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 Information Security Program must be document, reviewed, and implemented in alignment with industry standard frameworks (i.e. COBIT and NIST). All risks and controls must be documented, assessed, and aligned with industry standard frameworks.
- 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 process must exist to facilitate the identification, assessment, and compliance with legal and regulatory obligations impacting the supplier technology environment.
- A risk-based process must be in place for prioritization and remediation or risk acceptance of controls that have not been adopted or implemented.
- Awareness training on security policies, responsibilities and obligations, must be communicated and socialized to Supplier Personnel. including but not limited to, cybersecurity, technology, and data management.

PHYSICAL SECURITY

- Physical security processes and procedures must be in place for facilities with access to, or storage of, JPMC Confidential Information.
- 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.

ENVIRONMENTAL SECURITY

- 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.

CRYPTOGRAPHIC SERVICES AND DATA LOSS PREVENTION

- Suppliers and dependent subcontractors must develop a data protection policy that covers at a minimum the use of cryptographic mechanisms (e.g., encryption, hashing, digital signatures, etc.), key lifecycle management, and permitted cryptographic algorithms and associated key lengths.
- Suppliers and dependent subcontractors must have sufficient information classification for the purpose of data protection.
- The data protection policy must be reviewed against industry standards, applicable regulatory requirements, and best practices on a regular basis.
- All JPMC Highly Confidential and Confidential Information must be protected by industry (financial services) standard cryptography while in transit and at rest.
- All authentication credentials (e.g., passwords, personal identification numbers, challenge answers) must be encrypted in transit and at rest.
- All cryptographic keys must be managed throughout their lifecycle.
- Data Loss Prevention (DLP) processes, technology and/or solutions must be in place to detect and evaluate potential DLP events in order to protect sensitive data, including but not limited to non-public JPMC information, from being exfiltrated through user-initiated egress points such as email, websites, removable media, SaaS, vendor platforms, print, and messaging applications.
- Suppliers and dependent subcontractors must perform periodic assessments to evaluate the risk for data exfiltration and control effectiveness.

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 commensurate 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 and inventory, safeguarding of privileged accounts and credentials, privileged activity logging and post activity review requirements, and assurance that non-interactive privileged accounts (e.g., system accounts) are not used interactively by human users.
- A documented authentication and authorization policy must cover all applicable systems and networks and the provisioning of credentials including passwords and other secrets, supporting multi-factor authentication. This policy must include password complexity and reset requirements, 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 Supplier network.
    - Applications directly accessible from the internet.
    - The administration of application access.

- Federated identity management should be implemented for JPMC access to Supplier systems via industry standard, e.g. security assertion markup language (SAML) or OpenID Connect (OIDC) or other mechanisms that prevent JPMC workforce users from accessing Supplier systems from outside the JPMC network.

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

- 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.
- Retention schedule for various logs must be defined and followed.
- 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.

VULNERABILITY MANAGEMENT

- Suppliers must maintain a governance framework that includes regular reviews and updates to vulnerability management policies, procedures, and tools, ensuring that the program remains effective and up-to-date with industry standards.
- Supplier must include as part of their vulnerability management program, the receipt of vulnerability related security alerts and intelligence from external and internal sources to identify and monitor for vulnerabilities in their environment. Vulnerability alerts are acted upon in a timely manner, and threat intelligence is incorporated into the vulnerability management

practices.

- Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically or whenever significant changes occur, and prior to system provisioning for all systems that process, store, or transmit JPMC Confidential Information. The scanning tools used must cover all in-scope systems and applications, and the results must be documented and reviewed for completeness.
- 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. Remediation actions must be documented, and their effectiveness validated through follow-up assessments.
- Supplier must track and report key metrics related to vulnerability management**,** including but not limited to the number of vulnerabilities identified per scan, time taken for remediation, percentage of critical vulnerabilities remediated within SLA, and the success rates of remediation efforts.

PRIVACY

- Provide reasonable technical, organizational, personnel and physical measures to protect against the unauthorized or unlawful Processing of Personal Information and against the accidental loss and destruction of, or damage to, Personal Information.
- Promptly notify JPMC of any unauthorized or unlawful Processing, loss of, damage to or destruction of Personal Information; promptly take all necessary steps to investigate and remediate any security or confidentiality breach; promptly make available to JPMC any report generated in respect of such investigation.
- 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 not use government-assigned identification numbers (such as, but not limited to, Social Security Numbers or other national identifiers) as user IDs for logon to applications and systems
- If Supplier collects Personal Information from any individual on behalf of JPMC, Supplier must implement procedures to make a JPMC privacy notice available and obtain informed consent from individuals prior to collecting Personal Information.
- 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.
- Take reasonable efforts to ensure that Personal Information is accurate and complete, if such information is likely to be (i) used by JPMC or Supplier to make a decision that affects the individual to whom such Personal Information relates or (ii) disclosed by the Service Provider to another organization (where permitted by JPMC).
- Promptly notify JPMC of any order or request for disclosure of the Personal Information by a court, regulatory authority or law enforcement, unless such notification is otherwise prohibited by an applicable law.

TECHNOLOGY DEVELOPMENT

<u>System Development Life Cycle (SDLC)</u>

- Suppliers must develop, maintain, and enforce a System Development Life Cycle (SDLC) process that enables the identification, tracking and remediation of defects, vulnerabilities, coding errors and design flaws prior to production.
- The SDLC process must be adequately governed following a risk-based approach in-line with industry standards and frameworks, and continuously improve based on periodic assessments to ensure software is secure and suitable for production.
- The SDLC must establish the control requirements for software development that are

applicable to all software and development framework used.

- Functional and non-functional requirements must be continuously identified and implemented to prevent software obsolescence.

Third-Party Software

- Third party software and open-source code used must be appropriately licensed, inventoried, and where commercially licensed, be fully supported by the vendor.
- Implement a software supply chain security program to assess and manage the risks associated with third-party and open-source software. This includes, but is not limited to, verifying the integrity and authenticity of software components and ensuring they are free from known vulnerabilities.
- Continuously monitor and manage software dependencies to ensure that all third-party and open-source components are up-to-date and free from known vulnerabilities.
- Ensure that all third-party and open-source software components are used in compliance with their respective licenses and that any licensing obligations are met.
- Establish an incident response plan for third-party software vulnerabilities, including processes for vulnerability disclosure, patch management, and communication with affected stakeholders.

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

- Documented security policies and procedures that are reviewed on a periodic basis and must govern the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of confidential information, assets, and associated services.
- 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 to address; accuracy, timeliness, completeness of data, and structural correctness and for notifying JPMC of errors for data transmitted to or from JPMC. in accordance with quality specifications for the accuracy, timeliness, completeness, and structural correctness of the data.
- All JPMC data provided to and stored, both physically and digitally 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 provide reasonable safeguards against hazards, that include, but are not limited to, the following (Not limited to but including both physical and digital):
        - 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
- Supplier and dependent subcontractors must have controls in place to ensure JPMC data is collected, created, stored, and processed in compliance with applicable laws, regulations, and contractual obligations, inclusive of relevant data use restrictions and all applicable global data privacy laws.
- Business records are appropriately identified with the relevant retention requirement. Data within such business records is disposed of once the retention requirement has been met.
- 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 at a minimum the following attributes:
    - Description of Data
    - Sensitivity and Criticality Classification of Data
    - Retention/Destruction Requirements (and execution of those requirements)
    - Location of Data
    - Use of Data
- Supplier and dependent subcontractors must be able to maintain data provenance in accordance with Global Data Regulatory requirements.

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.

- Supplier must have a security event/incident response policy and procedure.
- Supplier Personnel must be trained to identify, and report suspected security weaknesses, suspicious activity, and security events or incidents.

BUSINESS RESILIENCY

Supplier Business Resiliency Planning

- Supplier must perform a Business Impact Analysis (BIA) to estimate the impact caused by disruptive failure to services provided for JPMC, which informs formal and comprehensive Business Resiliency (BR) plans to enable timely, orderly, and sustainable Recovery of business, support processes, operations and technology elements associated with the services provided for JPMC.
- Supplier BR plans must be updated, reviewed and approved on a regular basis or as material changes occur within their operating environment.
- Supplier BR plans must have Recovery Strategies to adequately address Supplier recovery in the event of disruption to the assets upon which the Supplier depends to provide services to JPMC. The strategy must meet JPMC RTOs and service level expectations (as defined in the relevant contracts). At a minimum Supplier BR Plans must consider Recovery Strategies for the following:
    - Disruption to Staff
    - Disruption to Site
    - Disruption to application(s)
    - Disruption to Supplier's subcontractors
- Maintain an Incident and Crisis Management Framework inclusive of a process to notify JPMC during a BR incident impacting the Supplier services provided to JPMC.
- Supplier Identified significant deficiencies/failures/limitations in Recovery capabilities must be communicated to JPMC in a timely manner.
- Supplier must provide contact information to JPMC for use in the event of disruption to either party, and update JPMC when changes occur.

Supplier Business Resiliency Testing

- Supplier must conduct testing of the effective operation of avenues of communication to all personnel and subcontractors associated with recovery plans and strategies at on a regular basis.
- Supplier must conduct testing of their planned Recovery Strategies to address disruption to assets upon which the Supplier depends to provide services to JPMC. Testing must be conducted on a risk based frequency by the Supplier for Site and Staff disruption, which at a minimum must:
    - Be conducted on a production day or production like condition by the Supplier staff that provide the in-scope services to JPMC.
    - Demonstrate that the in-scope Supplier processes tested recover within the RTO established by the relevant LOB or CF that has contracted the service(s).
- Assessment must be conducted on a risk based frequency by the Supplier to evaluate the sufficiency of their subcontractors resiliency controls Significant deficiencies and / or limitations in Supplier subcontractor Recovery capabilities must be identified and communicated to JPMC.
- Suppliers must also test on a risk based frequency their Recovery Strategies (e.g. manual work arounds or alternate processing with reference to supplier exit plans where applicable) for disruption to any critical subcontractor the Supplier uses to support JPMC.

TECHNOLOGY RESILIENCY

- The Supplier must ensure the adoption of a suitable recovery strategy for the technology service and provide suitable assurances of recovery capability following a disruptive event (i.e. operational disaster, destructive cyber event where the production environments have been compromised).
- The supplier must define recovery action plans documenting specific recovery procedures to guide the failover of the technology service to the disaster recovery site or redeploy the service including data restoration. The plan should include the following:

- 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.
    - Recovery 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 hosting/service providers critical to executing the Plan.
- Recovery Action plans must be tested annually using sufficient methodologies to provide suitable assurances that recovery objectives can be achieved:
    - The test must include a simulated disruption across the following scenarios:
        - Loss of Application Deployment (Service or Site) requiring failover of the service to the recovery site.
        - Loss of Data requiring a restoration from immutable backup.
        - Loss of both production/DR environment requiring a full rebuild of the infrastructure environment, application redeployment and data restoration.
    - Where the test scope simulates a failure to the production environment, the ability to support business operational workloads in the recovery site must be a condition for determining a successful test.
- All services 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 re-certified.
- 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.

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.