# Supplier Minimum Control Requirements – 2022 Updates

December 2022

JPMorgan Chase & Co.

# Supplier Minimum Control Requirements – 2022 Updates

## Introduction

This change log references the JPMorgan Chase & Co. Minimum Control Requirements document (MCR), published in December of 2022. 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 to the Minimum Control Requirements

# Supplier Minimum Control Requirements – 2022 Updates

## Section 1: Holistic Changes

| Subject of Change | Control Domain(s) | Description |
|---|---|---|
| None | N/A | • No changes to the structure/format/etc. of the Supplier Minimum Control Requirements for 2022 |

# Section 2: Changes to Specific Control Domains

# Supplier Minimum Control Requirements – 2022 Updates

## Section 2: Changes to Specific Control Domains

| Control Domain | Subject of Change | Description |
|---|---|---|
| **Technology Governance Risk and Compliance** | - Change to 1 existing statement | - Security policies and responsibilities, including cybersecurity awareness training, must be communicated and socialized within the organization to Supplier Personnel. |
| **Data Protection** | - Addition of 3 new statements<br>- Removal of 1 statement<br>- Change to 2 existing statements | - Suppliers and dependent subcontractors must have sufficient information classification for the purpose of data protection<br>- Data protection policy must be reviewed against industry standards on a regular basis.<br>- Supplier must implement appropriate technical configuration for the protection of encrypted portable media.<br>- ~~The ability to write to portable electronic media must be disabled where possible, and any exceptions must be documented~~<br>- All authentication credentials (e.g., passwords, personal identification numbers, challenge answers) must be encrypted in transit and at rest.<br>- Supplier's data protection policy must cover ~~data classifications,~~ encryption ~~use~~, key and certificate lifecycle management, permitted cryptographic algorithms and associated key lengths, message authentication, hash functions, digital signatures, and random number generation ~~and be reviewed against industry standards on a regular basis.~~ |

# Supplier Minimum Control Requirements – 2022 Updates

## Section 2: Changes to Specific Control Domains

| Control Domain | Subject of Change | Description |
|---|---|---|
| **Identity and Access Management** | • Addition of 2 new statements<br>• Removal of 1 statement<br>• Change to 1 existing statement | • 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<br>• Multi-factor authentication must be implemented for:<br>  • The initiation of any interactive privileged access session ~~and/or retrieval of credentials with privileged access~~<br>  • The administration of application access<br>~~• Management of privileged user accounts to include service accounts, must follow a documented process and be restricted.~~ |
| **Incident and Event Management** | • Addition of 1 new statement<br>• Removal of 1 statement<br>• Change to 2 existing statements | • Documented incident, event, or problem management procedures must include systematic tracking ~~of problems~~ from discovery to resolution.<br>• Supplier's event management policy and procedures must account for the ~~identification~~ detection, analysis, and presentation of anomalous events that indicate deviation from the norm beyond a defined threshold and engage JPMC via an incident management process.<br>~~• Supplier must also process and analyze events to determine if action is required, and to engage JPMC via the Incident Management process.~~<br>• Supplier's problem management policy must include documenting root cause analysis, implementation of permanent fix, preventative actions, and service improvement opportunities, providing conclusions to JPMC. |

# Supplier Minimum Control Requirements – 2022 Updates

## Section 2: Changes to Specific Control Domains

| Control Domain | Subject of Change | Description |
|---|---|---|
| **Security Configuration** | • Change to 1 existing statement | • Network and host-based intrusion detection and/or intrusion prevention systems ~~(IDS and IPS)~~ must be deployed with generated events fed into centralized systems for analysis. |
| **Security Operations** | • Change to 1 existing statement | • Supplier Personnel must be trained to identify and report suspected security weaknesses, suspicious activity, and security events or incidents. |
| **Technology Development** | • Addition of 1 new statement<br>• Addition to 1 existing statement | • Functional and non-functional requirements must be continuously identified and implemented to prevent software from becoming obsolete.<br>• 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. |
| **Technology Operations** | • Removal of 2 statements<br>• Addition of 3 new statements<br>• Change to 3 existing statements | • See MCR Document for specific language |
| **Privacy** | • Addition of 1 new statement | • 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. |

# Supplier Minimum Control Requirements – 2022 Updates

## Section 2: Changes to Specific Control Domains

| Control Domain | Subject of Change | Description |
|---|---|---|
| **Data Risk Management** | • Removal of 2 statements<br>• Change to 6 existing statements | • See MCR Document for specific language |
| **Organizational Security** | • Change to 2 existing statements | • Supplier personnel assigned to JPMC Services must ~~be provided a copy of~~ review the JPMC Supplier Code of Conduct available at: https://www.jpmorganchase.com/about/suppliers<br>• Supplier personnel must notify JPMC in the event of any potential~~, perceived~~ or actual conflicts of interest between Supplier personnel's outside business activities and personal relationships and JPMC business, clients, or employees. |