

RPM Technology Procurement Policy

WHY A POLICY REGARDING TECHNOLOGY PROCUREMENT?

RPM had deemed Information Technology as a Corporate-Driven & Center-Led function, with goals to reduce complexity, drive efficiencies and create technology standards across the organization. In order to meet these goals, RPM has a technology procurement policy.

WHAT DOES THIS POLICY APPLY TO?

This policy applies to the procurement, subscription or agreements as it pertains to (but not limited to):

- Software
- Hardware
- Networking
- Telephony
- Technology consulting services
- File sharing services
- Software as a Service (SaaS) offerings
- Infrastructure/Infrastructure as a Service (IaaS) offerings
- Platform as a Service (PaaS) offerings
- AI software, platforms, and services including:
 - Generative and predictive AI tools
 - AI-enabled services
 - AI consulting or integration services

TECHNOLOGY PROCUREMENT

All technology-based procurement must be submitted via the RPM One CapX system, and approved by local finance, group IT leadership and RPM IT leadership prior to any agreements, orders or proposals are executed. Technology offerings must be submitted via CapX regardless of spend type (Capital or Expense).

As part of the CapX submission, requested technology offering will be validated against other company standards to determine if there is a standard offering that could accomplish the same needs. A request to add to the standards must be made as part of the CapX submission and have valid reasoning/applicability to be considered.

ADDITIONAL AI PROCUREMENT REQUIREMENTS

For AI-related technologies, associates must consult the AI SharePoint site for the current list of approved AI tools prior to initiating procurement. If a desired technology is not listed, an evaluation of the technology will need to be performed by the AI Governance Office.

Vendors must provide documentation demonstrating compliance with RPM's AI standards, including:

- Model cards or algorithmic transparency reports
- AI policy documentation

Procurement will collaborate with the AI Governance Office to ensure all evaluations are completed prior to finalizing any agreements.

ADDITIONAL STEPS

In addition to notifying local finance, group IT leadership and RPM IT leadership via CapX; the following must occur:

- Group General Counsel must be notified.
 - If General Counsel determines that a Data Protection Impact Assessment (DPIA) form must be submitted, the DPIA must be fully completed prior to execution of any purchase or agreement.
- Complete the [Vendor Supplier Required Information Form](#) and forward to Operating Company Finance Team or local, trained LSEG (Refinitiv) users.
 - The requesting company finance team/trained users will input the vendor information into LSEG (Refinitiv) for Media Check & World Check verification. The results will be assessed by LSEG (Refinitiv) and will be given a score of “Low Risk”, “Medium Risk”, or “High Risk”. If “Medium” or “High”, RPM Compliance will execute expanded due diligence as appropriate. A list of local LSEG (Refinitiv) users [is available here](#); however, it should be noted that this is an evolving list.

This policy applies to all RPM and RPM subsidiary employees and any employee who violates this policy may be subject to disciplinary action up to and including termination. Any requests for exemption from this policy must be submitted to and approved by RPM’s Vice President – Global Systems or RPM’s Vice President – Commercial Excellence.