Revised May 1, 2025

RPM INTERNATIONAL INC.
DIGITAL COMMUNICATIONS
RECORDS MANAGEMENT POLICY

Purpose

The purpose of this Policy is to set a standard default retention period to be applied to digital messaging tools and applications used by associates of RPM International Inc. or any of its affiliated companies (collectively, the "Company") for business-related communications.

Scope

This policy applies to all chats, SMS, instant or text messages, direct messages, email and other digital business-related communication.

Policy

Automatic deletion settings applied to email, instant messages and text messages will be set to delete business-related communications (as defined in the Global Business-Related Communication Policy) no less than sixty (60) days and no more than six (6) months from the date of initial creation or receipt. The Company will cause e-mails, instant messages and chats, to the extent saved on Company-managed servers and platforms, to be deleted automatically from the applicable server. Email and instant message back-ups will be deleted in accordance with the Company's applicable back-up standards. Users are required to delete business-related communications from any tool, platform, application or device not directly managed by the Company, including, but not limited to, iMessage, SMS/MMS, WhatsApp and other messaging applications in accordance with this Policy.

Any business-related communications that are required to be retained beyond six (6) months, or that are not otherwise managed directly by the Company, shall be saved in accordance with the applicable Records and Information Management Policy, and made available to the Company upon request.

An associate may not save a business-related communication to external media or another computer, forward it to a personal email account, save it to a hard drive or take any other action for the sole purpose of avoiding timely deletion of business-related communications. The Company reserves the right to audit hard drives, devices and external media used to exchange business-related communication to ensure compliance with this Policy.

All deletions in accordance with this Policy are subject to suspension in accordance with the applicable Litigation Hold Policy. 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.