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 third party providers (subcontractors) who collect, transmit, share, store, control, process, manage or access JPMC Data, meets the stated Minimum Control Requirement. All Minimum Control Requirements should apply to dependent third party providers (subcontractors), even if dependent third party providers (subcontractors) 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.

As used in these Minimum Control Requirements, (i) "**including**" and its derivatives mean "including but not limited to", and; (ii) any capitalized terms not defined herein shall have the same meaning as set forth in the applicable Master Services Agreement.

Note that certain of these Minimum Control Requirements apply to Highly Confidential Information. **"Highly Confidential Information"** refers to a subset of Confidential Information, the disclosure of which to unauthorized parties could compromise business secrets, jeopardize important interests, or result, directly or indirectly, in serious adverse financial, reputational or regulatory consequences. Examples of Highly Confidential information include:

- Personal Information that is designated as Highly Confidential by JPMC. This includes a small number of information elements on their own, but is more typically a combination of PI elements that includes a PI direct identifier (*e.g.*, email address, first/ given name, family name, nickname, physical address, telephone number). If wrongly disclosed, these information elements could result in regulatory or customer notification requirements (*e.g.*, breach reporting), a significant increased risk of identity theft or fraud, or is considered highly sensitive to the individual
- Passwords and authentication credentials
- Security keys (*e.g.*, encryption keys), with the exception of public keys used in asymmetric encryption schemes
- **"Material Non Public Information (MNPI)"**, which refers to information that, prior to general or public disclosure, is likely to impact market valuations (*e.g.*, share prices), including (but not limited to):
    - Strategic planning information, prior to general or public disclosure
    - Information relating to mergers, acquisitions or divestitures
    - Initial Public Offering (IPO) financial details
    - Financial forecasts or results (*e.g.*, raw closing data analysis)
- Information revealing details of security incidents affecting JPMC

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. Roles and responsibilities for performing risk assessments and responding to results must be defined.

Risk Remediation.

Risk assessment remediation plans must have owners and use issue tracking to completion that regularly measures progress against target dates. Risk acceptances must include business justification, a clear description of the risk and acknowledgement by management.

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 by management on an annual 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. Methods of communication should include training programs, internal communications, and internal portals.

Education, awareness and cross-training program attendance reports must be maintained.

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 must be maintained.

Supplier Personnel Security Policy.

Background checks (including criminal) must be performed on applicable Supplier Personnel as required by the contract.

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.

Security Organization.

An established Information Security function must be in place and include:

A named employee of the Supplier accountable for leading information security initiatives in the Supplier organization.
Job responsibilities defined and assigned to ensure effective management of information security and appropriate separation of duties within the organization.
Clear definition of who is permitted to access, process or store a particular kind of data.
Periodic reviews of roles and responsibilities.
Review and approval of management of roles and responsibilities for assignment and regular reviews.

ASSET MANAGEMENT.

Controls must be in place to protect Supplier assets, including mechanisms to maintain an accurate inventory of assets and handling standards for introduction and transfer, removal and disposal of all assets based on asset classification. 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.

For hardware assets, inventory should include:

Asset control tag
Physical location (*e.g.*, mobile and removable devices should identify default location)
Asset owner
Operating system
Environment (*e.g.*, development, test or production)
Asset Classification

For software assets, inventory should include:

Environment (*e.g.*, development, test or production)
Software version
Host name and location
Software licenses

For other information resources, inventory should include:

Type
Logical location
Information owner
Information classification

Process for periodic asset recertification (*e.g.*, semi-annually, annually) must be documented. Identification of unauthorized or unsupported hardware/ software must be performed, *e.g.*, hardware through asset addition/ removal process from facility; software through scans of end-user workstations.

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 the sanitization of all technology holding electronic information, consistent with the requirements of NIST Standard 800-88 Revision 1, Appendix A ("Guidelines for Media Sanitization"). Notification of lost or misplaced assets, including personally-owned devices, must be made in all cases to internal management and to JPMC where JPMC Data is on or in the lost or misplaced assets. Replacement or risk mitigation strategies must be in place for operating systems, software applications and critical infrastructure components that are nearing end of life.

Personal Asset Controls.

Security controls (*e.g.*, virtual sandbox, remote wipe capability, encryption) must be in place if personal devices are used to perform business transactions or to access JPMC Data or systems where JPMC Data or transactions are stored or processed. Policies must be in place to ensure that Supplier Personnel maintain the security of these devices and must include requirements around timely application of updates and patches, password management, current anti-virus/anti-malware and prevention of "jailbreaking" or "rooting" personal devices.

Procedures must be in place to remove JPMC Data and access rights to systems on which JPMC Data are stored, processed, or transmitted from any device identified as compromised, reported as lost, transferred or sold, and upon termination or transfer of the device's owner to a role in which access is not required.

Prior to use of a personally-owned device as a means of authentication or to access JPMC Data, users must agree to terms and conditions, to include processes for registration of personally-owned devices, as well as for decommissioning devices, including cases in which devices are lost, stolen, or broken.

Procedures to assess the security of updated operating systems and the risks associated with malicious applications must be performed on a periodic and as-needed basis (*e.g.*, upon release of updates to common operating systems); these risks and recommendations must be communicated to device owners.

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 facilities must be restricted through use of access control procedures for authorized users (*e.g.*, badge access, turnstile entry doors and security guards at entrance); all access must be periodically recertified.

Visitor access must be logged in a physical access log and visitors must be escorted through restricted areas in the facility.

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.

Intrusion detection alarms must be installed at egress and ingress points and monitored when triggered.

Monitoring cameras (*e.g.*, CCTVs) must cover sensitive areas within the facility. The monitoring equipment (*e.g.*, CCTV) feed must be monitored either internally or externally by a qualified team. Alerting procedures must be defined and notification performed to qualified Supplier Personnel. Processes for retention and review of security logs (*e.g.*, access and visitor logs, CCTV) must be in place.

External doors to Supplier facilities must be monitored. Supplier Personnel with facility monitoring responsibilities must be trained with regards to their response to security events.

Clean desk/ clear screen policy must be defined. Printed outputs must be secured prior to close of Business Day.

Environmental Control.

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

COMMUNICATION AND CONNECTIVITY.

Supplier must implement robust controls over its communication network to safeguard data, tightly control access to network devices through management approval and subsequent audits, disable remote communications if no business need exists, log and monitor remote access, secure remote access devices, and use strong authentication and encryption to secure communications.

Network Identification.

Network diagram highlighting key internal network components, network boundary components and Demilitarized Zone (DMZ) environment must be documented and current.

A current data flow diagram must exist to identify the paths and environments in which all JPMC Data is or will be collected, accessed, and/or stored. In the event JPMC Data is sent or stored outside the Supplier network, data flow diagram must identify these environments as well.

All JPMC Data must be stored and maintained in a manner that allows for its return and/ or secure destruction upon request from JPMC.

If JPMC contract mandates a segregated physical environment, Supplier must take actions that assure compliance with those contract terms.

Firewalls.

Firewall management process must be documented. All changes to the firewall must be performed via change management processes. Firewall access must be restricted to a small set of super users/ administrators with appropriate approvals.

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).

Network/ Communications Security Policy.

Firewall rules and router Access Control Lists (ACLs) must be reviewed and approved by network administrators. IP addresses in the ACLs must be specific and anonymous connections not allowed.

Technology systems must be configured to provide only essential capabilities; unnecessary or non-secure functions, services, or ports must be disabled. Periodic recertification and authorization of firewall rules must be performed.

Clock Synchronization.

All systems must have their internal clocks set accurately and be synchronized to reliable time sources upon which JPMC and the Supplier have agreed.

Remote Access.

Unauthorized remote connections from devices (*e.g.*, modems) must be disabled as part of standard configuration.

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 (*e.g.*, TPP network) and remote network (*e.g.*, JPMC network) simultaneously (no split tunneling).

Remote sessions must be configured to prevent local storage and local printing of JPMC Data by the remote device.

Dependent third party provider (*i.e.*, subcontractor) remote access must adhere to the same controls and any subcontractor remote access must have a valid business justification.

Mobile Computing.

Mobile computing (where permitted) must be performed over encrypted channels.

Wireless access to the Supplier corporate network must be configured to require authentication. “Guest” wireless that provides access only to the Internet, and not the corporate network, is not impacted by this requirement.

Mobile devices that process or store JPMC Data must be protected by a pin or password, encryption, virtual sandbox, and remote wipe.

Web Access.

Web content filtering must be in place to restrict external webmail, instant messaging, file sharing and other data leak vectors for any Supplier Personnel with direct or indirect access to JPMC Data.

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 must include application, operating system and network infrastructure, including firewall changes. Emergency change management procedure must be specified, including factors leading to emergency change.

The change management policy/ procedure should include the following attributes:

Clearly identified roles and responsibilities (including separation of duties)
Impact or risk analysis of the change request
Testing prior to implementation of change
Security implications review
Authorization and approval (including JPMC approval for key changes affecting Service)
Post-installation validation
Back-out or recovery plans
Management sign-offs
Post-change review and notification (including JPMC for key changes affecting Service)

Emergency Fix Procedures.

Emergency change procedures must have stated roles and responsibilities for request and approval (including JPMC approval for key changes affecting Service). The procedures must include post-change implementation validation and documentation updates.

OPERATIONS.

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

Operational Procedures and Responsibilities.

Operational procedures must be documented in an operations manual and successfully executed. The operations manual should include, as applicable:

Scheduling requirements
Error handling (*e.g.*, transport of data, printing, copies)

Generating and handling special output
Maintenance and troubleshooting of systems
Documented procedures to manage SLAs/ KPIs and the reporting structure for escalations.

Problem Management.

Problem management processes/ procedures must be documented. Problem management lifecycle must include the following discrete steps as applicable:

Identification
Assignment of severity to each problem
Communication
Resolution
Training (if required)
Testing/ validation
Reporting

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.

Logical access policy and corresponding procedures must be documented. The logical access procedures must define the request, approval and access provisioning process. The logical access process must restrict user (local or remote) access based on user job function (role/ profile based, least privilege access) for applications, databases and remote users.

Procedures for onboarding, transferring (*e.g.*, change of role), and offboarding users in a timely manner must be documented, including prompt removal of access from Supplier Personnel whose employment is terminated. If group accounts are used, passwords must be changed upon any user's departure from the group, whether by termination or transfer.

User access recertification to determine access and privileges must be performed periodically.

Procedures for user inactivity threshold leading to account suspension and removal threshold must be documented.

Privileged Access.

Process for management of privileged user accounts (*e.g.* those accounts that have the ability to override system controls) must be defined, documented and maintained.

Responsibility for creation of and access to privileged accounts should be (based on organization size) limited to pre-authorized sets of users (*e.g.* administrators).

A review and governance process must be maintained such that privileged accounts are reviewed periodically to ensure appropriate documentation (*e.g.*, requests, approvals) is in-place prior to account creation, as well as evidence of continuing need.

Procedures for authorizing and tracking administrator passwords (*e.g.*, break glass) must be documented. Administrator passwords must be configured to expire more frequently than regular user passwords; these expiration configurations must be commensurate with the impact of their unauthorized use.

Usage of privileged accounts must be controlled through strong, agreed upon access mechanisms (*e.g.*, multi-factor authentication, electronic password vaulting) monitored, periodically reviewed and follow-up of exceptions documented. Non-personal privileged accounts must track activity such that it is reconcilable back to an individual user for any given usage and, in addition, passwords for such accounts must be reset within 24 hours of completion of use.

Remote control of desktop must be restricted to a specific role (*e.g.*, helpdesk administrators) and remote control must not be permitted unless and until the user gives permission.

Authentication and Authorization.

An approved initialization/ enrollment procedure, including sign-off by an authorized employee of the Supplier on all access requests, must be documented and followed to ensure only authorized individuals are granted appropriate entitlements.

A documented password policy must cover all applicable systems, applications and databases and password best practices must be deployed to protect unauthorized use of passwords.

A secure process must be documented and used to reset passwords.

Authentication credentials, including service account credentials (*e.g.*, functional IDs, impersonation accounts), must be encrypted in storage and must never be hard-coded, written down, stored within information systems in clear text or embedded directly in scripts or applications. Access to password files must be restricted only to system administrators.

If the authentication engine for application fails, the default action must always be to deny access. Failed login messages must only indicate that the login was unsuccessful.

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.

Data transmission control process and procedures to ensure data integrity must be documented.

Check sums and counts must be employed to validate that the data transmitted is the same as data received. For records sent through third party carriers (*e.g.*, UPS, FedEx, US Postal Service), return receipts controls must be employed. Digital certificates (*e.g.*, digital signature, server to server) utilized for ensuring data integrity during transmission must follow a documented process and procedure.

Data Transaction Controls.

Controls to prevent or identify duplicate transactions in financial messages must be documented.

ENCRYPTION.

Encryption policies and procedures must include specifications regarding encryption methods and strength, as well as key management and storage procedures. Encryption must satisfy requirements for protection of data both in transit and at rest.

Encryption Policy.

Data security policy that dictates encryption technical architecture and use must be documented and the encryption method and strength used to protect Confidential Information must be defined.

Encryption Key Management.

Cryptographic key management procedures must be documented and include references to key lifecycle management (including provisioning, distribution, and revocation) and key expiration dates.

Access to encryption keys must be restricted to named administrators.

Encryption keys must be protected in storage. Example methods of acceptable key storage include encrypting keys or storing encryption keys within a hardware security module (HSM).

Data-encrypting keys should not be stored on the same systems that perform encryption/ decryption operations.

Encryption Uses.

JPMC Data must 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 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.

Encryption details of storage and transmission of JPMC Data between Supplier systems must be documented. Approved and dedicated employees of the Supplier must be responsible for encrypting/ decrypting the data, if manual.

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.

Information security incident management policy and procedures must be documented, tested, and reviewed by management no less frequently than annually. The incident management policy and/ or procedures should include the following attributes:

Organizational structure is defined
Response team is identified
Response team availability is documented
Timelines for incident detection and disclosure are documented
Incident process lifecycle is defined including the following discrete steps:

Identification
Assignment of severity to each incident
Communication
Resolution
Training
Testing (check frequency)
Reporting

Incidents must be classified and prioritized.

Incident response procedures must include notification to the JPMC Delivery Manager or another contact listed in the contract.

Escalation/ Notification.

Incident response process must be executed as soon as Supplier is aware of the incident (irrespective of time of day). Incident response team members must be available as required by the contract.

BUSINESS CONTINUITY, DISASTER RECOVERY AND PANDEMIC.

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.

Formal business resiliency plans with comprehensive recovery strategies to address business interruptions of key resources supporting all JPMC services, including those provided by dependent third parties (*e.g.*, subcontractors), must be documented, tested and reviewed. The recovery plan strategy must have an acceptable alternative work location in place to ensure service level commitments are met.

Technology Recovery.

Technology Recovery Plans with comprehensive strategies to minimize service interruptions and ensure recovery of systems infrastructure, databases, applications, etc., must be documented, tested, reviewed and reapproved no less frequently than annually.

Pandemic Assessment.

Formal pandemic plans must be in place with comprehensive strategies to minimize service interruptions and ensure support of technology-related services within agreed upon time frames.

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.

Access to non-corporate/ personal email solutions must be restricted (*e.g.*, port restrictions, firewall rules or web filtering products). Emails containing Highly Confidential Information, Confidential Information, or Personal Information must be encrypted if leaving the Supplier network; preventive controls (*e.g.*, proxy rules, filtering products) must be in place to prevent Highly Confidential Information, Confidential Information, and Personal Information from being sent externally through email without encryption. Preventive and detective controls must block malicious e-mails/ attachments. Policy must prohibit auto-forwarding of emails. The encryption mechanism may be automated (*e.g.*, Transport Layer Security (TLS)) or manual (*e.g.*, Winzip encryption). If Supplier is sending emails on behalf of JPMC, additional controls must be implemented to restrict spam and phishing emails (*e.g.*, Domain Keys Identified Mail (DKIM), Sender Policy Framework (SPF)).

Authorized Instant Messaging (IM) Systems.

Access to external IM must be prohibited from Supplier's network. If internal IM is used, specific policies (*e.g.*, acceptable use policy) restrict the conduct of JPMC business over internal IM. JPMC Data must only be shared with users with a "need-to-know".

BACK-UP AND OFFSITE STORAGE.

Supplier must have a defined back-up policy and associated procedures for performing back-up of JPMC Data in a scheduled and timely manner. Effective controls must be established to safeguard backed-up data (on-site and off-site). Supplier must also ensure that JPMC Data is securely transferred or transported to and from back-up locations and conduct periodic tests to ensure that data can be safely recovered from backup devices.

Back-up and Redundancy Processes.

Back-up and redundancy processes covering both catastrophic and partial recovery requirements and off-site storage procedures must be documented. Procedures must refer to retention periods, encompass ability to fully restore applications and operating systems, and include that such back-ups support Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements. Periodic testing of successful restoration from redundancy systems and backup media must be demonstrated. The on-site staging area must have documented and demonstrated environmental controls (*e.g.*, humidity, temperature).

Back-up Media Destruction.

Procedures must be defined to instruct Supplier Personnel on the proper methods of backup media destruction. Back-up media destructed by a third party must have documented procedures (*e.g.*, certificate of destruction) for destruction confirmation. Evidence of off-site media destruction, conforming to JPMC requirements for secure deletion, must be obtained.

Offsite Storage.

Physical security plan/ policy for the offsite facility must be documented. Access controls must be enforced at entry points and in storage rooms. Access to the off-site facility must be restricted and there must be an approval process to obtain access. Electronic transmission of data to off-site location

must be encrypted. Back-up storage devices (*e.g.*, flash drives, CD, DVD, USB devices, back-up tapes) must be encrypted. Secure transportation procedures (*e.g.*, inventory tracking, signed checklists) of media to and from off-site locations must be defined.

MEDIA AND VITAL RECORDS.

Policies for handling and storing data must be in place to ensure safe, secure disposal of media and secure media in transit or transmission to and from Supplier.

Handling and Storage.

Electronic or paper records movement procedures must be documented. The procedures must include safe storage and secure transportation of electronic or paper records from source to destination, including any transit stops.

Record Control.

Paper records containing JPMC Data must be stored in secure bins. Access to bins must be limited to select Supplier Personnel only. Access recertification must be performed periodically (*e.g.*, quarterly, semi-annually, annually) to validate users with access to secure bins. Labeling must not associate bins or boxes directly with JPMC. 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. If a third party is used for secure shredding/ destruction, a services contract with confidentiality and security terms must be in place.

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 media/ vital records during transportation (*e.g.*, encryption of media, use of lockboxes with dual key system, securing of boxes during transport). Emergency procedures must be documented and an incident must be reported if any media/ records are lost/ unrecoverable during transport.

Warehouse Security.

Procedures for securely managing and storing physical media and paper records must be documented. Chain of custody and ownership process must be defined when the boxes are transferred between the organization and JPMC. Procedures to determine destruction dates of specific boxes must be in place. Tools or processes must be in place for periodic inventory validation. An independent audit to review operational processes must be performed.

THIRD PARTY RELATIONSHIPS.

All dependent third party providers (*i.e.*, subcontractors to the Supplier) must be identified, assessed, managed and monitored to ensure the confidentiality, integrity, and availability of any JPMC that they share, process, or transmit.

Selection and Oversight.

Supplier must have a process to identify all dependent third party providers (subcontractors) providing services to Supplier. An appropriate risk assessment to ensure that each third party provider can provide a suitable control environment associated with the services they provide must be performed prior to selection and on an on-going basis and monitoring mechanisms must be in place.

Lifecycle Management.

Supplier must have a process to establish appropriate contracts for all dependent third party providers prior to services being initiated, ensuring that appropriate security language is incorporated into all agreements with dependent third party providers.

Services must be transferable to an alternate third party provider if needed. A procedure for disengaging with third party providers must be documented, to include assurances that any JPMC Data shared has been recovered or securely destroyed and access terminated.

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 configuration documentation related to the Services provided to JPMC must be developed, maintained, and under revision control. Minimum Security Baselines (MSB) must be established and security hardening demonstrated. Procedures are to 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.

Documented operating system versions implemented for environments associated with the Services provided to JPMC. Multiple simultaneous logins to the environment must not be allowed for any single administrator. Unsupported operating systems must not be used.

Desktop Controls.

End-users must not be permitted to be local administrators to the workstations. Key desktop security settings (*e.g.*, screen saver, anti-virus) must be unalterable by end-users. Policy must include language preventing Supplier Personnel from storing any Highly Confidential Information, Confidential Information, or Personal Information on their desktops. Desktop peripheral devices must not allow ability to write from desktop to device (*e.g.*, CD, DVD, USB drives). Where writing is permitted, this must be on exception basis and business justification documented.

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 to mitigate security incidents (*e.g.*, zero-day or denial of service threats).

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 Highly Confidential Information, Confidential Information or Personal Information, the application must implement multi-factor authentication.

An additional, network-level restriction must be in place to secure JPMC/ corporate access to third party applications that handle Highly Confidential Information, Confidential Information, or Personal Information.

Software Development Life Cycle.

A Software Development Life Cycle (SDLC) methodology must be documented and include version control, release management procedures, and 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 adequate training regarding JPMorgan Chase & Co. Supplier Code of Conduct, compliance with applicable Laws, the proper provision of Services and other Deliverables and privacy training. The privacy training should include following:

Privacy information classification

Information on legal, regulatory and contractual responsibilities for privacy

Information on consequences (including penalties) for violations of applicable privacy Law, contractual obligations or company privacy program

Information on email and Internet usage guidelines regarding privacy and monitoring

Information on Supplier Personnel and Supplier equipment monitoring policies for privacy

Protocols used by the agents to authenticate the identity of the customer (*e.g.*, asking questions like mother's maiden name, DOB or security questions as selected by the customer) must be defined. Documents that contain Highly Confidential Information, Confidential Information, or Personal Information must remain in locked containers. Any alternate work arrangements (*e.g.*, work at home (if any)) must restrict the ability of customer service agents to copy data, transfer to external e-mails or enable ability to store it on web portals. All voice recordings must be performed over encrypted channels.

VULNERABILITY MONITORING.

Supplier must continuously gather and analyze information regarding existing and emerging threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security

controls. Monitoring controls must include related policy and procedure, virus and malicious code, intrusion detection, and event and state monitoring. Related logging must provide an effective control to highlight and investigate security events.

Vulnerability Policy and Procedure.

Vulnerability scans, including penetration tests, must be performed against internal and external networks and applications, both periodically and prior to system provisioning, to include both authenticated and unauthenticated vulnerability scans for all systems that process, store or transmit JPMC Data. The tests must be performed by a reputable external organization. Environments containing JPMC Data must be covered as part of the scope of the tests. All issues rated as critical or high risk must be communicated to management and remediated within appropriate timelines. These timelines must be communicated to JPMC and supported by policy.

Anti-virus and Malicious Code.

Servers, workstations and internet gateway devices must be updated periodically with latest anti-virus definitions. Defined procedures must highlight the anti-virus updates. Anti-virus tools must be configured to run weekly scans, virus detection, real time file write activity and signature files updates. Laptops and remote users must be covered under virus protection. Procedures to detect and remove any unauthorized or unsupported (*e.g.*, freeware) applications must be documented.

Intrusion Detection Administration.

Network and host-based intrusion detection tools must be deployed where Highly Confidential Information, Confidential Information, or Personal Information is stored, processed or accessed. Events generated by detection (or prevention) sensors must be configured for logging in centralized systems and event correlation tools should be used to analyze events and to identify potential incidents. Policies must be updated as required to respond to specific threats, or based on intruder profiles and patterns. Intrusion detection tools must perform real time scanning, signatures must be updated in a timely manner and automated alerting to appropriate individuals must be defined as part of intrusion detection systems.

Alert events should include following attributes:

Unique identifier
Date
Time
Priority level identifier
Source IP address
Destination IP address
Event description
Notification sent to appropriate teams
Event status

Security Event Monitoring.

Security events must be logged and transferred to a secure log aggregator solution for monitoring of exploits; events must be addressed and resolved in a timely manner, with actions taken documented. Network components, workstations, applications and any monitoring tools must be enabled to detect anomalous activity (*e.g.*, user, network, or server activity). Organizational responsibility for responding to events must be defined. Configuration checking tools or other logs must be utilized that record critical system configuration changes. The log permission must restrict alteration by administrators or any user.

Retention schedule for various logs must be defined and adhered to. Intrusion Detection System (IDS) effectiveness must be tested periodically.

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 being provided.

Regulatory Compliance.

Supplier must have processes for researching, evaluating, and complying with all national and other Laws and regulations that are relevant to the business, process, or activity being undertaken in the particular jurisdiction(s). Additionally, Supplier must be compliant with any applicable Laws for JPMC Data that is stored, managed, shared or accessed by Supplier.

Data retention and destruction procedures must be documented and followed to ensure that JPMC data is stored for required time periods and securely destroyed per scheduled expiration.

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.

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

Website.

Procedures around cookie activity must be compliant with the applicable global Laws (*e.g.*, specific EU Laws around requiring client consent prior to placing cookie on client workstation, providing information on cookie purpose).

System Development.

Privacy impact assessment must be conducted during the requirements/ design 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 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. Procedures to re-validate Personal Information on a recurring basis must be defined.

CLOUD TECHNOLOGY.

Adequate safeguards must ensure the confidentiality, integrity, and availability of JPMC Data stored, processed or transmitted using Cloud Technology. "**Cloud Technology**" is defined as any technology in which cloud computing, according to NIST Special Publication 800-145 ("Definition of Cloud Computing"), is in scope.

Minimum Control Requirements.

All of these Supplier Minimum Control Requirements apply to any use of Cloud Technology to store, process or transmit JPMC Data. In addition, the following specific requirements must be in place for Cloud Technology, including services provided by a dependent third party (subcontractor).

Pre-Approval.

Supplier must inform JPMC of and obtain JPMC's prior written approval of Cloud Technology before it is used to store, process or transmit JPMC Data.

All Cloud Technology providers must maintain annual compliance with at least the following certification(s): SOC2 Type 2, ISO/IEC 27001, 27002, 27017, and 27018; all services and locations used to store, process, or transmit JPMC Data must be included.

Supply Chain.

A trusted supply chain must be used for procuring hardware and software used to store, process or transmit JPMC Data.

Data Loss Prevention.

Where permitted by law, JPMC Highly Confidential Information, Confidential Information and Personal Information must be subject to Data Loss Prevention (DLP) filtering which must be deployed to all points of information egress, including host-based solutions, at all points of information egress from physical and virtualized systems (hosts and guests). Encrypted egress communications must be decrypted for inspection.

Environments with external or internet-facing components must have perimeter security solutions including firewalls, intrusion detection/prevention, content filtering proxies and DLP deployed at all points of egress.

Systems processing unencrypted Highly Confidential Information must be hosted on dedicated physical hardware to ensure isolation from other tenants.

Encryption and Key Management.

Highly Confidential Information, Confidential Information and Personal Information must be encrypted while in transit over any network and wherever stored.

Applications that store, process, or exchange Highly Confidential Information should be encrypted at the application layer.

Key management systems must be used for generation, storage and revocation of cryptographic keys; processes for management of key material, such as key ceremonies, must be documented. Data encrypting keys, Supplier-managed keys, and any unencrypted keys must be generated and stored on, and revoked by, Highly-available FIPS 140-2 Level 2 certified physical hardware security modules (HSMs) with tamper detection and response mechanisms that meet Level 3 Physical Security requirements and must not be stored on persistent storage devices. Data encrypting keys must be further encrypted using additional key and must be encrypted in storage. Cloud-hosted key management systems must make allowances for Supplier-managed keys to be imported, rotated periodically, and revoked as needed.

File Integrity Monitoring.

All systems that store, process, or transmit Highly Confidential Information, Confidential Information, and Personal Information must use host-based intrusion detection (or prevention) systems capable of performing file integrity monitoring for critical content files, system files, and configurations, and alerting when attempts to modify the system are detected. The host-based Intrusion Detection System/Intrusion Prevention System must be configured to perform file integrity comparisons to known good versions on a regular schedule.

Firewalls and Network Security.

Security domains must be established and controls must be implemented to ensure that only approved and authorized communications can pass from one domain to another. Every security domain must have a defined purpose and documented controls. All communications between security domains must be authorized and controlled based on least privilege/capability and via an authorized and approved security gateway. The default access between security domains must be "None" (*e.g.*, "Deny All"). All firewall devices must be evaluated for compliance with this requirement at least quarterly.

Isolated network segments must be used for out-of-band management of physical systems and virtualization operations (*e.g.*, virtual machine migrations).

Logging and Monitoring.

Infrastructure devices must be configured with logging and auditing features to monitor system health and allow forensic and security monitoring activities that track the following:

Application start/stop times
System boot/restart times
System configuration changes
Abnormal system events
Critical file changes
Utilization of resources
Remote access
Security control mechanisms
Capacity
Overloads

Outbound communications for unusual or unauthorized activities including the presence of malware (*e.g.*, malicious code, spyware, adware)

Periods of system unavailability

Security configuration management solutions must be used for ongoing monitoring of changes against baseline security standards. Annual reviews must be in place to ensure that baseline configurations are current against industry standards.

Exporting of logs to external providers must be disclosed to JPMC.

Perimeter Security.

All network services must pass through a security access gateway (firewall, web application firewall, reverse proxy, etc.) allowing only the specific hosts, protocols and services required to provide the functionality.

E-Discovery and Cloud Forensics.

The ability must be established to identify, preserve, collection, produce, dispose of, or deliver electronically stored information to JPMC upon request and in a timely manner.

A process must be established for managing information security incidents that may require forensic investigations. The process must include forensic investigation procedures that define preservation and isolation of evidence and chain of custody processes that are compliant with industry best practices for the recovery of admissible evidence. Evidence must be collected with the intention of possible legal action.

Vulnerability Management.

A network vulnerability assessment process must be implemented to assess all servers and infrastructure devices that form the network itself at least monthly. Systems must be evaluated at least bi-weekly to ensure timeliness of security updates.

BUSINESS PRACTICES.

Adequate 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 for management oversight of Supplier business operations, assurance of processes for responding to customer complaints, handling of non-public information, signing authority, code of conduct, change control, etc., must be documented.

Fraud.

A fraud detection, prevention and mitigation program, processes and procedures for monitoring actual and suspected instances of fraud, and specific notification and communication, internally and to JPMC, must be in place.