CME Group *LEADING WITH CONVICTION AND INTEGRITY*

CONFIDENTIALITY POLICY	**CME Group Policy Document No:**	**0009**
	Policy Document Issued By:	**Global Corporate Compliance & Ethics Team**
	Contact Information:	**Global Chief Compliance Officer**
	Date Policy Document Originally Issued:	**November 2013**
	Date Policy Document Last Revised:	**March 2015**

PURPOSE AND STATEMENT OF POLICY

The CME Group organization, including its wholly-owned subsidiaries (collectively, ***"CME Group"*** or the ***"Company"***), is committed to protecting its proprietary and confidential information, including information relating to its business, customers, vendors, strategic partners, employees and other third parties.

CME Group has adopted this Policy to set forth a framework designed to ensure:

- Information is evaluated and properly classified based upon the sensitivity and criticality of the information;
- Appropriate controls are implemented to protect and preserve information based upon its classification; and
- Any ***Regulatory Data*** (defined below), including any swap data received in connection with the Company's operation of data repositories, is used only for permitted purposes in accordance with applicable legal and regulatory requirements.

APPLICABILITY AND SCOPE

This Policy applies to all employees and internal consultants/temporary personnel resources of the CME Group organization, including all of its wholly-owned subsidiaries. The Policy also governs data relating to customers, partners, suppliers and shareholders.

CME Group Information regardless of format (e.g., verbal, hardcopy, electronic) must be protected in a manner commensurate with its classification. For purposes of this Policy, the term ***"CME Group Information"*** means any information classified as **CME Group Internal, CME Group Confidential** and **CME Group Highly Sensitive**. These standards apply at work and at home or any other location where you access CME Group Information regardless of the method for accessing the information.

To the extent CME Group engages a third party vendor to provide services, which include hosting or processing any information classified as **CME Group Confidential** or **CME Group Highly Sensitive**, the business owner of the relationship and representatives from the Cloud Review Team must review the vendor's process and controls against the standards of this Policy. Corporate Procurement can assist with arranging for the required reviews when engaging such vendors.

Your responsibilities to protect CME Group Information continue even after termination of employment with or service to the Company.

DATA CLASSIFICATION REQUIREMENTS AND SECURITY CONTROLS

In order to appropriately protect information, it must be categorized to distinguish the level of security required to safeguard it. Information classification is the process of assigning a level of sensitivity to information and determining to what degree the information needs to be controlled and secured.

The Company has established the following **FOUR** classifications to identify and rank its information to allow it to focus its controls and security efforts in an efficient and structured manner. ***Information Asset Custodians*** and ***Information Asset Owners*** (as defined in the **Corporate Information Security Policy** are accountable for ensuring the information is classified and establishing appropriate safeguards to protect the Integrity, Availability and Confidentiality of CME Group Information

Additional guidance, including specific examples of the type of information belonging to each of the four classifications, the required and available security measures to safeguard such information, the reasonable steps you should take to ensure its protection, the process for seeking approval for access to certain data or the transfer or copying of **CME Group Confidential** or **CME Group Highly Sensitive information** is available in the **Frequently Asked Questions - Confidentiality Policy**.

If you are uncertain of the appropriate classification, assume it is CME Group Confidential. You may contact **Global Information Security** or **Corporate Compliance**, if you have additional questions regarding the classification process or the classification of particular information.

> ***Public:*** Information available to the general public and/or created with the intention for broad distribution outside the Company. This information may be freely disseminated inside and outside the Company without exposing the Company, its customers or employees to financial loss or embarrassment, or jeopardizing the security of the Company's assets.
>
> → **Examples of Public Information:** marketing brochures, advertisements, press releases, published annual reports and content published to www.cmegroup.com.
>
> → **Examples of Security Measures:** version control, read only
>
> ***CME Group Internal:*** Information belonging to the Company created in the normal course of business with the intention of broad, general distribution within (but not outside) the Company. The disclosure, alteration or destruction of such information would create minimal risk of harm to the Company, its customers or employees. Information classified as CME Group Internal should not be shared publicly or outside the Company, except where there is a legitimate business need to do so. Information not broadly made available to the organization such as information maintained solely within a single Department or Division is not considered CME Group Internal.

→ **Examples of CME Group Internal Information:** new employee training materials, compliance policies for the general population, all employee communications, and information made available through a license or subscription.

→ **Examples of Security Measures:** do not distribute outside of the company without a legitimate business need.

CME Group Confidential: Information sensitive to the Company or a third party (e.g., a customer) should only be shared with individuals on a "need to know" basis, meaning the individual needs access to the information to perform their assigned job functions. Improper loss, corruption or disclosure of the information could significantly harm or adversely impact the Company, its customers or employees or could result in a breach of our legal obligations. ***It is expected that the bulk of the Company's information will be classified as CME Group Confidential and the security measures required will vary based on the sensitivity of the content of the information.***

→ **Examples of CME Group Confidential Information:** individual department information, information protected by confidentiality agreements, customer contact information, annual budget, strategic plans and M&A/transactions that are not material to the stock price.

→ **Examples of Security Measures:** Security measures must be designed to preserve the confidentiality and integrity of the information based on the degree to which the loss, corruption or disclosure of the information would harm or adversely impact the Company, its customers and employees or result in legal liability as discussed below. For example, do not leave CME Group Confidential information in hardcopy form unattended and/or unsecured. Electronic versions should be saved to areas with limited access and/or password protected/encrypted and transmitted using a secure method. It is the responsibility of the Information Asset Owner to determine the appropriate protections.

CME Group Highly Sensitive: Information where the unauthorized internal or external access to, alteration or inappropriate destruction of, the information could have a catastrophic impact to the Company, its customers or employees. ***For this information, data integrity is extremely vital and the highest possible levels of confidentiality, restricted access and security measures are essential.*** Refer to the **Frequently Asked Questions – Confidentiality Policy** and **Encryption Standards** for additional information.

→ **Examples of CME Group Highly Sensitive Information:** position data, order and messaging data and detailed transaction data (as defined below), credit card information, social security numbers, bank account information, employees' medical information or health insurance information and other information identified as personally identifiable information.

→ **Examples of Security Measures:** it is CME Group's position that information classified as CME Group Highly Sensitive must be subject to the highest security protections available, such as encryption, and implementable based on the information and/system at issue.

Information classified as **CME Group Confidential** and **CME Group Highly Sensitive** may only be provided outside of CME Group when appropriately authorized and subject to applicable protective measures, such as Non-Disclosure Agreements.

Any disposal of CME Group Information must be done in accordance with the retention requirements of the **Records and Information Management Policy** and the **Electronic Data Destruction Standards & Procedures**.

ADDITIONAL INFORMATION ON DATA COLLECTED FOR REGULATORY PURPOSES INCLUDING SWAP DATA MAINTAINED BY A REPOSITORY

In connection with our role in the financial services industry and the services we provide, many of our employees routinely receive and review information which has been collected to fulfill our obligations under applicable regulatory requirements, including, but not limited to, those set forth by the Commodity Futures Trading Commission (***"CFTC"***), the Financial Conduct Authority (***"FCA"***), the Bank of England (**"*BoE*"**) or the European Securities and Markets Authority (***"ESMA"***).

Regulatory Data, as defined below, is classified as **CME Group Highly Sensitive**. Regulatory Data should only be accessible to people authorized to access such data. It may be used only for regulatory, clearing, risk management, market operation, market and product research and development, and performance monitoring purposes in connection with ensuring the effective operation and integrity of our marketplace, clearing houses and trade repositories.

CME Group is committed to complying with all applicable regulations which require the Company to ensure the confidentiality, integrity and protection of information it receives in connection with its regulatory obligations and operation of trade repositories, including, but not limited to, CFTC, FCS, BoE, and ESMA rules and regulations, as well as requirements under EMIR (e.g., Article 80). The Company will take reasonable steps to prevent any misuse of such information.

For purposes of this Policy, ***Regulatory Data*** means proprietary data or personally identifiable information collected by the Company for the purposes of meeting its regulatory obligations. Regulatory Data includes:

- ***Position data*** – Data collected via the reporting of large trader positions as well as clearing member position data maintained in the Company's clearing and regulatory and repository systems, including trading strategies and valuations.
- ***Financial information*** – Financial records and other information, including account balance information and original third party or internal source documents used in the production of financial reports or used to demonstrate compliance with exchange rules, provided or reported by any entity, including a clearing organization, bank or broker.
- ***Detailed transaction data*** – Trade data including order and messaging data at the specific account or customer level, identifying the primary economic terms of a trade, including but not limited to, buy/sell or price information, from which market positions

and/or profit and loss might be derived. This also includes any swap data collected by our trade repositories.

- ***Investigative materials*** – Information collected as part of surveillance activities or investigations of potential rule violations, such as account statements, trading cards and order tickets, customer account agreements, bank records and video and audio recordings.

Notwithstanding anything to the contrary, any information received by the Company from third-party depositories of clearing members in its capacity as a designated self-regulatory organization (***"DSRO"***) (i) shall be accessible only by such personnel whose role is limited to the discharge of the Company's DSRO responsibilities, and (ii) may be used solely for the surveillance, monitoring or other regulatory purpose for which such information was collected.

Furthermore, access to swap data received by our trade repositories is limited to individuals directly employed by the trade repository itself or who are operating pursuant to a documented Service Level Agreement but only to the degree that such access is necessary for the individuals to perform their assigned job responsibilities, counterparties to a trade (with certain limitations) and approved regulators.

RESPONSIBLITIES REGARDING CONFIDENTIAL INFORMATION

CME Group Confidential and **CME Group Highly Sensitive Information** fall under the definition of ***"Confidential Information"*** as defined in the Acknowledgement and Acceptance of Confidentiality and Intellectual Property Policy and/or an applicable employment agreement (collectively, the ***"Confidentiality Agreement"***). Accordingly, you are obligated by your Confidentiality Agreement to hold all **CME Group Confidential** and **CME Group Highly Sensitive** information in the strictest confidence, and take reasonable precautions to prevent the unauthorized disclosure of such information.

If you receive any subpoena or become subject to any legal obligation to disclose any **CME Group Confidential** or **CME Group Highly Sensitive information** that is not part of your regular responsibilities at CME Group, you must contact an attorney in the Legal Department and comply with any objections made by the Company regarding such disclosure obligations.

Certain employees are also required to execute a Confidentiality, Non-Competition and Non-Solicitation Agreement which contains similar undertakings regarding the preservation and safeguarding of such information.

AVAILABLE RESOURCES AND RAISING CONCERNS

Questions regarding this Policy should be directed to the Global Chief Compliance Officer. Suspected violations of this Policy, including any inappropriate use, disclosure, destruction, theft or loss of **CME Group Confidential** or **CME Group Highly Sensitive Information** (including Regulatory Data) whether intentional or inadvertent, must be raised in accordance with the **Speak Up and Escalation Policy** and your obligations under your Confidentiality Agreement, including reporting to the CME Group Compliance & Ethics Helpline (www.ethicspoint.com). Local phone numbers are available on OpenExchange. Your timely reporting is necessary and

important to ensure the Company can appropriately respond to any inappropriate data disclosure or breach in accordance with applicable legal and regulatory requirements.

OVERSIGHT AND REVIEW OF POLICY

This Policy is subject to the oversight of the Global Corporate Compliance & Ethics Team. CME Group will periodically review and monitor compliance with this Policy as necessary and appropriate. CME Group personnel may be required to execute periodic certifications of compliance with this Policy, as well as attend any required educational programs associated with this Policy. This Policy is subject to review on an as needed basis but at least every three (3) years.

PENALTIES AND CONSEQUENCES

Breaches of the Company's commitment to carefully protect CME Group Confidential information can have serious repercussions on many levels, as well as damage the Company's reputation. Potential violations will be subject to investigation by the Company and/or its agents, and any failure to comply with this Policy may result in discipline, up to and including termination, referral to regulatory authorities, and potential civil and criminal exposure.

Revision History for Confidentiality Policy

Date	Revision
November 2013	• Incorporated the provisions of the separate Data Classification Policy which was retired. • Incorporated the provisions of the separate Confidentiality Policy for Market Regulation and Audit Departments and applied the confidentiality requirements to the entire organization. The separate policy was retired. • Incorporated additional regulatory requirements for the Company's regulated businesses such as CME Repository Services and the UK trade repository.
June 2014	• Incorporated additional regulatory requirements providing for collection of account balance information.
October 2014	• Incorporated clarification of access and use rights with respect to certain information collected in the discharge of designated self-regulatory responsibilities.
March 2015	• Incorporated additional data classification descriptions. • Incorporated examples of information within each data classification that require security measures to safeguard information.