Global Technology Acceptable Use Policy for Contingent Workers (AUP-CW)

The Acceptable Use Policy for Contingent Workers (AUP-CW) defines appropriate and inappropriate uses of JPMorgan Chase technology or information resources irrespective of their medium, and provides guidance to contingent workers' use of these resources, whether those resources are used for personal or business purposes.

For each new engagement in which a JPMC contingent worker is assigned, all JPMC contingent workers are required to confirm that they understand their information security responsibilities by reviewing and affirming to this AUP-CW and the Supplier Code of Conduct.

DEFINITION

For the purposes of this document, the terms "inappropriate use" of JPMorgan Chase information resources and "inappropriate material" include any uses or material that could be construed by a reasonable person or a court of law as being generally offensive, abusive, illegal, immoral, or unethical; in violation of applicable laws, regulations, or corporate policies or standards; or that in any way jeopardizes the confidentiality, integrity, or availability of the Firm's technology or information resources or intellectual property, or that compromises the Firm's tangible or intangible assets, including its name, reputation, and logo. Contingent workers must not use the Firm's technology or information resources for inappropriate purposes. Inappropriate use is grounds for termination of engagement and other remedies available to JPMC.

As it relates to contingent workers, an "Assignment Sponsor" is the day-to-day manager for the contingent worker who is responsible for the engagement.

APPROPRIATE USES

The following list is provided as guidance to contingent workers; it is not meant to include examples of all types of appropriate use:

- Agree to report to your Assignment Sponsor any possible threat or incident to ensure the Firm's information resources in their area are protected from accidents, tampering, viruses and unauthorized use or modification.
- Understand that the Firm has a vested interest in maintaining the integrity of copyrighted information, and should be particularly sensitive to copyrighted information.
- Agree to handle all information stored on a computer or downloaded to portable media such as flash drives and hard copies with appropriate care to prevent unauthorized disclosure of the information.
- Agree to protect passwords and never disclose or share them with anyone, and agree to make passwords hard to guess by following the Firm's password composition standards.
- Agree to report to their Assignment Sponsor any possible or actual security violations that come to their attention, and understand that violation of this AUP-CW can lead to termination of engagement.
- Understand that by using JPMorgan Chase's information resources, contingent workers knowingly agree and consent to their usage being monitored and examined, and acknowledge JPMorgan Chase's right, subject to applicable laws and regulations, to conduct such monitoring, including, but not limited to, retrieving, reading, inspecting and disclosing any information therein.

INAPPROPRIATE USES

The following list is provided as guidance to users; it is not meant to include examples of all types of inappropriate use. If you are unsure if an anticipated use of JPMorgan Chase information resources is inappropriate, consult with your manager or your LOB Information Risk Manager.

1. **General Terms** – Inappropriate use of JPMorgan Chase's information resources includes, but is not limited to, the following:

    - Using information resources for personal business.
    - Using information resources for actions that violate this AUP-CW, the Supplier Code of Conduct or any other JPMorgan Chase supplier policy.

- Using information resources in a manner that jeopardizes the confidentiality, integrity, or availability of the information resources.
- Transmitting information in violation of applicable law or regulation, this AUP-CW, the Supplier Code of Conduct, or any other JPMorgan Chase supplier policy.
- Using non-JPMorgan Chase owned, leased, or authorized equipment including removable storage media to store, process, or transmit non-public JPMorgan Chase information.

2. **Inappropriate Uses of Email** - Inappropriate use of email includes, but is not limited to, the following:

    - Sending or forwarding email from a JPMorgan Chase managed email account to:
        - A personal account or external corporate account. Contingent workers must not forward emails from a JPMorgan Chase managed email account to their personal email account or external corporate email account for any purpose.
        - Any non-JPMorgan Chase managed email account via directory entries, agents, or applications, including those that are automated.
    - Using a non-Firm managed account to store JPMorgan Chase email.
    - Forwarding electronic chain letters.
    - Using a JPMorgan Chase managed email account for unauthorized solicitation purposes.
    - Using a JPMorgan Chase managed email account for any other purpose outside the scope of engagement.

3. **Inappropriate Uses of Authentication Information** – Users must establish, alter, and retain sole, secure knowledge of passwords and any other means of identity authentication as directed by JPMC. Inappropriate uses/conditions that could compromise authentication information, systems, or network security include, but are not limited to, the following:

    - Using software to log keystrokes in a production environment.
    - Using or possessing password cracking programs, security vulnerability assessment, exploitation tools, or network sniffers to capture and view transmitted data, network discovery tools, system discovery or inventorying tools, unless as part of engagement as expressly authorized in a contract with JPMC and signed by both JPMC and Supplier.

4. **Inappropriate Uses of Software** – Inappropriate activity with software files/programs includes, but is not limited to, the following:

    - Downloading, uploading, copying, or distributing software or electronic files in violation of their copyright.
    - Downloading, uploading, saving, or trading music or video files whether or not the action is in violation of applicable copyright restrictions.
    - Downloading or uploading any software or electronic files, including legitimate information, without up-to-date virus protection measures in place.
    - Intentionally accessing, downloading, uploading, saving, or sending sexual, pornographic, discriminatory, or criminal material.

5. **Inappropriate Activity Regarding System Builds/Configurations** – Inappropriate activity to modify system builds or configurations includes, but is not limited to, the following:

    - Disabling or removing any security software; for example, access control or computer virus control.
    - Installing, disabling, or removing software, other than device drivers, on a JPMorgan Chase computer.

6. **Inappropriate Internet-related Activity** – Inappropriate Internet-related activity includes, but is not limited to, the following:

    - Sending or storing the Firm's data or files on non-JPMC web-based data storage services, for example, Google Drive, Mega, 4Shared, iCloud, etc.
    - Establishing undocumented and unapproved Internet or other external network connections that could allow a non-JPMorgan Chase user to gain access to JPMorgan Chase systems and

information.

- Using the JPMorgan Chase Intranet to access non-corporate-standard email accounts such as MS Hotmail, Yahoo Mail, and Gmail.
- Placing JPMorgan Chase material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP).
- Posting non-public JPMorgan Chase or any other type of information that may compromise the security of the Firm's assets or violate supplier policies or the Supplier Code of Conduct via Internet-accessible message boards, blogs, social networks and other forms of communication. For more details, please also see the Continent Work Social Media Policy.
- Using the JPMorgan Chase name or logo on the Internet.
- Gambling.
- Accessing or downloading pornographic material.
- Making or posting indecent, offensive, discriminatory, harassing, or disruptive remarks, or other inappropriate content.
- Creating or using intranet blogs that contain Confidential or Highly Confidential information.