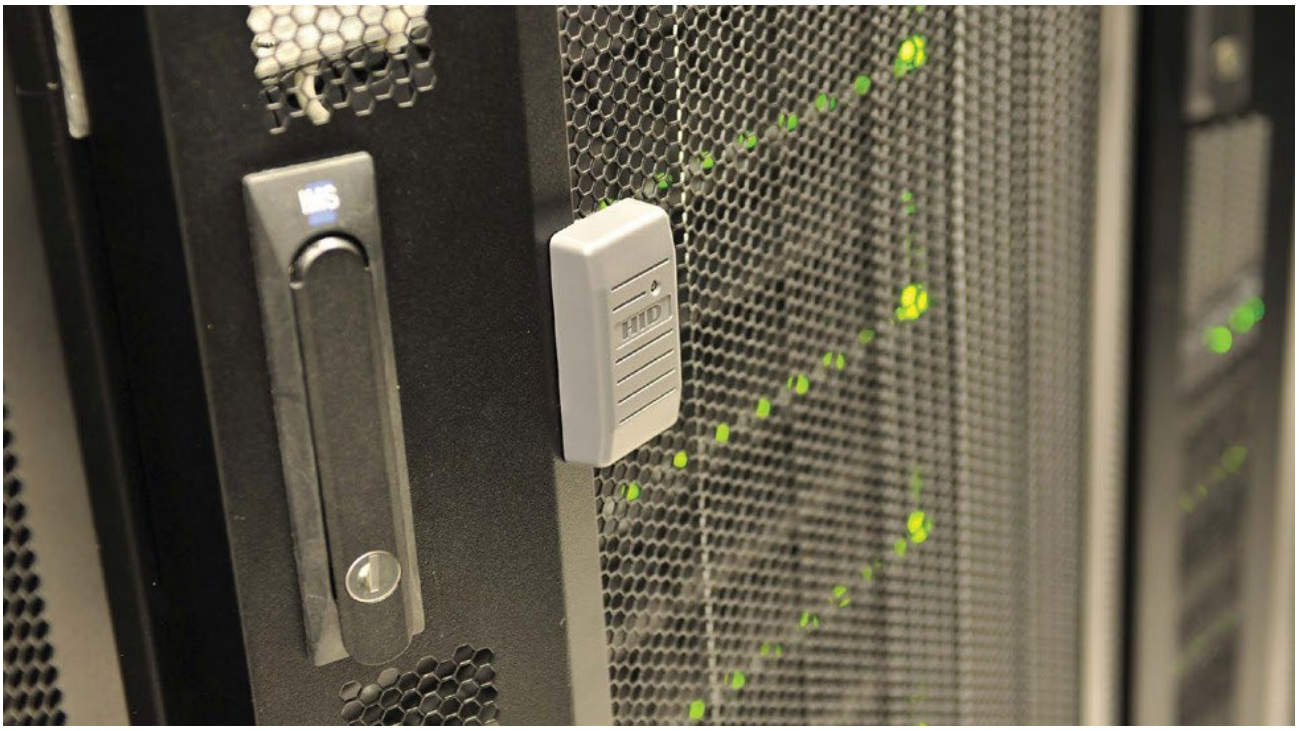
London Stock Exchange Group (LSEG)

FMC Portal

INFORMATION SECURITY WHITE PAPER

LSEG



Introduction:

LSEG is one of the world's leading providers of financial markets infrastructure and delivers financial data, analytics, news and index products to more than 40,000 customers in 190 countries.

We help organisations fund innovation, manage risk and create jobs by partnering with customers at every point in the trade lifecycle: from informing their pre-trade decisions and executing trades to raising capital, clearing and optimisation.

Backed by more than three centuries of experience, innovative technologies and a team of 23,000 people in 70 countries, we are driving financial stability, empowering economies and enabling you to grow sustainably.

The Financial Modelling and Conversion (FMC) Portal is a user-friendly web interface that enables LSEG customers to connect with the Financial Modelling and Conversions team. Through this portal, customers can request the conversion or creation of Excel models tailored to their specific needs. Users can conveniently upload their existing models, and once the conversion process is complete, they gain secure access to the converted files. Authentication for downloading the converted excel model is ensured by specifying the email addresses provided during the initial request.

Customers can choose to deploy integration and distribution capabilities on-site, use our hosted and managed service, access it via the public cloud, or use any combination of these models to suit their specific needs for flexibility and efficiency.

We provide the tools and insights to solve customers' more complex enterprise challenges from reducing data delivery and infrastructure costs, to driving innovation and efficiency.

At LSEG, protecting our customers' information is at the core of our information security strategy. We have established policies and a governance structure to mitigate and respond to potential security risks. We align ourselves to multiple security and risk frameworks and assess the effectiveness of our security program on an ongoing basis. We are committed to providing a secure environment for the personal data and confidential information we hold.

This document provides a high-level view of LSEG's approach to information security and compliance for **FMC Portal (https://fmc.refinitiv.com)**.

INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT

LSEG operates a Three Lines of Defence model, providing appropriate segregation of duties and clear roles and responsibilities across the LSEG's Divisions and Functions, including Risk, Compliance and Internal Audit. LSEG has an established Enterprise-wide Risk Management Framework, which is the main point of reference for the key aspects of group-wide risk management arrangements.

This includes:

• Risk Identification

• Risk Assessments

• Risk Monitoring

• Risk Reporting

• Portfolio Management

MEASUREMENT OF EFFECTIVENESS

To protect LSEG and your data, the performance and effectiveness of the information security and data privacy controls within the company and associated third parties are regularly tested using a variety of means.

CHIEF INFORMATION SECURITY OFFICE

The Chief Information Security Officer is a board delegated, centralised group role, responsible for defining the information security standards and providing appropriate controls and capabilities to the group.

POLICY & STANDARDS

LSEG maintains a comprehensive set of group internal policies endorsed by the Board and Executive Leadership Team. The policies outline key principles and take into consideration relevant industry standards and regulatory requirements relating to information security and data privacy.

SECURITY IN HUMAN RESOURCES

LSEG employees are subject to appropriate background and security checks at hiring, in line with applicable laws and commensurate with the sensitivity of the information that they access, and the security sensitivity of the role being filled. Third parties supplying contractors to LSEG are similarly required to ensure appropriate checks are performed before contractors provide services to LSEG.

SECURITY IN MERGERS & ACQUISITIONS

LSEG maintains a number of standard practices and policies to mitigate information security risks during corporate activity such as acquisitions, divestments, joint ventures and minority investments. These standard practices and policies cover all aspects of the integration and divestiture lifecycle.

ASSET MANAGEMENT

LSEG maintains a centralised inventory of hardware and software with information about the purpose of each type of asset and its criticality to the business, including configuration data, in a centralised configuration management database (CMDB).

DATA CLASSIFICATION AND HANDLING

The LSEG data classification and handling standard mandates the rules for the classification and handling of data held by the company. Data is classified according to its sensitivity to determine the level of controls required.

TECHNICAL CONTROLS

Security standards are aligned to global industry standards, including those defined by the National Institute of Standards (NIST) and Technology and the Cyber Risk Institute and define the implementation of technical controls such as:

- Access Management
- Anti-malware
- Network security
- Secure configuration and hardening
- Mobile device management
- Vulnerability and Patch management
- Software development lifecycle and application security
- System monitoring
- Cloud security

CHANGE MANAGEMENT

LSEG has defined a formal change control policy and procedures to ensure changes are introduced to live operations in consistent and structured manner, minimising business impact or disruption. Items considered for change control are tracked through a formal process, covering both application and infrastructures assets.

SECURITY OPERATIONS AND INCIDENT RESPONSE

A security incident response plan and associated processes and runbooks exist to address incidents as they are identified. Information Security Incidents are managed by a dedicated Global Security Operations Centre (GSOC).

DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT

LSEG has established a global framework, to address disruptions of varying scope, including, but not limited to, large-scale location-specific events.

THIRD PARTY SECURITY

LSEG has established information security requirements for its suppliers in line with LSEG's Information Security Policy and related standards. These requirements must be met by all third parties with access to LSEG's data and networks.

PHYSICAL AND ENVIRONMENTAL SECURITY

Physical security controls are implemented at LSEG in line with the Group Physical Security Policy and standards. Standards include minimum requirements for the physical security protection measures that must be applied. A variety of secure methods are used to protect LSEG group facilities.