JPMC'S MINIMUM CONTROL REQUIREMENTS

These Minimum Control Requirements ("**Minimum Control Requirements**") are stated at a relatively high level, and JPMC recognizes that there may be multiple approaches to accomplish a particular Minimum Control Requirement. Supplier must document in reasonable detail how a particular control, including those pertaining to dependent suppliers (subcontractors) who collect, transmit, share, store, control, process, manage or access JPMC Data, meets the stated Minimum Control Requirement. All Minimum Control Requirements apply to dependent suppliers, even if dependent suppliers are not specifically mentioned in the particular control requirement. JPMC may revise the Minimum Control Requirements from time to time, and such revisions will become effective upon publication to the Supplier portal. Supplier will comply with and implement the revised JPMC Minimum Control Requirements as soon as commercially reasonable or otherwise agreed in writing by JPMC. The term "should" in these Minimum Control Requirements means that Supplier will use commercially reasonable efforts to accomplish the stated Minimum Control Requirement, and will document those efforts in reasonable detail, including the rationale, if any, for deviation. This documentation may be reviewed by Auditors to assess the control and the merit of the rationale for deviation. Not all of the stated Minimum Control Requirements will apply to all Services or other Deliverables, but Supplier must be able to reasonably show how the Minimum Control Requirement does not apply. These Minimum Control Requirements do not limit Supplier's obligations under the Agreement or applicable Law, and do not limit the scope of an audit by JPMC. JPMC may use TruSight Solutions, LLC ("**TruSight**") as an external Auditor to facilitate and conduct Audits. TruSight, in turn, may use an independent firm, *e.g.*, EY, as an external Auditor to conduct Audits. Supplier will cooperate with any such external Auditor as reasonably requested by JPMC or any such external Auditor, including entering into agreements any of them may request from time to time, fully and promptly answering questionnaires that JPMC or any of them may submit (including submitting information using electronic or other portals or facilities), meeting with any of them to facilitate the Audit, and not requesting any of them to execute a separate non-disclosure agreement.

As used in these Minimum Control Requirements, (i) "**including**" and its derivatives mean "including but not limited to"; (ii) any capitalized terms not defined herein shall have the same meaning as set forth in the Master Agreement relating to the Services and other Deliverables to which these Minimum Control Requirements relate (the "**Agreement**"); and, (iii) "Confidential Information" is understood to include "Highly Confidential Information", "Personal Information", and "JPMC Data".

RISK MANAGEMENT.

The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.

Risk Assessment.

A risk assessment must be performed annually to verify the implementation of controls that protect business operations and JPMC Data.

SECURITY POLICY.

A documented set of rules and procedures must regulate the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of information and associated services.

Security Policies and Exception Process.

Security policies must be documented, reviewed, and approved, with management oversight, on a periodic basis, following industry best practices.

A risk based exception management process must be in place for prioritization, approval, and remediation or risk acceptance of controls that have not been adopted or implemented.

Awareness and Education Program.

Security policies and responsibilities must be communicated and socialized within the organization to Supplier Personnel (*e.g.*, both employees and contractors). Supplier Personnel must be trained to identify and report suspected security weaknesses and incidents.

ORGANIZATIONAL SECURITY.

A Supplier Personnel security policy and agreements, established organizational requirements to ensure proper training and competent performance, and an appropriate and accountable security organization must be in place.

Organization.

Training and job competence of Supplier Personnel providing services to JPMC must be monitored using a formal performance and appraisal process. Current organizational charts representing key management responsibilities for services provided, including services provided by dependent suppliers, regardless of tier, must be maintained.

Supplier Personnel Security Policy.

Background checks (including criminal) must be performed on applicable Supplier Personnel.

Agreements.

Supplier Personnel must be subject to written non-disclosure or confidentiality obligations before being assigned to JPMC services and granted access to JPMC systems and information.

TECHNOLOGY ASSET MANAGEMENT.

Controls must be in place to protect assets, including mechanisms to maintain an accurate inventory of assets and handling standards for introduction and transfer, removal and disposal of all assets. Any personally-owned devices used by Supplier Personnel for business purposes must be taken into account.

Accountability.

A process for maintaining an inventory of hardware and software assets and other information resources, such as databases and file structures, must be documented.

Process for periodic asset recertification must be documented. Identification of unauthorized or unsupported hardware/ software must be performed.

Disposal or Reuse.

Procedures for disposal or reuse of equipment used for logical and physical storage must accomplish sufficient destruction of JPMC Data. Procedures must be documented for sanitization, consistent with the requirements of NIST Standard 800-88 Revision 1, Appendix A ("Guidelines for Media Sanitization").

Personal Asset Controls.

Security policies and controls must be documented, reviewed, and approved, with management oversight, on a periodic basis, if personal devices are used to perform business transactions or to access systems where JPMC Data or transactions are stored or processed.

Procedures must be in place to remove JPMC Data and access rights to systems on which JPMC Data are stored, processed, or transmitted.

PHYSICAL AND ENVIRONMENTAL.

Controls must be in place to protect against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.

Physical and Environmental Security Policy.

Physical and environmental security plans must exist for facilities and scenarios involving access or storage of JPMC Data. Additional physical and environmental controls must be required and enforced for server/ datacenter locations.

Physical Control.

Storage of JPMC Data at new facilities or locations that are not a Supplier facility must be pre-approved by JPMC before use.

Physical access, to include visitor access, to facilities must be restricted and all access periodically recertified.

Asset addition/ removal process from the facility must be documented. Approval from JPMC must be obtained before assets with JPMC Data are removed from the facility.

Policies must be in place to ensure that information is accessed on a need-to-know basis.

Environmental Control.

Facilities, including data and processing centers, must maintain appropriate environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection. Environmental control components must be monitored and periodically tested.

COMMUNICATION AND CONNECTIVITY.

Supplier must implement controls over its communication network to safeguard data. Controls must include securing network and implementation of encryption, logging and monitoring, and disabling communications where no business need exists.

Network Identification.

A network diagram, to include all devices, must be kept current to facilitate analysis and incident response.

A current data flow diagram must depict JPMC Data from origination to end point (including data shared with dependent suppliers).

Data Storage.

All JPMC Data, including JPMC Data shared with dependent suppliers, must be stored and maintained in a manner that allows for its return or secure destruction upon request from JPMC.

Firewalls.

Firewalls must be used for the isolation of all environments, to include physical, virtual, network devices, production and non-production, and application/ presentation layers. Firewall management must follow a process that includes restriction of administrative access and that is documented, reviewed, and approved, with management oversight, on a periodic basis.

The production network must be either firewalled or physically isolated from the development and test environments. Multi-tier security architectures that segment application tiers (*e.g.*, presentation layer, application and data) must be used.

Periodic network vulnerability scans must be performed and any critical vulnerabilities identified must be remediated within a defined and reasonable timeframe (*e.g.*, within three months).

Clock Synchronization.

Network devices must have internal clocks synchronized to reliable time sources.

Remote Access.

The data flow in the remote connection must be encrypted and multi-factor authentication must be utilized during the login process.

Remote connection settings must limit the ability of remote users to access both initiating network and remote network simultaneously (*i.e.*, no split tunneling).

Dependent suppliers' remote access must adhere to the same controls and any subcontractor remote access must have a valid business justification.

Wireless Access.

When used to provide services for JPMC, wireless access to the Supplier corporate network must be configured to require authentication and be encrypted.

Data Loss Prevention.

Data Loss Prevention (DLP) solutions should be deployed to protect JPMC Data, including all points of egress, except to the extent prohibited by legal or regulatory restrictions.

CHANGE MANAGEMENT.

Changes to the system, network, applications, data files structures, other system components and physical/ environmental changes must be monitored and controlled through a formal change control environment. Changes must be reviewed, approved and monitored during post-implementation to ensure that expected changes and their desired result are accurate.

Change Policy and Procedure.

Change management policy, including application, operating system, network infrastructure and firewall changes must be documented, reviewed and approved, with management oversight, on a periodic basis. An emergency change management procedure must be specified, including factors leading to emergency change.

The change management policy must include clearly identified roles and responsibilities so as to support separation of duties (*e.g.*, request, approve, implement). The approval process must include pre- and post-evaluation of change. Changes materially affecting JPMC services must be communicated to JPMC prior to implementation.

Emergency Change Procedures.

Emergency change procedures must be in place. Changes materially affecting JPMC services must be communicated to JPMC.

OPERATIONS.

Documented operational procedures must ensure correct and secure operation of the Supplier's assets.

Operational Procedures and Responsibilities.

Operational procedures must be documented and, include monitoring of capacity, performance, service level agreement and key performance indicators.

Problem Management.

Documented problem management processes and procedures must include systematic tracking of problems from discovery to resolution.

LOGICAL ACCESS CONTROL.

Authentication and authorization controls must be appropriately robust for the risk of the data, application and platform; access rights must be granted based on the principle of least privilege and monitored to log access and security events, using software that enables rapid analysis of user activities.

Logical Access Control Policy.

Documented logical access policies and procedures must support role-based, "need-to-know" access (*e.g.*, interdepartmental transfers, terminations) and ensure separation of duties during the approval and provisioning process. Each account provisioned must be uniquely identified. All accounts must be recertified on a periodic basis.

Privileged Access.

Management of privileged user accounts (*e.g.*, those accounts that have the ability to override system controls), to include service accounts, must follow a documented processes and be restricted.

A periodic review and governance process must be maintained to ensure appropriate provisioning of privileged access.

Authentication and Authorization.

A documented authentication and authorization policy must cover all applicable systems. That policy must include password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized. Authentication credentials must be encrypted, including in transit to and from dependent suppliers' environments or when stored by dependent suppliers.

DATA INTEGRITY.

Controls must ensure that any data stored, received, controlled or otherwise accessed is accurate and reliable. Inspection procedures must be in place to validate data integrity.

Data Transmission Controls.

Processes, procedures and controls must be documented, reviewed, and approved, with management oversight, on a periodic basis, to ensure data integrity during transmission and to validate that the data transmitted is the same as data received.

Data Transaction Controls.

Controls must be in place to protect the integrity of data transactions at rest and in transit.

ENCRYPTION.

Data must be protected and should be encrypted, both in transit and at rest, including when shared with dependent suppliers.

Encryption Policy.

Data protection policy must cover data classifications, encryption use, key and certificate lifecycle management, cryptographic algorithms and associated key lengths. Policy must be documented, reviewed, and approved with management oversight, on a periodic basis.

Encryption Uses.

JPMC Data must be protected, and should be encrypted, while in transit and at rest across the following types of assets:

- Public shared networks
- Non-wired networks
- Cloud services
- Desktop and portable computing devices
- Mobile devices
- Portable media
- Back-ups
- 'Plug & play' storage devices

Highly Confidential Information must be protected, and should be encrypted, when stored on the types of assets listed above and while in transit over any network; authentication credentials must be encrypted at all times, in transit or in storage.

INCIDENT RESPONSE.

A documented plan and associated procedures, to include the responsibilities of Supplier Personnel and identification of parties to be notified in case of an information security incident, must be in place.

Incident Response Process.

The information security incident management program must be documented, tested, updated as needed, reviewed, and approved, with management oversight, on a periodic basis. The incident management policy and procedures must include prioritization, roles and responsibilities, procedures for escalation (internal) and notification (to JPMC), tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity.

BUSINESS CONTINUITY AND DISASTER RECOVERY.

Suppliers must have formal documented recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to the business unit, support group unit,

application, or infrastructure component. Plans assure timely and orderly recovery of business, support processes, operations and technology components within an agreed upon time frame and include orderly restoration of business activities when the primary work environment is unavailable.

Business Recovery Plans.

Comprehensive business resiliency plans addressing business interruptions of key resources supporting all JPMC services, including those provided by dependent suppliers, must be documented, tested, reviewed, and approved, with management oversight, on a periodic basis. The business resiliency plan must have an acceptable alternative work location in place to ensure service level commitments are met.

Technology Recovery.

Technology recovery plans to minimize service interruptions and ensure recovery of systems, infrastructure, databases, applications, etc., must be documented, tested, reviewed, and approved with management oversight, on a periodic basis.

EMAIL AND IM.

Policies and procedures must be established and adhered to that ensure proper control of an electronic mail and/ or instant messaging system that displays and/ or contains JPMC Data.

Authorized E-mail Systems and Instant Messaging.

Access to non-corporate/ personal email and instant messaging solutions must be restricted. Controls must be in place to prevent Confidential Information from being sent externally through email or instant messaging without encryption. Preventive controls must block malicious messages and attachments. Controls must be in place to prevent auto-forwarding of emails.

BACK-UP AND OFFSITE STORAGE.

Supplier must have policies and procedures for back-up of JPMC Data. Back-up media must be protected in storage, offsite storage, and sanitized prior to disposal or reuse.

Back-up and Redundancy Processes.

Processes enabling full restoration of all systems, applications, and data must be documented, reviewed, and approved, with management oversight, on a periodic basis.

Back-up Media Destruction.

Back-up media must be rendered unreadable when no longer required.

Offsite Storage.

Physical security policy for the offsite facility must be documented, reviewed, and approved, with management oversight, on a periodic basis. Back-up storage devices must be encrypted. Secure transportation procedures of media to and from offsite locations must be defined.

MEDIA AND VITAL RECORDS.

Policies for handling and storing electronic media containing JPMC Data and paper records must be in place, including secure disposal of media and secure transport and transmission to and from Supplier and dependent suppliers.

Handling and Storage.

Electronic media and paper records storage and movement procedures must be documented, reviewed, and approved, with management oversight, on a periodic basis, both by Supplier and dependent suppliers.

Record Control.

Electronic media and paper records must be stored in secure bins. Retention procedures for all paper and electronic records must be in accordance with JPMC record retention requirements. Document destruction or shredding must be performed in a secure manner.

Transportation Logistics.

The company utilized for transportation of media must be licensed and bonded to provide the services. The transportation company drivers must undergo background checks and receive training to safeguard information during transport. Controls must be in place to safeguard electronic media and paper records during transportation.

THIRD PARTY RELATIONSHIPS.

All dependent suppliers must be identified, assessed, managed and monitored. Dependent suppliers that provide material services, or that support Supplier's provision of material services to JPMC, must comply with all control requirements applicable to any such services.

Selection and Oversight.

Supplier must have a process to identify all dependent suppliers providing services to Supplier; these dependent suppliers must be disclosed to JPMC and approved to the extent required by the Master Agreement. Risk assessments of each dependent supplier's control environment must be performed.

Lifecycle Management.

Supplier must establish contracts with dependent suppliers providing material services; these contracts must incorporate security control requirements, including data protection controls and notification of security and privacy breaches must be included.

Performance review processes must be in place to ensure dependent suppliers' fulfillment of contract terms and conditions.

STANDARD BUILDS.

Information systems must be deployed with appropriate security configurations and reviewed periodically for compliance with Supplier's security policies and standards.

Secure Configuration Availability.

Standard security configurations must be established and security hardening demonstrated. Process documentation must be developed, maintained, and under revision control, with management oversight, on a periodic basis. Configurations must include security patches, vulnerability management, default passwords, registry settings, file directory rights and permissions.

System Patches.

Security patch process and procedures, to include requirements for timely patch application, must be documented.

Operating System.

All versions of operating systems in use must be supported and respective security baselines documented.

Desktop Controls.

Systems must be configured to provide only essential capabilities. Policy must prohibit storing of Confidential Information on desktops. The ability to write to electronic media must be limited to documented exceptions.

APPLICATION.

Supplier must have an established software development lifecycle for the purpose of defining, acquiring, developing, enhancing, modifying, testing or implementing information systems. Supplier must ensure that all web-based and mobile applications used to store, receive, send, control or access JPMC Data are monitored, controlled and protected.

Functional Requirements.

Applications must implement controls that protect against known vulnerabilities and threats, including Open Web Application Security Project (OWASP) Top 10 Risks, risks outlined in NIST, FFIEC, and PCI (PCI-DSS, PA-DSS, PCI Pin Security), and denial of service (DDOS) attacks.

Application layer controls must provide the ability to filter the source of malicious traffic.

Restrictions must also be placed on or in front of web server resources to limit denial of service (DoS) attacks.

Supplier must monitor uptime on a hosted web or mobile application.

The application must perform verification checks for completeness, balancing and reconciliation to data-file balances after transaction updates.

Applications must have the ability to determine that operating environments are at acceptable levels, including root/ jailbreak checks, software/ operating system/ patch level checks, and to prevent launch on devices that have been compromised or are insufficiently up-to-date.

Procedures around consent (for the users) and procedures to re-validate on a recurring basis any Personal Information gathered, stored, sent, received, or accessed by applications must be defined.

Where requirements or risk factors indicate that single-factor authentication is inadequate, including all instances of external connections to JPMC networks as well as corporate/ non-customer authentication to Internet-facing applications that involve high-risk transactions such as the ability to transfer funds or to access Confidential Information the application must implement multi-factor authentication.

An additional, network-level restriction must be in place to secure JPMC/ corporate access to dependent supplier hosted applications that handle Confidential Information.

Software Development Life Cycle.

A Software Development Life Cycle (SDLC) methodology, including release management procedures, must be documented, reviewed, approved, and version controlled, with management oversight, on a periodic basis. These must include activities that foster development of secure software, for example:

- Security requirements in requirements phase,
- Secure architecture design,
- Static code analysis during development,
- Dynamic scanning or penetration testing of code during QA phase, and
- Remediation of vulnerabilities rated High and above before moving to the next phase.

Validation of security requirements (*e.g.*, Information Security (IS) sign-offs, periodic IS reviews, static/ dynamic scanning) must follow a documented methodology.

SDLC methodology must include requirements for documentation and be managed by appropriate access controls. Developer access to production environments must be restricted by policy and in implementation.

Code certification, including security review of code developed by third parties (*e.g.*, open source, contracted developers), must be performed. Third party and open source code used in applications must be appropriately licensed, inventoried, supported, patches applied timely, tested prior to use in production, and evaluated for security defects on an on-going basis, with any identified gaps remediated in a timely manner.

Testing and Remediation.

Software executables related to client/ server architecture that are involved in handling JPMC Data must be undergo vulnerability assessments and penetration tests (both the client and server components) prior to release and on an on-going basis, either internally or using external experts, and any gaps identified must be remediated in a timely manner.

Testing must be based on, at a minimum, the OWASP Top 10 risks (or the OWASP Mobile Top 10 risks, where applicable) and the SysAdmin, Audit, Networking, and Security Institute (SANS) Top 25 software security risks, or comparable replacement.

Where JPMC production data is used in a test environment, the level of control must be consistent with production controls. Production data must be sanitized (*e.g.*, masking of all Personal Information) before use in non-production environments.

CUSTOMER CONTACT.

Suppliers providing call center or telemarketing services must have defined and enforced operational procedures that ensure the confidentiality, integrity and availability of JPMC Data.

Customer Contact Operations.

Prior to working on JPMC related calls, customer contact agents must receive training regarding the proper provision of Services and other Deliverables and privacy training, which must cover:

- privacy information classification,
- legal, regulatory and contract responsibilities for privacy,
- consequences (including penalties) for violations of privacy Law,
- contract obligations,
- email and internet usage guidelines regarding privacy and monitoring, and
- information on Supplier Personnel and Supplier equipment monitoring policies.

Protocols used by the agents to authenticate the identity of the customer must be defined.

VULNERABILITY MONITORING.

Supplier must continuously gather information and analyze vulnerabilities in light of existing and emerging threats and actual attacks. Processes must include vulnerability scans, anti-malware, Intrusion Detection Systems, Intrusion Prevention Systems, logging and security information and event management analysis and correlation.

Vulnerability Scanning and Issue Resolution.

Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically and prior to system provisioning for all systems that process, store or transmit JPMC Data. Remediation plans and timelines must be communicated to JPMC.

Malware.

All devices must be kept up-to-date with latest anti-virus definitions to mitigate known threats. Anti-virus tools must be configured to run periodic scans to detect, log and disposition malware.

Intrusion Detection/ Prevention.

Network and host-based intrusion detection and intrusion prevention systems (IDS and IPS) must be deployed with events generated fed into centralized systems for analysis. These systems must accommodate routine updates and real-time alerting. IDS/ IPS signatures must be kept up-to-date to respond to threats.

Logging and Event Correlation.

Monitoring and logging must support centralization of all security events for analysis and correlation. Organizational responsibility for responding to events must be defined. Retention schedule for various logs must be defined and followed.

REGULATORY COMPLIANCE.

Processes must be in place to ensure the protection of JPMC Data and compliance with legal and regulatory requirements applicable to the Services and other Deliverables.

Regulatory Compliance.

Supplier must comply with and have processes for researching, evaluating, and complying with, all Laws relevant to the business, process, or activity being undertaken in the particular jurisdiction(s). Any alleged non-compliance with Laws, regulatory inquiries, and actual or threatened legal claims, must be escalated to JPMC.

PRIVACY.

Supplier must implement effective controls to ensure appropriate processing and protection of Personal Information.

Confidential Information.

Supplier must ensure that all JPMC Minimum Control Requirements that apply to Confidential Information are also implemented with respect to Personal Information.

Logical Access Control.

Social Security Numbers or other national or identifiers must not be utilized as User IDs for logon to applications.

Website.

Procedures around cookie activity must be compliant with the applicable Laws.

System Development.

Privacy impact assessment must be conducted during the requirements phase of system development to evaluate the impact to Personal Information.

Monitoring.

Privacy impact assessment must be performed to review the scope of monitoring. The assessment must not conflict with any applicable local and other Laws.

Regulatory Compliance.

Procedures around consent, as applicable, for the users must be defined. A privacy notice or information banner exists and must be acknowledged by the end user whenever Personal Information is collected, transmitted, processed or stored. Procedures around collecting Personal Information as required by the Law must be defined and restrictions on disclosing that Information must be documented. A process to allow users to access correct, opt-out, delete, restrict, make portable, or object to the processing of, Personal Information must be documented, reviewed, and approved, with management oversight, on a periodic basis.

CLOUD TECHNOLOGY.

Adequate safeguards must ensure the confidentiality, integrity, and availability of JPMC Data stored, processed or transmitted using cloud technology (either as a cloud customer or cloud provider, to include dependent suppliers), using industry standards (*i.e.*, NIST SP 800-145, NIST SP 500-322).

Audit Assurance and Compliance.

The cloud environment in which data is stored, processed or transmitted must be compliant with relevant industry standards and regulatory restrictions.

Application and Interface Security.

Threat modeling must be conducted throughout the software development lifecycle, including vulnerability assessments, including Static/ Dynamic scanning and code review, to identify defects and complete remediations before hosting in cloud environments.

Business Continuity Management and Operational Resiliency.

Business continuity plans to meet JPMC recovery objectives must be in place.

Data Security and Information Lifecycle Management.

Proper segmentation of data environments and segregation between customers must be employed; segmentation/ segregation must enable proper sanitization, per industry requirements.

Encryption and Key Management.

All communications must be encrypted in-transit between environments.

Governance and Risk Management.

Comprehensive risk assessment processes and centralized monitoring that enables incident response and forensic investigation must be used to ensure proper governance and oversight.

Identity and Access Management.

Management of accounts, including accounts with privileged access, must prevent unauthorized access and mitigate the impacts thereof.

Interoperability and Portability.

JPMC Data must be available upon request, in an industry standard format, so as to ensure portability and interoperability.

Infrastructure and Virtualization Security.

Controls defending against cyberattacks, including principle of least privilege, baseline management, intrusion detection/ prevention systems, host/ network-based firewalls, segmentation,

isolation, perimeter security, access management, detailed data flow information, network time, and a SIEM solution must be implemented.

Security Incident Management, E-Discovery and Cloud Forensics.

Technology and associated processes must support the ability to isolate all JPMC Data and systems, maintain the system state, and preserve artifacts required for incident response and forensics investigations.

Supply Chain Management, Transparency and Accountability.

Supplier must be accountable for the confidentiality, availability and integrity of all data, to include data processed in cloud environments by dependent suppliers.

Threat and Vulnerability Management.

Vulnerability scans (authenticated and non-authenticated) must be performed, both internally and externally, for all systems. Processes must be in place to ensure tracking and remediation.

BUSINESS PRACTICES.

Policies and procedures must ensure management oversight of business operations as well as appropriate responses to any suspected instances of fraud.

Business Practices.

Policies and procedures addressing Supplier business operations, processes for responding to customer complaints, handling of non-public information, signing authority, code of conduct, and change control must be documented, reviewed, and approved, with management oversight, on a periodic basis, and made available to Supplier Personnel.

Fraud.

A fraud detection, prevention and mitigation program, processes and procedures for monitoring and reporting actual and suspected instances of fraud, and specific notification and communication, internally and to JPMC, must be documented, reviewed, and approved, with management oversight, on a periodic basis.

DATA USE.

Suppliers and dependent suppliers who receive, send, transmit, store, create, generate, collect, control, process or have access to JPMC Data, must do so solely to provide services to JPMC.

Data Use.

Policies and processes covering data use and restrictions, including for JPMC Data shared with dependent suppliers, must be documented and reviewed, with management oversight, on a periodic basis. Uses and restrictions must include transformation, aggregation, de-identification, creation of derivatives, or alteration of JPMC Data.