Bloomberg - Data Policy Document

Bloomberg Data Security Policy

Purpose:
To establish the responsibilities and outline the standard measures for protecting all sensitive and confidential data handled by Bloomberg.

Scope:
This policy applies to all employees, affiliates, and third-party service providers of Bloomberg.

1. Proprietary Market Data:

- **Real-Time Data:** Real-time financial market data, analytical outputs, and proprietary market indicators are not to be shared with unauthorized external parties.
- **Historical Data:** Historical financial data and related analyses are confidential and should not be disclosed unless it is part of a sanctioned release.

2. Operational Data:

- **Internal Reports:** Operational performance metrics, internal audit reports, and efficiency analyses must remain confidential and are to be circulated internally only to authorized personnel.
- **Network and Security Information:** Information about Bloomberg's security practices, network configurations, and IT infrastructure are classified and should not be disclosed to maintain system security.

3. Employee Information:

- **Personal Details:** Employee personal details, payroll information, and employment records are confidential and should only be accessed by HR and designated management teams.

4. Compliance and Regulatory Information:

- **Regulatory Communications:** Communications with regulators and responses to regulatory inquiries should not be shared externally, except as directed by legal counsel.

Policy Enforcement:
Strict compliance with this policy is mandatory for all employees and breaches will lead to disciplinary action.

Incident Response:
Immediate reporting of any unauthorized data disclosure to the Data Security team is required.