.

8. Deviations

8.1 All requests for deviations or variance to this document must be submitted using BMS4-739 Information Security Deviation Request Form and processed in accordance with BMS4-738 Deviation and Change Approval Procedure.

9. Records

9.1 Records shall be retained as evidence of the results of this document. In accordance with GMS03-10-36 Control of Documented Information.