ACCEPTABLE USE OF AND ACCESS TO COMPANY DEVICES, DATA AND TECHNOLOGY POLICY

Purpose

The purpose of this Policy is to define the parameters for the proper use of Devices, Company Data and Company Technology (as defined at the end of this document) in an effort to ensure appropriate use, security and privacy requirements and measures are observed and followed. Additionally, this Policy is meant to set user expectations and clearly identify certain rights that the Company retains with respect to Devices, Company Data and Company Technology.

Scope

This Policy applies to all employees, consultants, contractors, interns, casual or temporary workers and employment agency staff (collectively or along "you" or "your") of any RPM company (collectively the "Company") who are using Devices or Company Technology for business purposes, handling Company Data or using Company Technology unless otherwise provided herein. This Policy applies to your use both during and outside of regular working hours and regardless of location.

Personal Equipment used for business purposes are subject to this Policy to the extent permissible under applicable law. Any use of Personal Equipment for Company business is required to be documented and approved in advance by your IT Department and your manager.

Employees of non-U.S. RPM companies should read this Policy in conjunction with any applicable country-specific addendum for proper application. For the avoidance of doubt, any provision of this Policy that conflicts with applicable local law shall be replaced by the applicable provisions in the country-specific addendum. If no such addendum exists, any conflicting provision of this Policy will be deemed deleted to the minimum extent necessary but shall not affect the validity and enforceability of the rest of this Policy.

Acceptable Use

- You agree to safeguard and maintain all Company Data as confidential where applicable.
- Your use of a Device, Company Data or Company Technology should not negatively affect the Company's reputation.
- You will only use Company Data for the business purposes for which it was intended, and any use for a purpose different from that for which it was originally intended is prohibited.
- You will minimize the amount of Company Data stored on your Devices or approved Personal Equipment by accessing information on Company Technology remotely when possible, and deleting any data saved locally on your Device or Personal Equipment as soon as it is no longer required. Retention of Company Data must comply with the applicable data management or retention policy.

- You understand and acknowledge that we do not provide electronic communication services related to Devices and that those services are performed by third party providers. These third-party providers, which may include AT&T, Verizon or other electronic communications service providers, may collect and use location information from Devices in accordance with their own policies and procedures.
- You acknowledge that by using the Device and connected electronic communication service that you are bound by and agree to such third-party terms, policies and procedures. We encourage you to familiarize yourself with these documents, which can be located on the applicable third-party's website(s).

Uses Requiring Prior Approval

- You may not use public unsecured Wi-Fi to access Company Data without prior approval from your IT department. An example of an unsecured Wi-Fi would be a coffee shop with an open connection that does not require a password. A hotel network protected by a password is not considered unsecured for purposes of this policy.
- You must have a proper license and prior approval from your local IT department to download, install or use software or any copyrighted or trademarked materials on your Device.
- You must have prior approval from your local IT department for the use of any cloud storage applications with respect to Company Data.

Use and Access Security Requirements

- At all times, you must use your best efforts to secure Devices, Personal Equipment, Company Data and Company Technology against unauthorized access, loss, theft or use.
- You must use passwords for all Devices and Personal Equipment and the passwords must be in compliance with RPM's End User Password Policy, which includes the use of 10-character passwords. Passwords must not be shared, and any compromises of passwords must be reported via the Reportable Events Page.
- You must have Anti-virus or anti-malware software installed on any Device or Personal Equipment before connecting to Company Technology or accessing Company Data.
- You must contact your local IT department or issuelog@rpminc.com immediately and complete a Reportable Event form in the event there is a loss or theft of a Device or Personal Equipment or any Company Data in general, or if you suspect that a virus has been introduced into or on a Device, Personal Equipment, Company Technology, or if you click on a suspicious link or open a suspicious document.
- Sensitive Personal Data and other confidential Company Data such as trade secrets, pricing or other proprietary information shall at a minimum be encrypted or password protected when stored and emailed. Document passwords shall not be sent in the body of the email containing the document.
- You should avoid clicking on unsolicited or junk electronic communications ("spam") and suspicious links whether in email, text or any other form as these are often spam and can contain viruses. Seek assistance from your local IT help desk or

issuelog@rpminc.com if you have any concerns about the legitimacy of any electronic communications.

Use and Access Prohibitions

- Your Device is assigned to you and should not be used by others.
- You may not store Company Data on, upload or back-up Company Data to any unencrypted or unprotected flash drive or hard drive. Any such existing copies must be deleted immediately.
- You may not use your Personal email addresses to conduct Company business or store or process Company Data (including for convenience to print a document) without prior written approval.
- You may not alter or tamper with any Company Technology security or administrative controls or settings.
- You may not conduct illegal activity on, through or by using any Device or Company Technology.
- You may not use Company Technology, Company Data and Devices to solicit non-company business for personal gain or profit or for any other illegal purpose.
- You may not use Devices and Company Technology to visit Internet sites that contain Objectionable Content.
- You may not use Company Technology for storing, displaying, sending or receiving Objectionable Content; annoying, harassing, or intimidating another party; or making or posting indecent remarks, proposals or materials.
- You may not post personal opinions or content in such a way that it could be construed to be associated with, endorsed by or interpreted to be the opinion of the Company.

Company Rights

To protect Devices, Company Technology and Company Data from unauthorized loss, disclosure, access, destruction or alteration, the Company may

- Monitor your use of Company Technology;
- Access your Device or Personal Equipment in accordance with this Policy; and
- Review information or activities contained on the Device, Personal Equipment or performed while using Company Technology.

The Company reserves the right to intercept, access, inspect, review, copy, delete and/or disclose all information and messages sent over, using or stored on its Devices or Company Technology in accordance with applicable Company policies and law. Devices, Company Data and Company Technology are and remain the property of the Company.

The Company may immediately remove access to Devices, Company Technology and, where appropriate, remove any Company Data, including any Company-related Personal Data from a Device or Personal Equipment if a breach of this policy, or a security incident have occurred or are reasonably suspected. The Company reserves the right to wipe or clear Company Data from any device, including Personal Equipment, or Company Technology, which may include

the deletion or loss of non-Company information Personal Data, pictures and other media; and to limit or deny an individual access to, or use of Devices, Company Technology or Company Data, regardless of the mode by which such data is accessed, at any time and for any reason. However, the Company will only monitor, intercept or review activity to the extent permitted by law and to comply with Company policy, a legal obligation or for legitimate business purposes, including, without limitation, in order to:

- prevent misuse and ensure proper operation of the Device or Company Technology and protect Company Data;
- ensure compliance with law, regulations, or our rules, standards of conduct and policies in force from time to time (including this Policy); and
- ensure that Company Technology or Devices are not used for any unlawful purposes or activities that may damage our business or reputation.

Definitions

"Company Data" means data, materials, communications and information, such as email, voicemail, documents, files, instant messages, internet and social media postings, that are created, transmitted, received, distributed, stored or recorded during the course of employment or while performing business related tasks

"Company Managed" means under the organizational control of the Company

"Company Technology" means Company owned or provided internet/intranet access, networks, websites, applications, social networking platforms, e-mail, file sharing or storage platforms, telephone and video conferencing services

"Devices" means Company-managed computers, laptops, smartphones and tablets

"Objectionable Content" means obscene, derogatory, hateful, threatening, defamatory or other objectionable content

"Personal Data" means information that identifies or relates to natural persons

"Personal Equipment" means a personal mobile device or computer to access, process, store Company Data or interface with Company Technology

"Sensitive Personal Data" means Personal Data that is sensitive in nature or is considered a special category of data including, but not limited to, personal identification numbers, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric or genetic information; or information about a person's health, sex life or sexual orientation; or employee performance data, financial or banking data

Violations

Any employee who violates this Policy or any applicable addendum to this Policy or who directs or who knowingly permits a subordinate to violate a Company Policy or addendum may be subject to disciplinary action up to and including termination.

How to Report Suspected Violation

A suspected violation of this policy can be reported to a supervisor or the Human Resources, Legal and/or Compliance departments. A suspected violation may also be reported via the internet with the Company's Third-Party vendor by using the Hotline Online.