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 documented, 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.
- A documented risk management program must be in place to effectively evaluate, mitigate, and monitor risks across the technology environment.
- An assessment must be performed annually to verify the identification, implementation, and effectiveness 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.
- 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 applicable environmental controls, such as 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 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.
- All storage media containing JPMC data, regardless of its classification, must be encrypted. Furthermore, highly confidential and confidential information must be secured with industry-standard encryption while in transit and at rest.

IDENTITY AND ACCESS MANAGEMENT

- A documented authentication and authorization policy must cover all production systems and networks and the provisioning of credentials including passwords and other secrets. This policy must include password complexity and identity verification for reset requirements, thresholds for lockout for failed login attempts, and thresholds for inactivity. Policy must include Multi-factor authentication (MFA) requirements and MFA must be implemented for:
    - The initiation of any interactive privileged access session.
    - External connectivity to the Supplier network.
    - Applications directly accessible from the internet, including JPMC access to Supplier systems when federated identity management is not supported.
    - The administration of application access.
- Each account provisioned must be uniquely identified and traceable to an individual user with 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.
- 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.
- 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.

- 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.

SECURITY CONFIGURATION

- The supplier must segregate networks based on risk profiles and have a governance process in place to approve and periodically review connectivity requests.
- The supplier must implement controls to protect its infrastructure and services against distributed denial of service (DDoS) and web application attacks.
- The supplier must have network access controls in place to prevent unauthorized devices from accessing the supplier's internal network.
- The supplier must have controls in place to inspect and control network traffic leaving the supplier to block known malicious sites and activity.
- The supplier must implement controls that allow for the detection and analysis of intrusion events.
- The supplier must document their network architecture and keep it up to date.
- The supplier must define, deploy, and manage secure baseline configurations for each major version of defined asset types and endpoints, which are based on industry best practices and the principle of least functionality.
- The supplier must employ configuration management mechanisms to identify and manage deviation from approved secure baseline configuration builds for in-scope asset types.
- The supplier must have malware protection mechanisms in place that protect endpoints, inbound and outbound connectivity, and email services.
- The supplier must strictly separate personal email domains from corporate email domains, ensuring that all corporate actions and data are only associated with approved corporate email domains.
- The supplier must log security events and feed them into a Security Event & Incident Management platform for the purpose of monitoring and alerting of suspicious cyber activity.

SECURITY OPERATIONS

- The supplier must have a brand protection program that protects the supplier, its brands, and its customers from brand infringement activities.
- The supplier must have a process for supporting and/or conducting forensic activities including data collection, data/evidence preservation for future analysis, analysis, reporting of findings, and closure.
- The supplier must regularly conduct cybersecurity exercises such as red teaming and social engineering engagements to identify gaps in people, processes, and technology. Findings must be reported, reviewed and accepted by stakeholders.
- The supplier must have a Security Information and Event Management (SIEM) system that allows for aggregation and correlation of security logs and data from multiple sources for the purpose of detecting and alerting on cyber related threats and malicious activity.
- The supplier must have a defined retention schedule for security logs and protect the integrity of those logs.
- The supplier must have a governance process that ensures the effectiveness of its security monitoring processes.
- The supplier must have a dedicated security operations function that continuously monitors for cyber threats and events.
- The supplier must have fraud and threat intelligence processes that protect the supplier and its customers from fraudulent activities and threats that might disrupt operations.

VULNERABILITY MANAGEMENT

- The supplier must have a vulnerability management program that:
    - Supports the receipt of vulnerability related security alerts and intelligence from reputable external and internal sources to identify and monitor for vulnerabilities in their environment.
    - Supports identification of vulnerabilities through vulnerability scanning, internal assessments, and external vulnerability identifications programs.
    - Supports the prioritization, evaluation, and classification of all discovered vulnerabilities, including assessment of their criticality and impact based on the CVSS (Common Vulnerability Scoring System) industry standard.
    - Governs the remediation of actionable vulnerabilities through a framework that also tracks and reports 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.
    - Periodically evaluates the effectiveness of the vulnerability management processes.
- The supplier must have a penetration testing program for the purpose of identifying security weaknesses in applications, infrastructure, and network security controls (e.g. firewall configuration, intrusion detection policies etc.). These assessments must be performed at defined intervals on in-scope applications, infrastructure, and network security controls. The penetration testing program must ensure the use of a standardized testing framework that incorporates industry best practices and must include a governance process which evaluates the effectiveness of the program.

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. Ensure compliance with applicable data protection regulations and relevant local laws.
- Promptly notify JPMC of any unauthorized or unlawful Processing, loss, damage or destruction of Personal Information. Take all necessary steps to investigate and remediate any security or confidentiality breach; promptly make available to JPMC any report generated from such investigation.
- Supplier must maintain documented procedures for collecting, processing and disclosing Personal Information including any legal restrictions, contractual arrangements and/or JPMC privacy policies. Regularly review and update these procedures to reflect changes in regulations.
- 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. Additionally, ensure such IDs are protected from unauthorized access.
- If Supplier collects Personal Information from any individual on behalf of JPMC, including information collected via websites, Supplier must implement procedures to make the relevant JPMC privacy notice(s) available and obtain informed consent from individuals (in line with regulatory requirements) prior to collecting Personal Information.
- Provide complete and timely responses to JPMC, and take necessary actions 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

System Development Life Cycle (SDLC)

- 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 to include planning and 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 to outline the planning, recording, 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 to cover patch compliance and hygiene activities to keep the systems secure, stable, and up to date by addressing vulnerabilities, bug fixes, and features enhancements. 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 Supplier 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 and Highly Confidential information, assets, and associated services.
- Supplier must ensure all Confidential and Highly Confidential production data is de-identified or

declassified for use prior to moving it to any non-production environment (e.g., Environments used solely for the support of development, testing or evaluation of technology).

- 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
- Suppliers must have controls in place to ensure compliance with data localization laws by ensuring data is physically (original or in copy) stored within the required geographic boundaries and adheres to applicable regional or country safeguards.
- Business records are appropriately identified with the relevant JPMC retention requirements. Data within such business records is retained until the end of the retention period and then 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
    - JPMC Retention/Destruction Requirements
    - Location of Data
    - Use of Data per contractual agreement
- 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, and maintaining a Software Bill of Materials (SBOM) for all software assets.
- 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.

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 to ensure 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 a Technology and Cyber Incident Management process documented that includes incident tracking, reporting, prioritization of incident response based on classification, internal escalation, remediation, preservation of data, and data loss tracking (if any) 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 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 service disruption caused by the following:
    - Disruption to Staff
    - Disruption to Site
    - Disruption to Application(s)
    - Disruption to Supplier's subcontractors
    - Disruption to any other supporting elements required for providing services to JPMC
- 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 their 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 test the effectiveness of their communication protocols to contact all personnel and subcontractors associated with Supplier recovery plans and execution of Supplier planned recovery strategies on a regular basis.
- Supplier must test all planned Recovery Strategies to address disruption to the services provided to JPMC. Testing must be conducted on a risk based frequency, and as a minimum include all planned Recovery Strategies related to service disruption caused by the following:
    - Disruption to Supplier Staff *
    - Disruption to Supplier Site(s) *
    - Disruption to Supplier Application(s)

- Disruption to Supplier sub-contractors
- Disruption to any other supporting elements required for providing services to JPMC

* Considerations should encompass conducting tests on a production day or in production-like environments, and demonstrating recovery within established RTOs and service level requirements

- Subcontractor disruption
  - 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 (including data loss tolerance) 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.