Bring Your Own Device (BYOD) Policy

Purpose

The purpose of this policy is to define acceptable practices, responsibilities, and procedures for those who access Company data, applications, systems, software, and networks ("Company resources") using personal or non-company owned mobile or computing devices, including laptops, mobile phones, smartphones, tablets, and PCs (each a "Personal Device").

Scope

This Policy applies to all employees, consultants, contractors and temporary workers of RPM International Inc. and its subsidiaries (collectively "RPM" or the "Company") who use a Personal Device to access Company resources.

All Company BYOD Programs are subject to approval by RPM and the respective Group IT Department.

The use of Personal Devices that are "jailbroken", "rooted", or have been subjected to any other method of altering or disabling built-in protections or compromising the operating system in any way, are not permitted when accessing Company resources.

By using a Personal Device to access Company resources, you acknowledge that you have read this document and understand the Company's rights and your responsibilities.

Use of a Personal Device to access Company resources is voluntary, subject to approval, and by no means constitutes a request by Company, direct or implied, to conduct business on your Personal Device outside of predetermined and regularly scheduled business hours. If a mobile or computing device is required for your role with the Company, you may contact your local IT department for your mobile and/or computing device options.

By using a Personal Device to access Company resources, you acknowledge and agree to the following:

- You may not use a Personal Device to access Company resources that is not approved by the Company IT department.
- Prior to using a Personal Device to access Company resources you will contact your local IT department who will assist you with the enrollment process.
- You will allow IT to load and set the standards for Company resources onto your Personal Device upon reasonable request. Security standards as of the date of issuance of this policy are listed in Appendix A and are subject to change without notice.
- You may be asked to promptly, and without alteration, bring or send your Personal Device(s) to the Company IT Department upon notification that it is needed for discovery or other litigation purposes.
- Your Personal Device may be remotely wiped by IT, when necessary, as may be solely determined by the Company. This may result in the destruction of your personal data and information stored on the Personal Device.

- You are solely responsible for separately backing up any personal content on your Personal Device. Company will in no way be responsible for damaged, lost, or stolen Personal Devices or any personal content on them.
- You will keep your Personal Device updated and in good working order.
- You will not use unapproved messaging apps on any device to send business communications.
- All business communications are the property of the Company and you acknowledge that you have no right or title to those business communications. You must retain business records and Company information in accordance with the Company's record retention obligations, including those conducted through approved instant messaging and other applications.
- You are only allowed to access Company resources using two Personal Devices at any given time.
- The Company's End User Password Policy including policy elements such as passcode, passcode timeout, passcode complexity and encryption will be enforced on your Personal Device.
- You will take appropriate precautions to prevent others from obtaining access to your Personal Device and will not provide access credentials including assigned passwords, PINs or other credentials for your Personal Device to any other individual or business.
- You will be responsible for all transactions and interactions made with your credentials.
- You will not backup or restore any Company resources that originated through or were a product of the relationship or employment with the Company without prior Company authorization. Any attempt to backup or restore such information may subject you to legal action.
- You will certify/confirm the removal of all Company resources stored on your Personal Device(s) immediately in the event your relationship with the Company ends.
- Upon loss or theft of your Personal Device, you will submit a report through the Reportable Events Portal or by calling the helpdesk. In such event, your Personal Device may be remotely wiped, in an effort to mitigate any potential risk to Company resources.
- The act of remotely wiping data from your Personal Device does not cancel any services or subscriptions related to your Personal Device or applications installed on it for which You will remain responsible.
- You may download and install applications to your Personal Device only from the trusted public application stores listed below:
    - Apple – Apple App Store
    - Android – Google Play Store

  - Windows – Windows Store
  - Amazon – Amazon App Store

- Only approved applications may be utilized for conducting Company business. If you have any question about whether a particular application is approved for Company use, contact your local IT department or the RPM Information Security team at Infosec@rpminc.com.

- The Help Desk is not able to provide support related to Personal Device replacement or upgrade, nor is it able to provide support with respect to embedded software unrelated to the Company.

- Any exceptions to this Policy will be determined by and should be routed to the Information Security Department at InfoSec@rpminc.com and are approved by the RPM Information Technology Department.

In the event you have questions or concerns related to the application or use of this Policy you may contact the information security department at Infosec@rpminc.com or the RPM Legal and Compliance department by emailing Dataprotection@rpminc.com.

The Company may, at any time and at its discretion, modify or discontinue this Policy. Continued use of your Personal Device to access Company resources signifies your acceptance of any such changes.

Violations of this Policy may result in termination of your eligibility to use a Personal Device to access Company resources and may subject you to potential disciplinary actions, up to, and including, / termination of employment/relationship with Company.

How to Report Suspected Violations

A suspected violation of this policy can be reported to your immediate supervisor, Human Resources, or the Legal & Compliance department. Employees may also use 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.

APPENDIX A: Security Criteria for Personal Devices accessing Company resources

All Personal Devices connecting to or accessing Company resources must meet the following security criteria:

- All Personal Devices must be on the latest operating system version within three months of release.
- All users must select strong passwords and change passwords in accordance with the RPM password management policy.
- All Personal Devices must be configured with a minimum password length of ten characters.
- All Personal Devices must be secured with a password-protected screensaver and must be configured to automatically lock after a predefined period of inactivity.
- All Personal Devices must be managed by one of the following two options, each of which must be approved in advance by the RPM IT Department:
    - A Mobile Device Management (MDM) tool; or
    - A Mobile Application Management tool.
- In the event the Personal Device is managed by a MAM, all access to Company resources and processing of Company related business information must be authorized by the MAM tool.
- Certain Personal Devices such as laptops and PCs require antivirus with updated signatures. Antivirus platforms should be from a known reputable vendor such as Trend, Sophos, Symantec, Bitdefender and Norton.