

RPM INTERNATIONAL INC. REPORTABLE EVENTS POLICY

Purpose

The purpose of this Policy is to ensure that RPM International Inc. (“RPM”) is timely informed about events that could materially impact its business.

Scope

This Policy applies to all employees and events, incidents and matters impacting or affecting RPM or any RPM Subsidiary (the “Company”).

Policy

You have a duty to report all incidents and matters described below impacting, affecting or associated with the Company, or those that are in violation of RPM’s Code of Conduct, The Values and Expectations of 168, or any RPM Policy that does or could otherwise materially impact the Company’s financial condition, cash flows, operations or safety (each a “Reportable Event”) using the [RPM Reportable Events site](#).

Reportable Events shall be submitted within 24 hours after the discovery of the Reportable Event. However, data security and data privacy incidents shall be reported immediately.

The following is a list of examples of Reportable Events that require reporting under this Policy. **Even if an event is not listed below, if there is any doubt as to whether something is material or is otherwise a Reportable Event, you should report it.**

EXAMPLES OF REPORTABLE EVENTS

1. Data Privacy and Data Security Incidents

- The loss or theft of any phone, tablet, laptop, computer, flash drive or any similar type of device with access to or that may contain Company data, whether the device is Company owned or personal.
- Incidents that:
 - i) compromise the security of any information technology system, device, network or physical location that contains or is used to access Company information (ransomware, hacking, unexplained network outage, other unauthorized access or theft); or
 - ii) compromise the privacy or confidentiality of Company or personal data of our associates or third parties (including successful phishing attempts, even if intercepted by IT, it must be reported immediately (even if all facts are not yet known).

- Any event that infects or disables a home or personal wireless network that is used to connect Company devices or access Company data. This would include an unknown disruption to services, notice from a wireless provider that a data breach has occurred, hacking or breach of a device connected to that network, or malicious activity discovered on that network. This does not include events that are due to non-malicious activities, for example, power outages or suspension of services by the provider for non-payment.
- The receipt of a notice of a data breach from a vendor or service provider used by the Company.
- Theft or loss of a device containing Company records or access to Company networks.
- Any unauthorized, inappropriate or accidental disclosure, access, theft, “leak” or compromise of anyone’s personal information that is stored or processed by or on behalf of the Company.

If a data incident includes the unauthorized encryption of any data or device, the theft of confidential or proprietary information, or otherwise results in, or is expected to result in, a disruption to, or lack of availability of, any servers or email communication, then in addition to a Reportable Event filing, you must **immediately** contact: RPM’s Vice President – Global Systems, Mark Rankin at mrankin@rpm-inc.com /330-220-6043 (office)/440-279-3074 (mobile) or RPM’s Senior Director of Information Security, Mike Metivier at mmetivier@rpm-inc.com /330-273-8833 (office)/330-242-6152 (mobile), or InfoSec@rpm-inc.com.

2. Environment, Health and Safety; Accidents; Injuries; Property Damage

- Any accident or incident that results in:
 - hospitalization, death, bone fracture, loss of organ function or body part, burns or permanent disfigurement to any person, (employee or third party) at a Company facility or involving a Company employee or product or;
 - a failure to properly contain, store, transport, discharge or dispose of any chemicals or pollutants.
- Any incident involving a burning fire, smoke proceeding a potential fire, smoldering material, explosion/flashback, or electrical arc flash involving RPM owned/leased property or on project sites involving RPM employees or a company product regardless of size or duration.
- Any environmental testing or remediation activity at an RPM operating company location (leased or owned) requires notification via the Reportable Events Portal and approval before commencement of any work by the RPM Corporate EH&S staff (VP of EH&S -

lbowers@rpm-inc.com or Director of Env. Affairs - mfrushour@rpm-inc.com). This includes but is not limited to:

- Soil and groundwater sampling and/or remediation;
 - Vapor Intrusion sampling and/or remediation;
 - Underground storage tank (UST) extraction;
 - Sediment sampling;
 - Excavation of concrete containment systems, cisterns or associated underground material transfer equipment/systems;
 - Any other remediation or sampling activity that requires notification or approval of a government agency.
- Property loss that, irrespective of insurance recovery or third-party reimbursement, could potentially exceed:
 - \$15,000 if property is located outside of North America; or
 - \$100,000 if property is located in North America.

3. Business Interruption; Loss of Business

- Unexpected disruption or interruption in manufacturing or shipping that exceeds one day.
- Unplanned closure of a Company facility or office.
- Termination or material change to a business relationship that constitutes 10% or more of the reporting Company's sales on an annual basis or is otherwise material to a Company. See [*RPM's Contract Management Policy*](#) for additional reporting requirements.

4. Product Quality Concerns

- Disposal or rework of inventory resulting from safety or regulatory compliance concerns.
- A product "recall" or "call-back."

5. Government Inspections; Inquiries; Investigations; Notifications

- A facility visit, notice of inquiry (written or otherwise), inspection, notice of violation, investigation or other contact from a law enforcement, governmental or regulatory agency, regardless of findings. *Note: The annual local fire code compliance inspection is exempt from reporting unless a violation is noted or communicated during the inspection.
- Receipt of notice of any fine or settlement of any fine issued by a governmental or regulatory agency.
- An event that does or could require notification to a government or regulatory agency.

- Receipt of notice or inquiry from a Non-Governmental Organization (NGO) or Media outlet pertaining to concerns of Environmental, Sustainability, or Human Rights violations by the company or within the company's supply chain.

6. Lawsuits; Claims

- All lawsuits, judgments, notices, fines and claims of any kind, including written demands for refunds, replacements, repairs or other compensation from a customer, end user, or third party or failure to pay from a supplier without lawyers involved (collectively, "Claims"), are Reportable Events **unless**:
 - Served on a Company in the United States through CSC;
 - Filed in any small claims court or for which the potential liability or loss is less than \$25,000 (unless there are 3 or more related Claims);
 - Otherwise sent to Matthew Kucharson, Senior Director of Litigation and Litigation Counsel, at mkucharson@rpm-inc.com or John Fisher, Director of Litigation and Litigation Counsel, at jofisher@rpm-inc.com;
 - An allegation of potential liability (warranty claim) of less than \$250,000 (all warranty claims greater than \$250,000 are reportable events).

7. Violations; Investigations; Policies

- Any intent to investigate any director or officer (or the equivalent) of any Company for any reason.
- Allegations and investigations of any employee regarding fraud, theft, a violation of the Values and Expectations of 168 or employee relations issues that fall into the following categories:
 - Accounting / Audit Irregularities;
 - Bribery/Kickbacks/Improper Payments;
 - Conflicts of Interest;
 - Discrimination;
 - Falsification of Company Records;
 - Fraud;
 - Gifts, Entertainment or Expense Reporting;
 - Harassment;
 - Hostile Work Environment;
 - Improper Loans to Executives;
 - Insider Trading;
 - Release of Confidential or Proprietary Information;
 - Retaliation of Whistleblowers;
 - Sexual Harassment;
 - Theft;

- Trade/Export Control Discrepancy;
- Wage/Hour Issues;
- Workplace Violence/Threats;
- Wrongful Termination;
- Any material violation of an RPM Policy, including but not limited to the “Values and Expectations of 168”.

Investigations must not commence until the Reportable Event has been submitted. If you need support or guidance from the RPM Legal and Compliance Department on how to proceed with the investigation please contact Shelley Earl – searl@rpminc.com or Jessica Bieszczak – jbieszczak@rpminc.com, for Europe please contact Caroline Watson – cwatson@rpminc.com. Please ensure that your reportable event submission provides details such as who, what, where, when and how related to the matter to be investigated and who the investigator will be. If there is concern that the welfare/safety of an employee is at risk, please call your group’s or the RPM Legal and Compliance team immediately to discuss.

8. Business Development

- Entry into a confidentiality agreement, letter of intent or other agreement with respect to any potential acquisition or divestiture transaction which has not received the prior approval of the RPM Corporate Development Department.

9. Human Resources

- Appointment, termination, resignation or retirement of any Company officer, or director or the equivalent.
- Commencement of negotiation of a severance package for any officer or director or the equivalent of a Company. Pursuant to [*RPM's Contract Management Policy*](#), officer and director severance packages must be reviewed by RPM’s Vice President - Corporate Benefits and Risk Management prior to finalizing or executing such agreement.
- Employment agreements for any officer or director or the equivalent, whether or not required by statute, and any other employment agreement not otherwise required by statute, the terms of which have not been previously reviewed and approved by RPM’s Corporate Development Department in connection with an acquisition, Vice President - Corporate Benefits and Risk Management, General Counsel or Associate General Counsel.
- Changes to compensation (salary, bonuses, supplemental benefits or other perquisites) of an officer or director of a Company without the approval of RPM’s Vice President - Corporate Benefits and Risk Management.
- Request by a labor union for information about a location at which it does not presently represent employees of a Company or any notice or posting with respect to an effort to organize employees, works council or otherwise at a location. In addition to the reportable

event filing please provide notice to either Janeen Kastner jkastner@rpm-inc.com or Jessica Bieszczak jbieszczak@rpm-inc.com.

- Commencement of formal negotiations with a labor union or works council with respect to an existing or proposed new or renewed collective bargaining agreement. In addition to the reportable event filing please provide notice to either Janeen Kastner jkastner@rpm-inc.com or Jessica Bieszczak jbieszczak@rpm-inc.com.

10. Credit

- Entry into any third-party credit agreement, loan agreement, promissory note, letter of credit, financial derivative contract or similar financing arrangement or credit extension, without the prior consent of RPM's Corporate Treasury Department.
- Default under any third-party credit agreement, credit facility or other financing or credit extension arrangement including those included in the above bullet point.
- Any guaranty of the debt, financial condition or financial performance of another party, including an affiliate.

11. Trade

- Any shipment of Company goods to or through Iran, Cuba, Russia, Syria, North Korea, Venezuela, the Crimean, Donestsk or Luhansk Regions of Ukraine, Belarus or any other country that is subject to sanctions or an embargo by the United States, the United Kingdom or the European Union.
- Any transaction occurring with an individual or organization identified in the Specially Designated Nationals or Blocked Persons lists issued by the U.S. Department of Treasury's Office of Foreign Asset Control (OFAC) or located in or controlled by an entity in Iran, Cuba, Syria, North Korea, Venezuela, the Crimean, Donestsk or Luhansk Regions of Ukraine, Russia, Belarus or any other country that is subject to sanctions by the United States, United Kingdom or the European Union.
- Unauthorized export or import of a product without the proper license.
- Import of goods produced (in whole or in part) in the Xinjiang Region of China.
- Any agreement that contains boycott language contrary to the U.S.'s anti-boycott laws. For example, agreements that support the boycott of Israel.

How to Report Suspected Violation

A suspected violation of this policy can be reported to your immediate supervisor, Human Resources, or the Legal & Compliance department. Employees are also welcome to contact the Company's [Hotline](#) to report their concerns to RPM. 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 report a Policy violation, 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.