

**RPM INTERNATIONAL INC.**  
**RECORDS AND INFORMATION MANAGEMENT POLICY**

Records, data and other documents, information and communications are important assets. Company Records, defined below, include essentially all records you produce or receive in your capacity as an associate of RPM International Inc. or any of its affiliated companies (collectively, the “Company”), whether in paper or through digital means. The law requires that the Company maintain certain types of corporate records, usually for a specified period of time. Failure to retain those records for those minimum periods or keeping records longer than necessary could subject you and the Company to penalties and fines, cause the loss of rights, obstruct justice, spoil potential evidence in a lawsuit, place the Company in contempt of court, or seriously disadvantage the Company in litigation.

**Purpose**

The purpose of this Policy is to define what constitutes a Company Record and set forth appropriate timelines related to the preservation and deletion of those Company Records.

**Scope**

This Policy applies to all employees (collectively or alone “you” or “your”) of the Company and any and all records created, received, maintained or stored by the Company or in the course of performing your duties for the Company (“Company Records”). This pertains to all forms of media, including, but not limited to:

- handwritten, typed, or printed documents on paper;
- electronic documents (e.g., e-mail, instant messages, text messages, spreadsheets, electronic notes, storage apps, databases, Web sites, cloud storage, CDs, flash drives- see the [RPM Business Communications Policy](#) for additional information on digital business-related communications);
- video;
- audio;
- graphic representations; and
- network servers and document management systems.

**Policy**

Company Records must be retained for the time period set forth on: Schedule A for those governed by the United States, or for the different period set forth on the data retention or information management schedule applicable to the respective jurisdictions and local law. If you have questions related to the retention of Company Records in your jurisdiction, please contact your group’s internal legal counsel or [dataprotection@rpm-inc.com](mailto:dataprotection@rpm-inc.com).

Upon the expiration of the designated retention time period, Company Records must be destroyed, unless retention is otherwise required by law or any applicable litigation hold.

Company Records designated in the applicable schedule as “permanent” shall never be destroyed. To the extent there are conflicts about the period to retain a certain Company

Record, you shall keep it for the longer of the conflicting periods. In no case shall copies of Company Records be retained longer than the designated retention time or otherwise be retained in contravention of any Company Policy.

Drafts of Company Records shall be retained for the applicable period set forth on Schedule A. Should no period be set forth on Schedule A, drafts shall be destroyed no later than six (6) months following completion/submission/execution of the final Company Record.

Disposal of Records shall comply with all applicable legal requirements, including secure destruction of Company Records containing confidential, consumer or health-related information, or personally identifiable information about employees or third parties. Secure disposal of paper documents includes burning, pulverizing or shredding so that the information cannot practicably be read or reconstructed.

### **Litigation Holds**

Destruction of Company Records shall be suspended pursuant to a Litigation Hold as provided in the Company's Litigation Hold Policy. Once Company Records are subject to a Litigation Hold, destruction of any of those Company Records, even inadvertent destruction, may result in severe penalties. Please reference the Litigation Hold Policy for further details. The Company retains the right to report any violations of law to appropriate authorities.

### **Requests for Exceptions**

Requests for exceptions from this Policy shall be submitted to [dataprotection@rpm-inc.com](mailto:dataprotection@rpm-inc.com), with final approval granted by the RPM General Counsel. All requests for exceptions must be supported by evidence that the purpose and basic objectives of this Policy will be met.

**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.**