Supplier Minimum Control Requirements – 2018 Updates

This change log references the JPMorgan Chase & Co. Minimum Control Requirements document (MCR), published in December of 2018. It specifies material changes made in this update cycle to facilitate comparison with the prior version. Use this change log as a guide and refer to the Minimum Control Requirements document itself for the exact wording of the controls.

Section 1: Holistic Changes Applied to Multiple Control Categories

Minimum Control Requirements – Section 1: Holistic Changes

Subject of Change	Control Categories	Description
The MCR document states control objectives corresponding to questions asked of all JPMC suppliers subject to an audit by JPMC.	All except Application	• Details of implementation and additional requirements not included in the MCR document on this basis may be addressed in audits of specific suppliers, as described on page 1 of the document.
"Dependent suppliers" (*i.e.*, subcontractors) are mentioned for emphasis in specific control areas.	Introduction (pg.1), Organizational Security, Communications and Connectivity, Logical Access, Encryption, Business Continuity and Disaster Recovery, Media and Vital Records, Third Party Relationships, Cloud Technology, Data Use	• Subcontractors to the JPMC supplier are now referred to as "dependent suppliers" within the MCR. • Note that "dependent suppliers" includes subcontractors, regardless of tier, including any respective subcontractors to a firm with which the supplier has a direct contract. • While all controls are applicable to dependent suppliers, some control categories include specific call-outs to highlight the relevance to dependent suppliers' control environments in accomplishing the required objective.
Data classifications are mentioned only where they serve as drivers for specific control requirements.	All	• The following statements regarding data classifications have been added to the first page of the MCR document: *(ii) 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 (the "Agreement"); and, (iii) "Confidential Information" is understood to include "Highly Confidential Information", "Personal Information", and "JPMC Data".* • "Highly Confidential Information" and "Personal Information" are mentioned only where data classifications impact control requirements *(e.g.,* Encryption).
Documented policies and procedures require periodic review and approval, with management oversight.	All	• Requirements around documentation of processes and procedures have been standardized across the MCR document. • Specific periodicity for review and re-approval will be addressed in the audit process.

Section 2: Material Changes to Specific Control Categories

Minimum Control Requirements – Section 2: Material Changes

Control Category	Page(s)	Description	Specific Wording *(See MCR for complete text.)*
Introduction	1	• Added formal language stating that JPMC may use TruSight to perform an assessment and, when that occurs, a separate non-disclosure agreement is not required.	• *JPMC may use TruSight Solutions, LLC ("TruSight") as an external Auditor to facilitate and conduct Audits. TruSight, in turn, may use an independent firm, e.g., EY, as an external Auditor to conduct Audits. Supplier will cooperate with any such external Auditor as reasonably requested by JPMC or any such external Auditor, including entering into agreements…*
Technology Asset Management	3	• Modified name of control category.	• *Technology Asset Management*
		• Broadened control objective statement.	• *Controls must be in place to protect assets, including mechanisms to maintain an accurate inventory of assets and handling standards for introduction and transfer, removal and disposal of all assets.*
		• Broadened control by removing detail.	• *Procedures must be documented for sanitization…*
Communication and Connectivity	4	• High-level control objective rephrased for clarity.	• *Supplier must implement controls over its communication network to safeguard data. Controls must include securing network and implementation of encryption, logging and monitoring, and disabling communications where no business need exists.*
		• Added a Data Loss Prevention control; previously, DLP was covered only in the Cloud Technology section.	• *Data Loss Prevention (DLP) solutions should be deployed to protect JPMC Data, including all points of egress, except to the extent prohibited by legal or regulatory restrictions.*

Minimum Control Requirements – Section 2: Material Changes

Control Category	Page(s)	Description	Specific Wording *(See MCR for complete text.)*
Data Integrity	6-7	• Controls broadened.	• *Processes, procedures and controls must be documented, reviewed, and approved, with management oversight, on a periodic basis, to ensure data integrity…* • *Controls must be in place to protect the integrity of data transactions at rest and in transit.*
Encryption	7	• Data protection is now the stated objective aim; encryption is required where achievable by means of "commercially reasonable efforts".	• *Data must be protected and should be encrypted, both in transit and at rest, including when shared with dependent suppliers.*
		• See page 1 of the MCR document for the definition of the term "should" and requirements for documenting rationale for any deviation.	• *JPMC Data must be protected, and should be encrypted, while in transit…* • *Highly Confidential Information must be protected, and should be encrypted, when stored…*
		• Encryption key management requirements are called our under the "Encryption Policy" sub-header.	• *Data protection policy must cover data classifications, encryption use, key and certificate lifecycle management, cryptographic algorithms…*
Incident Response	7	• Prioritization, containment and remediation added to the list of required specifications in policies and procedures. • Process requirements include preservation of data for forensic analysis.	• *The incident management policy and procedures must include prioritization, roles and responsibilities, procedures for escalation (internal) and notification (to JPMC), tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity.*

Minimum Control Requirements – Section 2: Material Changes

Control Category	Page(s)	Description	Specific Wording *(See MCR for complete text.)*
Business Continuity and Disaster Recovery	7-8	• Control category name changed from "Business Continuity, Disaster Recovery and Pandemic" to "Business Continuity and Disaster Recovery". • Pandemic-related control requirements may be addressed in audit processes with specific suppliers.	• *BUSINESS CONTINUITY AND DISASTER RECOVERY*
Back-up and Offsite Storage	8	• High-level control objective rephrased for clarity.	• *Supplier must have policies and procedures for back-up of JPMC Data. Back-up media must be protected in storage, offsite storage, and sanitized prior to disposal or reuse.*
		• Control rephrased.	• *Back-up media must be rendered unreadable when no longer required.*
Media and Vital Records	9	• Controls amended to cover storage and movement of paper records and electronic media.	• *Electronic media and paper records storage and movement procedures must be documented, reviewed, and approved, with management oversight, on a periodic basis, both by Supplier and dependent suppliers.* • *Electronic media and paper records must be stored in secure bins.*
Third Party Relationships	9	• Dependent suppliers must be approved by JPMC "to the extent required by the Master Agreement.**"**	• *Supplier must have a process to identify all dependent suppliers providing services to Supplier; these dependent suppliers must be disclosed to JPMC and approved to the extent required by the Master Agreement.*
		• Performance reviews on dependent suppliers must be performed.	• *Performance review processes must be in place to ensure dependent suppliers' fulfillment of contractual terms and conditions.*

Minimum Control Requirements – Section 2: Material Changes

Control Category	Page(s)	Description	Specific Wording *(See MCR for complete text.)*
Standard Builds	9-10	• Control broadened.	• *Systems must be configured to provide only essential capabilities.*
		• Control revised.	• *The ability to write to electronic media must be limited to documented exceptions.*
Customer Contact	12	• Control revised.	• *Prior to working on JPMC related calls, customer contact agents must receive training regarding the proper provision of Services and other Deliverables and privacy training, which must cover:..*
Vulnerability Monitoring	12	• High-level control objective revised. (Sub-headers altered for correspondence with revised controls.)	• *Supplier must continuously gather information and analyze vulnerabilities in light of existing and emerging threats and actual attacks. Processes must include vulnerability scans, anti-malware,…*
		• Controls strengthened.	• *All devices must be kept up-to-date with latest anti-virus definitions to mitigate known threats. Anti-virus tools must be configured to run periodic scans to detect, log and disposition malware.*
		• Control revised to focus on up-to-date signatures.	• *IDS/ IPS signatures must be kept up-to-date to respond to threats..*
Regulatory Compliance	13	• Controls clarified and strengthened.	• *Supplier must comply with and have processes for researching, evaluating, and complying with, all Laws relevant to the business, process, or activity being undertaken in the particular jurisdiction(s). Any alleged non-compliance with Laws, regulatory inquiries,…*
		• Data retention control (covered in the Media and Vital Records section) removed.	

Minimum Control Requirements – Section 2: Material Changes

Control Category	Page(s)	Description	Specific Wording *(See MCR for complete text.)*
Privacy	13	• Added controls related to users' rights in relation to their Private Information.	• *A process to allow users to access correct, opt-out, delete, restrict, make portable, or object to the processing of, Personal Information must be documented, reviewed, and approved, with management oversight, on a periodic basis.*
Cloud Technology	14-15	• Cloud section completely revised.	Please see the MCR document itself.
Business Practices	15	• Control strengthened to include that Supplier Personnel must have access to policies and procedures.	• *Policies and procedures addressing Supplier business operations, processes for responding to customer complaints, handling of non-public information, signing authority, code of conduct, and change control must be documented, reviewed, and approved, with management oversight, on a periodic basis, and made available to Supplier Personnel.*
		• Fraud related control amended to include reporting.	• *A fraud detection, prevention and mitigation program, processes and procedures for monitoring and reporting actual and suspected instances of fraud…*
Data Use	15	• Data Use control category added.	Please see the MCR document itself.