# Systems Monitoring

Purpose

The following describes the practices of JPMorgan Chase & Co., its affiliates and its subsidiaries and the entity that employs you, or for which you provide services (collectively, "JPMC"), with respect to the monitoring of JPMC's physical facilities, equipment and systems (collectively, the "Systems"). These Systems are provided for work-related purposes and monitoring is designed to protect the Systems and your use of the Systems. JPMC monitors the Systems to protect you, your colleagues, the firm, and others as described when you log into your workstation, in our Supplier Code of Conduct, and in this document.

Scope and Application

Systems monitoring applies to JPMC employees or other persons who use JPMC's equipment and systems in the context of an employment or other working relationship with JPMC (collectively, "Workers"). Some Workers may be more frequently monitored than others due to the nature of their work, including registered and licensed personnel and traders (regulated workers). The Systems include business equipment and electronic communications tools, such as servers, terminals, computers, databases, applications, telephones, mobile and portable devices, fax and copy machines, printers, internet, email, instant messaging platforms, and voicemail. Systems monitoring applies to your JPMC equipment, your personal equipment when accessing the Systems, and the communications, information, and materials conveyed or accessed using the Systems.

Monitoring Activities

JPMC may conduct monitoring as described in this document, and in additional notices that may be provided to you, subject to applicable laws and regulations. JPMC's monitoring activities may include:

- monitoring and logging of (1) traffic and usage data (such as routing, addressing, or signaling information, time and date stamps, sender and recipient details and file size) related to incoming, outgoing and internal electronic communications, including emails sent to and from JPMC accounts, chats and instant messages on JPMC-approved channels for business use (such as Bloomberg messages), and any other data moving across the Systems (including internet traffic); and (2) Systems activity, including files or information accessed or downloaded from, or uploaded to Systems;
- monitoring contents of (1) emails sent to and from JPMC accounts; (2) chats and instant messages on JPMC-approved channels for business use; (3) faxes sent to or from JPMC fax numbers; (4) text messages (SMS) sent to or from Systems; (5) files or information accessed or downloaded from, or uploaded to Systems; and (6) internet usage (including pages visited and searches made) (collectively, the "Content");
- monitoring telephone calls to or from JPMC work telephones as required or permitted by applicable laws and subject to any required notices;
- capturing Workers' physical presence at JPMC's facilities via for example access badges and video cameras, which record activities at exits, entrances, corridors, and other public areas; and
- logging hours worked if applicable to the Worker.

To the extent permitted by applicable law, JPMC may at all times monitor, access, retrieve, record, and review information obtained via monitoring activities, including any Content, and any personal use of the Systems, as reasonably necessary or advisable in JPMC's interests for purposes including:

- preventing and investigating activities that could violate JPMC's policies or applicable laws, such as market abuse, financial crimes, bank regulatory and reporting violations, improper product marketing, mis-selling, trade violations, Code of Conduct violations, or misuse or inappropriate sharing of information;

- detecting, blocking, and flagging offensive terms or Content on the Systems; access to inappropriate or unauthorized websites or IP addresses; and unauthorized transmissions of confidential, proprietary, or sensitive information;
- finding lost or deleted messages;
- auditing and conducting other internal analyses;
- complying with legal or regulatory obligations; and
- protecting the security of JPMC's Systems or other assets, including flagging potential misuse of the Systems and detecting viruses and malicious software and unauthorized access.

Monitoring activities may be conducted (1) by automated means, sampling or manual reviews; and (2) routinely or in connection with specific incidents, investigations, or inquiries from human resources or other departments. Subject to applicable laws and regulations, information obtained from the monitoring activities may be used as the basis to take disciplinary actions, up to and including termination or other legal action, for violations of JPMC's policies or applicable laws.

Personal Information

While conducting monitoring activities, JPMC may obtain and process personal information about you and others, including names, email addresses, home addresses, account information, and other personal information, that may reside on the Systems. JPMC takes steps to process the minimum personal information necessary when conducting monitoring activities. To the extent permitted by applicable law, the monitoring activities are required to promote adherence to applicable policies and regulations.

Disclosures

As permitted or required by law and for the purposes noted above, JPMC may disclose Content or other information obtained in connection with monitoring activities to JPMC affiliates or to third parties, service providers, regulators, supervisory bodies, law enforcement, or other government agencies. JPMC and its affiliates may jointly use any information collected in connection with monitoring activities for the purposes described here.

Cross-Border Data Transfers

JPMC may transfer the information it obtains in connection with monitoring activities to countries other than the country in which the information originally was collected, including to the United States, subject to applicable laws and regulations.

Retention

JPMC may retain the information obtained in connection with the monitoring activities for as long as (1) necessary to accomplish the purposes for which the information was collected or (2) the information is stored for legal or regulatory purposes such as regarding regulated workers.

Rights of Workers

This document describes any rights you may have, including rights to access and correct information JPMC obtains about you, in accordance with established procedures in your country. Please direct any questions you may have to your JPMC assignment sponsor.