JPMorgan Chase & Co. Minimum Control Requirements

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 Supplier must have in place as part of Supplier's standard policies and procedures. As technology trends change, Supplier should ensure they are adhering to these Minimum Control Requirements as it relates to any new and emerging technologies. 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, responsibilities and obligations, including cybersecurity and technology controls awareness training, 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 to, 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, intrusion alarm system) must be in place with a defined retention period. CCTV must have a defined retention period.
- 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

- Suppliers and dependent subcontractors must have sufficient information classification for the purpose of data protection.
- All JPMC Highly Confidential and Confidential Information must be protected and encrypted by strong cryptography in transit and at rest (including in backup)
- All authentication credentials (e.g., passwords, personal identification numbers, challenge answers) must be encrypted in transit and at rest.
- The data protection policy must cover encryption, key and certificate lifecycle management, permitted cryptographic algorithms and associated key lengths, message authentication, hash functions, digital signatures, and random number generation.
- The data protection policy must be reviewed against industry standards on a regular basis.
- Appropriate technical configuration(s) for encryption must be implemented for portable media.

IDENTITY AND ACCESS MANAGEMENT

- Documented logical access policies and procedures, including those that support attribute-based or role-based access, must ensure user access is commiserate with a user's job responsibility and must support "need-to-know" access based on the principle of least privilege, and ensure segregation of duties and the prevention of toxic combinations 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.
- A privileged account management process and control policy must be documented, covering privileged (system or elevated user) and non-privileged (personal) account separation, privileged account discovery, safeguarding of privileged accounts, post activity usage review requirements, and assurance that non-interactive privileged accounts (e.g., system accounts) are not used interactively by end users
- A documented authentication and authorization policy must cover all applicable systems and networks and must include provisioning complexity and reset requirements for passwords and other secrets in addition to 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 interactive privileged access session.
    - External connectivity to the JPMC network.
    - Applications directly accessible from the internet.
    - The administration of application access.
- Federated identity management must be implemented for JPMC access to Supplier systems via industry standard security assertion markup language (SAML).

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.
- 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/or intrusion prevention systems must be deployed with generated events fed into centralized systems for analysis.
- 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.
- 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, suspicious activity, and security events or incidents.
- Data loss prevention (DLP) technology, processes, and/or solutions must be deployed to protect against the exfiltration of JPMC information through all channels of communication.
- 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 including social engineering exercises (e.g., phishing), red teaming, and tabletop exercises with appropriate reporting, remediation/acceptance, and tracking of findings.
- Access to non-corporate/personal email and instant messaging solutions must be restricted.

VULNERABILITYMANAGEMENT

- Supplier must include as part of their vulnerability management program, the receipt of vulnerability related security alerts and intelligence from external and internal sources in order to identify and monitor for vulnerabilities in their environment.
- 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 through intelligence gathering, 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.
- Supplier's processing of Personal Information must not conflict with any applicable Laws.
- If Supplier will collect Personal Information from individuals on behalf of JPMC Supplier must have procedures for making available a JPMC privacy notice and/or obtaining prior, informed consent from individuals.
- Supplier must have procedures in place to provide complete and timely responses to JPMC, and take actions necessary to honor individual rights requests, including but not limited to requests to access, correct, opt-out, delete, restrict, make portable, or object to the processing of Personal Information.
- Supplier must have documented procedures for collecting, processing and disclosing Personal Information including any restrictions imposed by law, contractual arrangements and/or JPMC privacy policies.
- Supplier must have a process to notify JPMC of any event that may or will impact that confidentiality, integrity or availability of personal information, including unauthorized or suspicious intrusion into systems storing such personal information.

TECHNOLOGY DEVELOPMENT

System Development Life Cycle (SDLC)

- Suppliers must operate an established System Development Life Cycle (SDLC) process.
- SDLC governance must be established, documented, and enforced to identify and remediate defects, vulnerabilities, coding errors, and design flaws prior to production using a risk-based approach and in line with industry standards and frameworks.
- The SDLC must establish the control requirements for software development that are applicable to any software and development framework or model used.
- Functional and non-functional requirements must be continuously identified and implemented to prevent software from becoming obsolete.

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

- Suppliers must have a Capacity Management process documented that includes monitoring of capacity headroom and performance to ensure availability; this process must be reviewed on an annual basis.
- Suppliers must have a Change Management process documented that outlines the planning, approvals procedure, testing, implementation, post validation, emergency change procedure, and retention of logs for audit purposes; this process must be reviewed on an annual basis. Any changes materially affecting JPMC services must be communicated to JPMC prior to implementation.

- Suppliers must have a Technology Maintenance process documented for infrastructure assets that covers patch compliance and hygiene activities; this process must be reviewed on an annual basis.

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 and Supplier Code of Conduct applicable to any such services.

DATA MANAGEMENT

- Suppliers and dependent subcontractors that regularly provide data to JPMC must maintain and provide a data dictionary or equivalent data classification artifact, including any agreed-upon metadata for data provided to JPMC.
- Supplier and dependent subcontractors must have controls in place to allow JPMC to validate that a complete set of data has been received in an agreed-upon format. Supplier must have a process for notifying JPMC of errors for data transmitted to or from JPMC in accordance with quality specifications for the accuracy, timeliness, and completeness of the data.
- All JPMC data provided to and stored by Supplier and dependent subcontractors must be stored and retained in a manner that:
    - Includes the capability to access and, where required, retrieve the data as needed.
    - Avoids loss due to media decay or technology obsolescence.
    - Is stored in secure locations that provides reasonable safeguards against hazards, that include, but are not limited to, the following:
        - Ordinary hazards, such as power loss, minor fire, water, mildew, rodents, and insects
        - Man-made hazards, such as theft, accidental loss, sabotage, and commercial espionage
        - Disasters, such as fire, flood, earthquakes, hurricanes, and explosions
- Is in accordance with applicable laws, regulations, and contractual obligations.
- Protects the data from unauthorized access/alteration.
- If Supplier or dependent subcontractor hosts data on behalf of JPMC, Supplier and dependent subcontractors must maintain and validate with JPMC (at least annually) a complete and accurate inventory of JPMC data with the following attributes:
    - Classification
    - Retention/Destruction Requirements (and execution of those requirements)
    - Location
- Suppliers and dependent subcontractors who receive, provide, transmit, store, create, generate, collect, control, process, or have access to JPMC Confidential Information must do so solely to provide services to JPMC.
- Supplier and dependent subcontractors must be able to maintain data provenance.

INFORMATION & TECHNOLOGY ASSET MANAGEMENT

- Supplier must have a sufficient technology asset registration policy and procedure, including unique identifiers for all assets, appropriate classification, asset ownership, and asset location, including proper licensing and meeting all 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, procedures addressing lost/stolen 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.
- Supplier must ensure assets are transported in a secure manner.

INCIDENT AND EVENT MANAGEMENT

- Suppliers must have an Event Management process documented that ensures anomalous events are monitored, detected, analyzed and actioned for all production and disaster recovery applications and infrastructure. This process must be reviewed on an annual basis.
- Suppliers must have a Problem Management process documented that ensures root cause analysis is performed for all incidents impacting production and disaster recovery applications and infrastructure, with permanent fixes implemented and reoccurrences of incidents minimized; this process must be reviewed on an annual basis.
- Suppliers must have an Incident Management process documented that includes incident tracking, reporting, classification, prioritization, internal escalation, remediation, and preservation of data for all incidents impacting production and disaster recovery applications and infrastructure; this process must be reviewed on an annual basis. Supplier must notify and engage JPMC in compliance with the contract or applicable local regulations, if services to JPMC or JPMC data is impacted.

BUSINESS RESILIENCY

- Supplier must have formal, comprehensive business resiliency plans to enable timely, orderly, and sustainable recovery of business, support processes, operations and technology elements associated with the services provided for JPMC.
- Supplier must perform a Business Impact Analysis (BIA) to estimate the impact caused by disruptive failure to services provided for JPMC so that appropriate Recovery Strategies can be developed 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
- Supplier recovery plans must have recovery strategies in place to adequately address the following disruption scenarios to meet JPMC RTO and service level expectations (as defined in the relevant contracts):
    - Loss of staff
    - Loss of site
    - Loss of application (where application disaster recovery is available)
    - Loss of Supplier's subcontractors (where subcontractor recovery is available)
- The resiliency plans must have acceptable alternative work locations/strategies in place to ensure service level commitments are met.
- Supplier recovery plans must be updated, reviewed and approved by the Supplier's management at least annually or as material changes occur within Supplier's operating environment.
- Resiliency plans, including recovery strategies must be tested on a regular basis, noted deficiencies/failures should be addressed timely, and testing should:
    - be conducted in conditions comparable to production
    - demonstrate recovery within the established Recovery Time Objectives
    - be tested annually
- Supplier must conduct testing of the effective operation of avenues of communication to all personnel and subcontractors associated with recovery plans and strategies at least annually.

- Any change that may involve, but is not limited to, changes in Supplier's business strategy, service, process, assets, and regulatory/legal obligations that could result in significant changes to the BIA or plans and/or affect the recovery of the process or infrastructure, must be tested within a year of the effective date of the significant change.

TECHNOLOGY RESILIENCY

- The Supplier must have formal technology recovery plans and technical capability and implemented recovery strategies adopted to ensure appropriate capabilities are in place to limit impact following a disruptive event (i.e. operational disaster or destructive cyber event where both the primary (production) and secondary (disaster recovery) systems or data have been compromised or destroyed. The formal technology recovery plans must include:
    - Details of approved recovery objectives (RTO, RPO, Maximum Tolerable Downtime).
    - Identified resources and specific actions required to help minimize losses in the event of a disruption to services provided to JPMC or resources supporting those services.
    - Procedures required to redeploy an application and restore associated data following a loss.
    - Processes and procedures required to enable recovery of internal IT services to normal production operation, within the RTO, as defined in relevant contracts.
    - 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.
    - Relevant Supplier's subcontractors, including cloud service providers critical to executing the recovery procedures
- Recovery plans must be tested on a regular basis using sufficient methodologies and frequencies which include testing long term strategies. Test failures must be re-tested within a reasonable amount of time.
- Any change that could affect the recovery of the process or infrastructure, including 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.
- All service provided by the Supplier (applications and associated hosts) must employ a backup policy to ensure the availability of data required for full application recoverability.
    - The policy must define datasets, frequencies, criteria for a successful backup, annual test requirements, offsite storage requirements, and retention periods.
    - The backup policy must be annually reviewed and recertified.
- Supplier must have a crisis management framework including initial notification to JPMC, ongoing contact with JPMC during an incident impacting the services being performed by Supplier, and an after action review of the incident.
- JPMC Confidential Information must be available upon request, in an industry standard format, so as to ensure portability and interoperability.

ORGANIZATIONAL SECURITY

- Supplier Personnel assigned to JPMC Services must review the JPMC Supplier Code of Conduct available at: https://www.jpmorganchase.com/about/suppliers.
- Supplier Personnel must notify JPMC in the event of any potential 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, including cybersecurity awareness, 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 (addressing, e.g., proper handling of individual personal information in light of privacy laws and regulations), including as may be specified in the relevant contract(s) and/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) and/or as directed by JPMC.