Effective October 6, 2022

End-User Mobile Device Management Notice

Purpose

The purpose of this Policy is to provide transparency around the types of information collected through the Company's mobile device management (MDM) software and set forth parameters for personally owned devices enrolled in the Company MDM program.

Scope

This Policy applies to the MDM provider and RPM International Inc.'s and its subsidiaries' ("RPM") MDM program.

I. Data Collected by and through the MDM

While the specific software provider may change from time to time, the MDM provider remains a third-party provider of technology services and has documented technical security measures designed to protect information collected via mobile devices.

When users enroll device(s) with the MDM; the MDM provider collects, processes and shares data derived from enrolled mobile devices with RPM to support its business operations and conduct legitimate data security functions in line with RPM's Acceptable Use Policy and respective Employee Privacy Policies.

Information may be collected from the following sources:

- The Microsoft Endpoint Manager admin center (administered by employees of RPM).
- End-user devices (during usage), including:
  - Customer account existence at third party services (no collection of passwords).
  - Security monitoring information,
  - Diagnostic, performance, and usage information.

We will never see or have access to:

- An end users' calling or web browsing history
- Information entered into a website through a web browser
- Text message content
- Contact lists saved to the device or a personal application
- Passwords used to access personal accounts
- Calendar data saved to the device or a personal application
- Photos, including those in a photo application or your camera roll.

Information that is collected by or through the MDM falls into two categories: "required" and "other", described more fully below. Each category may include customer data, personal data, diagnostic data, and/or service-generated data.

Required Data

Required data consists of information that is necessary to use the service and achieve RPM's legitimate business interests in securing its data and property. Required data may be tied to a user, device, or application and is essential to make use of the MDM. Required data may contain both personal data and non-personal data.

Personal Data Collected

Personal data includes information that may directly or indirectly identify the end user and pseudonymized data with a unique identifier generated by the system.

Non-Personal Data Collected

Non-personal data includes service-generated system metadata and organizational/tenant information. RPM, through the MDM provider, also collects access control data to manage access to administrative roles and functions through features like role-based access control.

The following is a list of specific data types routinely collected by or through the MDM:

Category	Data Type
Access Control Information	Privacy keys for certificates
	Static authenticators (customer's password)
Admin and account information	Active Directory ID of each customer IT admin
	Admin user first name and last name
	Admin username
	Email address of account owner
	Payment data for customer billing
	Phone Number
	Subscription Key
	UPN (email)
Admin Created Data	Compliance Policies
	Group Policies
	Line-of-Business (LOB) application
	PowerShell scripts
	Profile names
Application Inventory	App ID
	App Name
	Installation Location
	Size
	Version
Audit log information, including data about the following activities	Information related to any action within the system including but not limited to assigning, creating, deleting or managing access, performance of remote tasks and any updates to an account.

Device Data	Account ID
	Apple ID for iOS/iPadOS devices
	Azure Active Directory Device ID
	MDM Device ID
	Device Storage Space
	EAS device ID
	MDM device management ID
	Data related to the location of the device
	Mac Address for Mac devices
	Network Information
	Platform-specific IDs
	Tenant ID
	Windows ID for Windows devices
Hardware Inventory Information	Device Name
	Device Type
	ICCID
	IMEI Number
	IP address
	Manufacturer
	Model
	Operating System
	Operating System version
	Serial Number
	Wi-Fi Mac Address
Managed Application Information	Azure Active Directory Device ID
	Device Enrollment Status
	Device Health Status
	Encryption Keys
	MDM Device Management ID
	Last application check-in date/time
	Managed application device tag
	Managed application ID
	Managed application SDK version
	MAM enrollment data/time
	MAM enrollment status
Support Information	Business contact information (name, phone number, email address)
	Email discussions with Microsoft support, product, and/or customer experience team members
Tenant Account Information (this data is available from the Microsoft Endpoint Manager Admin Console)	InstalledDeviceCount: The number of devices on which the application is installed

	Number of devise or users enrolled
	Number of identified device platforms
	Number of installed devices
	notApplicableDeviceCount: The number of devices for which the application is not applicable
	notInstalledDeviceCount: The number of devices for which the application is applicable, but not installed
	pendingInstallDeviceCount: The number of devices for which the application is applicable, and installation is pending
End-User Personal Data	Owner name/user display (the Azure-registered name of the user as identified by AzureUserID)
	Phone number associated with the device
	Third-party user identifies (like AppleID)
	User principal name or email address

<u>Other Data</u>
The MDM may also collect other data including:

- Device health monitoring including:
  - Endpoint Analytics: RAM Utilization, Processor Load, and Disk Usage
  - Windows Updates to determine whether a device is ready for a feature update.

II. Personal Devices

Under certain circumstances an End-User may be permitted to use a personal device for Company business under a bring your own device (BYOD) policy. Devices used to access Company information under a BYOD policy are required to be enrolled with the MDM.

Enrolling a device with the MDM will make information, such as device model and serial number, visible to IT administrators and support personnel with administrator access.

i. RPM will have access to the following data on an MDM enrolled personal device:

- Device owner
- Device name
- Device serial number
- Device model, such as Google Pixel
- Device manufacturer, such as Microsoft
- Operating system and version, such as iOS 12.0.1
- Device IMEI

- The last four digits of the phone number associated with the personal device
- App inventory and app names, such as Microsoft Word
    - RPM will only see your managed app inventory, which includes work apps.
- RPM cannot view the location of a personal device.

ii. Other Information obtained from Personal Devices

- Under certain circumstances, RPM may see and access certain aspects of a device when assisting with or troubleshooting device setup. This type of access will be triggered by a request from the End-User for technical support. If technical support needs to remote onto the device to provide the required support; he/she may see information on that device if the owner has any files or window open during the remote session.
- RPM may access storage size information to find out if low space is causing issues installing a required app

In the event you have questions or concerns related to the application or use of this Policy you may contact the Information Security Team at infosec@rpminc.com or the RPM Legal and Compliance department by emailing dataprotection@rpminc.com.

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 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.