RPM International Inc.

Effective May 1, 2025

RPM International Inc.
Global Business-Related Communications Policy

We each have a responsibility to ensure business-related communications are exchanged through and on secure, approved, and supervised devices, apps, channels, and systems. Exchanging business-related information through a mechanism that is not managed or otherwise approved by RPM International Inc. or its affiliated companies (collectively, the "Company") could expose the Company to security risks and legal fines. *See the end of this Policy for a definition of what constitutes "business-related" communications. See the RPM Records and Information Management Policy for more information on Company Records. See the RPM Global Default Retention of Digital Messages Policy for more information on how long digital business-related communications should be retained.*

Purpose

The purpose of this policy is to: a) confirm that business-related communications are Company Records belonging to the Company; b) direct that the exchange of business-related communication occurs through and on Company managed or approved devices, apps, channels, and systems; and c) ensure that all Company Records are properly retained and produced in accordance with the Company's legal and ethical obligations.

Scope

This Policy applies to all employees (collectively or alone "you" or "your") of the Company and all business-related communications occurring both during and outside regular working hours, regardless of location or means of delivery.

Policy

- All business-related communications constitute Company Records which belong to and are the property of the Company.
- Business-related communications are to be transmitted only via Company managed tools, software, apps, systems or other appropriately vetted and approved applications or channels, as determined by RPM Information Security in coordination with group IT leaders.
- RPM Information Security must review and approve all communication tools, apps, or platforms that you want to use for business-related communication.
- Chats, SMS, instant or text messages, direct messages, email and other digital communication that constitutes business-related communication shall be properly maintained in accordance with the Company's Records Management policies and made fully accessible to the Company upon request.
- If a tool, application, system, or channel is approved for use which allows for instant deletion or otherwise is configured to encrypt, hide, or conceal the contents of communications by default (i.e. Snapchat, WhatsApp, WeChat) the settings shall be altered as necessary to ensure business-related communications are retained and available to the Company upon request. In the event the settings are not able to be configured in accordance with the Company's Default Retention of Digital Messages Policy, such tool, application, system, or channel is strictly prohibited and may not be used for business-related communication.

- Business-related communication shall not be stored on or sent through personal devices unless such device has been approved for use by the Company in accordance with the RPM BYOD Policy.
- Any business-related communications that have occurred on a platform or through a device, channel or application which has not been approved by the Company must immediately be transferred to an approved platform or archived by forwarding to a company-managed email address, platform, or system and deleted from the original platform, channel, device, and/or application.
- You must notify your supervisor and RPM Information Security of the use of any unapproved platform, channel or system and take steps to minimize future occurrences.
- The Company reserves the right to inspect hard drives, devices and external media used to exchange business-related communication to ensure compliance with this Policy.

Definitions

"Business-related" means topics and exchanges about or in reference to any Company matter including, but not limited to, pricing and payment terms; fees, charges, invoices and payments requested or made; product returns or complaints related to products, services, or customer service response; sales quotes, bids, and RFPs; litigation, legal notices and contractual negotiations; customer lists, specifications, or obligations and requests related to Company action or inaction; information related to Company financials, accounting records, processes, procedures and internal controls; corporate gifts, donations and contributions; employee administration, benefits, succession planning, termination and disciplinary matters; direct marketing or lead generation; environmental concerns, issues, fines or remediation; non-public, proprietary or confidential Company information; licenses, patents, and registrations; or exchanges with or about government officials involved in or related to the Company or its products or services; however, "business-related" does not include incidental or personal communications between internal or external parties related to matters having nothing to do with Company products, services, debts, payments, or employee administration, such as scheduling coordination or obtaining directions to a location.

This policy does not restrict or intend to violate or restrain any personal rights given to associates by law or mandatory legislation in specific jurisdictions, nor does it restrict associates from discussing their wages, hours, or other terms and conditions of employment, or other legally protected activities, including but not limited to under Section 7 of the National Labor Relations Act ("NLRA").

Company policies referred to in this Policy can be obtained on the Company's internal policy page, Navigator, at https://navigator.rpminc.com/. Any questions or concerns related to this Policy can be sent to infosec@rpminc.com or dataprotection@rpminc.com.

A suspected violation of this policy can be reported to your supervisor, human resources, or to any member of the legal or compliance departments. Employees are also welcome to contact the Company's Hotline to report their concerns to RPM. A suspected violation received by anyone in a management or supervisory role must be reported to RPM as a Reportable Event. Allegations will be investigated thoroughly and objectively. For more information, refer to RPM's Hotline and Non-Retaliation Policy. Any employee who violates this Policy, including the failure to submit a Reportable Event, directs or who knowingly permits a subordinate to violate a Policy, or who engages in retaliatory actions, may be subject to disciplinary action up to and including termination. The Company retains the right to report any violations of a Policy that are also illegal to the appropriate authorities.