INTRODUCTION

These Minimum Control Requirements (“Minimum Control Requirements”) are stated in a general manner, and JPMC recognizes that there may be multiple approaches to accomplish a particular Minimum Control Requirement. These Minimum Control Requirements are not intended to replace Supplier’s standard policies and procedures but are intended to address the minimum controls that the Supplier must have in place as part of Supplier’s standard policies and procedures. Supplier must document in reasonable detail how a particular control meets the stated Minimum Control Requirement. All Minimum Control Requirements apply to Supplier’s subcontractors that have, process, or otherwise have access to JPMC Confidential Information or JPMC Systems. The term “should” in these Minimum Control Requirements means that Supplier will use commercially reasonable efforts to accomplish the stated Minimum Control Requirement. Any required policies, procedures, or processes mentioned in these Minimum Control Requirements must be documented, reviewed, and approved, with management oversight, on a periodic basis. 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. Supplier must comply with and have processes for researching, evaluating, and complying with, all Laws in the applicable jurisdiction(s).

As used in these Minimum Control Requirements, 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.

TECHNOLOGY GOVERNANCE, RISK, AND COMPLIANCE

- The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.
- A risk assessment must be performed annually to verify the implementation of controls that protect business operations and JPMC Confidential Information.
- A documented set of security policies and procedures must govern the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of information, assets, and associated services.
- A risk-based exception management process must be in place for prioritization and remediation or risk acceptance of controls that have not been adopted or implemented.
- Security policies and responsibilities must be communicated and socialized within the organization to Supplier Personnel.

PHYSICAL AND ENVIRONMENTAL SECURITY

- Physical and environmental security processes and procedures must be in place for facilities with access or storage of JPMC Confidential Information.
- Personnel should be granted access to areas of the facility based on the principle of least privilege.
- Physical access to facilities must be restricted, with all access recertified on a regular schedule.
• Detective monitoring controls (e.g. CCTV) must be in place with a defined retention period.
• Addition or removal of assets from the facility must be documented and tracked.
• Supplier must obtain approval from JPMC prior to allowing assets with JPMC Confidential Information to be removed from the facility.
• Facilities 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.

DATA PROTECTION
• JPMC Confidential Information must be protected and encrypted in transit and at rest (including in backup) as well as when shared with Supplier’s subcontractors.
• Authentication credentials must be encrypted in transit and at rest.
• Data protection policy must cover data classifications, encryption use, key and certificate lifecycle management, permitted cryptographic algorithms and associated key lengths, message authentication, hash functions, digital signatures, random number generation and be reviewed against industry standards on a regular basis.

IDENTITY AND ACCESS MANAGEMENT
• Documented logical access policies and procedures must support role-based, “need-to-know” access based on the principle of least privilege, and ensure segregation of duties during the approval and provisioning process
• Logical access policies must cover remote access, access request approval prior to access provisioning and periodic recertification of access.
• Each account provisioned must be uniquely identified.
• Management of privileged user accounts to include service accounts, must follow a documented process and be restricted.
• A documented authentication and authorization policy must cover all applicable systems and networks and include password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized.
• The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change of role.
• Multi-factor authentication must be implemented for:
  • The initiation of any privileged access session and/or retrieval of credentials with privileged access
  • External connectivity to the JPMC network
  • Applications directly accessible from the internet

SECURITY CONFIGURATION
• Supplier must implement controls over its communication network to safeguard data.
• A network diagram, to include all devices, as well as a data flow diagram must be kept current.
• Network devices must have internal clocks synchronized to reliable time sources.
• Standard security configurations, using the principles of least functionality/privileges, must be established and security hardening demonstrated.
• Information systems must be deployed with appropriate security configurations and reviewed periodically for compliance with Supplier’s security policies and standards.
Drift or deviation from hardened builds/security configuration baselines must be identified, reported, and remediated.

The production network must be isolated from the development and test environments.

Malware protection mechanisms must exist to detect and/or prevent against malware and other threats.

Malware protection mechanisms must be configured to perform real-time or scheduled scans of systems, and alert when malware is discovered.

All devices and malware protection mechanisms must be kept up-to-date with latest anti-virus software and definitions.

Network and host-based intrusion detection and intrusion prevention systems (IDS and IPS) must be deployed with generated events fed into centralized systems for analysis.

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

Supplier must have policies, procedures, and controls that ensure proper control of an electronic mail and/or instant messaging system that displays and/or contains JPMC information.

Access to non-corporate/personal email and instant messaging solutions must be restricted.

Preventive controls must block malicious messages and attachments as well as prevent auto-forwarding of emails.

SECURITY OPERATIONS

Supplier Personnel must be trained to identify and report suspected security weaknesses and events/incidents.

Data Loss Prevention (DLP) technology, processes, and/or solutions must be deployed to protect against the exfiltration of JPMC information.

Supplier must have a security event/incident response policy and procedure.

Retention schedule for various logs must be defined and followed.

Security event logs from information systems must be collected, centrally managed, analyzed, and correlated for the purpose of detecting anomalous behavior that may indicate malicious events/incidents.

A fraud and threat 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 established.

Supplier should have a procedure for conducting digital forensics including data collection, data/evidence preservation for future analysis, analysis, reporting of findings, and closure.

A process should be in place to conduct attack simulations on a segregated environment including social engineering exercises (e.g., phishing), red teaming, and tabletop exercises with appropriate reporting, remediation/acceptance, and tracking of findings.

VULNERABILITY MANAGEMENT

Supplier must continuously gather vulnerability intelligence data in light of existing and emerging threats as well as actual attacks that may impact their systems.

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 Confidential Information.

Any critical vulnerabilities identified during vulnerability scans or penetration testing must be prioritized and remediated within a well-defined timeframe commensurate with the vulnerability risk.
PRIVACY
- Supplier must implement effective controls to ensure appropriate processing and protection of Personal Information.
- Social Security Numbers or other national identifiers must not be utilized as User IDs for logon to applications.
- Privacy impact assessment must be conducted during the requirements phase of system development to evaluate the impact to Personal Information and review the scope of monitoring.
- The privacy impact assessment must not conflict with any applicable local and other Laws.
- Supplier must have procedures for obtaining consent from users to collect Personal Information, giving users the ability to access, correct, opt-out, delete, restrict, make portable, or object to the processing of Personal Information.
- A privacy notice or information banner must be in place, requiring acknowledgement 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.

TECHNOLOGY DEVELOPMENT
System Development Life Cycle (SDLC)
- Suppliers must operate an established System Development Life Cycle (SDLC) process.
- The SDLC must establish the control requirements for software development that are applicable to any software and development framework, or model, used.
- The SDLC must include a Secure Design Review, and preventive and detective controls to identify vulnerabilities and design flaws.
- A procedure must be documented and enforced to remediate vulnerabilities and design flaws prior to production using a risk-based approach.

Third-Party Software
- Third party and open source code or software used must be appropriately licensed, inventoried, and where commercially licensed, be fully supported by the vendor.

TECHNOLOGY OPERATIONS
- Documented operational procedures must ensure correct and secure operation of Supplier’s assets.
- Operational procedures must include monitoring of capacity, performance, service level agreements, and key performance indicators.
- Supplier must have policies and procedures for back-up of JPMC Confidential Information.
- Media must be protected in storage including offsite storage.
- Processes enabling full restoration of all systems, applications, and data must be established.
- Procedures must be in place to destroy JPMC Confidential Information prior to disposal or reuse of equipment used for logical and physical storage.
- Retention procedures for all records must be in accordance with JPMC record retention requirements.
- The ability to write to portable electronic media must be limited to documented exceptions.
- 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 pre- and post-implementation to
ensure that expected changes and their desired result are accurate.

- An emergency change management procedure must be specified, including factors leading to emergency change.
- Any changes materially affecting JPMC services must be communicated to JPMC prior to implementation.

THIRD PARTY RELATIONSHIPS

- Supplier’s subcontractors must be identified, assessed, managed, and monitored in accordance with the terms of the Master Agreement with JPMC, including compliance with JPMC’s Minimum Control Requirements applicable to any such services.

RECORDS MANAGEMENT

- In the event that Supplier is maintaining records on behalf of JPMC, Supplier must maintain and validate with JPMC (at least annually) a complete and accurate inventory of all types of JPMC records with the following attributes for each record:
  - Ownership
  - Record Type
  - Description
  - Retention Requirements
  - Location
- Records created, received, stored and/or retained must follow a defined, regularly-reviewed procedure that manages the record throughout its lifecycle.
- Information must be retained as per the requirements provided by JPMC via the Service Records Exhibit, if applicable.
- For any information that is held according to Supplier retention obligations must be disposed of or destroyed in accordance with the relevant contract(s).

DATA

- Suppliers and dependent subcontractors who receive, send, transmit, store, create, generate, collect, control, process or have access to JPMC Confidential Information, must do so solely to provide services to JPMC.
- Controls must ensure that any data stored, received, controlled, or otherwise accessed (including any data provided to JPMC) is accurate and reliable.
- Controls must be in place to ensure the integrity of JPMC Confidential Information when transmitted and to validate that the same information is received.
- Policies and processes covering data use and restrictions, including for JPMC Confidential Information shared with dependent suppliers, must be established.
- Supplier must be able to demonstrate data origination.

TECHNOLOGY ASSET MANAGEMENT

- Supplier must have a sufficient technology asset registration policy and procedure including unique identifiers for all assets, appropriate classification, asset ownership, asset location, and proper licensing, legal, regulatory, contractual, or support requirements.
- Supplier must maintain an appropriate technology asset inventory governance structure to include recorded changes to asset records, sufficient back up of asset registers, annual integrity validation of the asset registers, asset ownership recertification, timely asset register updates when asset records are altered, regular license audits of assets, and remediation of unauthorized
assets.

- A technology asset lifecycle management program must be put in place that includes accurate lifecycle status of all assets, identification of assets not in compliance with the lifecycle management policy, and notification to asset owners of non-compliant assets.
- A technology asset provisioning and disposal program must be in place to include only procuring technology assets from appropriately sourced suppliers and disposing of/removing/deleting all technology assets in a secure manner when they reach end of life.

INCIDENT AND EVENT MANAGEMENT

- Documented incident, event, or problem management procedures must include systematic tracking of problems from discovery to resolution.
- Supplier's event management policy and procedures must account for the identification of anomalous events that indicate deviation from the norm beyond a defined threshold.
- Supplier must also process and analyze events to determine if action is required, and to engage JPMC via the Incident Management process.
- The incident management policy and procedures must include the responsibilities of Supplier Personnel and identification of parties to be notified in case of an information security event/incident.
- The Supplier’s incident management policy and procedures must also include prioritization, roles and responsibilities, internal escalation, notification to JPMC, tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity.

BUSINESS RESILIENCY

- Supplier must have formal, comprehensive business resiliency plans to enable timely, orderly, and sustainable recovery of business, support processes, operations and technology components within an agreed upon time frame.
- Supplier must perform a Business Impact Analysis (BIA) to determine their business resilience process criticality and to define a Recovery Time Objective (RTO) for all processes they utilize to support the services or functions being performed for JPMC.
- Business resiliency plans must identify key resources and address business interruptions of those resources supporting all JPMC services, including those provided by Supplier’s subcontractors
- Resiliency plans must have acceptable recovery capabilities in place to adequately address the following disruption scenarios to meet JPMC recovery time objectives and service level applications:
  - Loss of Staff
  - Loss of Site
  - Loss of Application (Application DR is Available)
  - Loss of a Third Party’s Vendors (Vendor’s Recovery is Available)
- The resiliency plans must have acceptable alternative work locations/strategies in place to ensure service level commitments are met.
- Resiliency plans must be tested on a regular basis and noted deficiencies/failures should be addressed timely.
- Any change that could affect the recovery of the process or infrastructure, may involve, but is not limited to, changes in business strategy, service, process, assets, and regulatory / legal obligations, resulting in significant changes to the BIA or Plans must require a new test of the recovery plans affected by the significant change.
TECHNOLOGY RESILIENCY

- Supplier must have formal technology recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to services provided to JPMC or resources supporting those services.
- Supplier recovery plans must identify Supplier’s own critical processes, supporting assets, dependencies, critical points of failure, recovery staff personnel and recovery capabilities to address business interruptions to processes that support JPMC services.
- Technology recovery plans (including those specific to cyber-attack scenarios) must be established to limit service interruption.
- Technology recovery capability must include the ability to recover from a destructive Cyber event in which:
  - the primary (production) systems have been compromised or destroyed, and
  - both the primary and secondary (DR) systems have been compromised or destroyed.
- Technology recovery plans must ensure timely, orderly, and sustainable recovery of technology components within a defined recovery time objective.
- Recovery plans must also include Supplier’s subcontractors, including cloud service providers.
- Recovery plans must be tested on a regular basis using sufficient testing which includes testing long term strategies.
- Supplier must have a crisis management framework including initial notification to JPMC and ongoing contact with JPMC during an incident impacting the services being performed by Supplier.
- JPMC Confidential Information must be available upon request, in an industry standard format, so as to ensure portability and interoperability.
- Any change that could affect the recovery of the process or infrastructure, including (but not limited to) significant changes in personnel, organizational structure, technology, location, or strategy must require a new test of the technology recovery plans affected by the significant change.

ORGANIZATIONAL SECURITY

- Supplier personnel assigned to JPMC Services must be provided a copy of the JPMC Supplier Code of Conduct
- Supplier personnel must notify JPMC in the event of any potential, perceived or actual conflicts of interest between Supplier personnel’s outside business activities and personal relationships and JPMC business, clients, or employees.
- Supplier must provide training to Supplier Personnel on job responsibilities, and ensure Supplier personnel complete any assigned JPMC training.
- Supplier must conduct a formal, tracked performance and appraisal review process of its personnel.
- Supplier must maintain current organizational charts representing key management responsibilities for services provided to JPMC, including all related services provided by dependent third party suppliers.
- Supplier must perform appropriate background checks on its personnel.
- Supplier must ensure its personnel have agreed to non-disclosure or confidentiality obligations before assigning to JPMC services and giving access to JPMC systems and information.
CUSTOMER CONTACT

- If it is providing customer service (e.g., customer contact agents and related operations), Supplier must have defined and enforced operational procedures that ensure the confidentiality, integrity and availability of JPMC Confidential Information, as well as the provision of services and other deliverables in compliance with the relevant contract(s).
- Supplier must maintain and implement effective procedures for the authentication of each customer, including as may be directed by JPMC.
- Customer contact agents must receive privacy training (e.g., addressing proper handling of individual personal information in light of privacy laws and regulations), as may be specified in the relevant contract(s) or as directed by JPMC.
- Any complaints received regarding JPMC or any services provided for or on behalf of JPMC, must be reported to JPMC as may be specified in the relevant contract(s) or as directed by JPMC.