END USER PASSWORD POLICY

WHY HAVE AN END USER PASSWORD POLICY FOR RPM AND SUBSIDIARY EMPLOYEES?

Proper passwords reduce the risk of a breach of RPM and your company's systems, network(s) or data ("Company Data") and help ensure proper protection of such data.

WHAT ARE THE PASSWORD REQUIREMENTS?

End users are required to use a 10-character minimum password to access all Company owned computers, cell phones and tablets (each a "device"). Further, end users are required to use a 10-character password on all phones, watches, tablets, applications, websites, systems, accounts, documents and emails that access, store or are used to transmit confidential Personal Data (as defined in the RPM Global Data Protection Policy) or other Company confidential data (collectively, "Confidential Company Data") whether or not Company owned. If a password of at least 10 characters is not permitted, you must use the maximum length permitted. The Company reserves the right to change password requirements and to require end users to change passwords at any time and for any reason. Exceptions, other than as detailed above due to inherent system limitations, must be approved by your IT department. Note that a biometric replacement for a password (such as fingerprint, iris, or facial recognition) is permitted.

Contact your IT department with any questions regarding this policy or if you need assistance changing any password to comply with the terms hereof.

This policy applies to all RPM and RPM subsidiary (collectively, the "Company") end users. Any employee who violates this Policy may be subject to disciplinary action up to and including termination.

PASSWORD MANAGEMENT AND STORAGE TIPS

- Do not use well-known or publicly posted information
- Do not use a single 10-character word such as "mozzarella" or "expectancy" or an easily identifiable string such as "abcdefghijk" or "1234567890"
- Use a combination of words and/or numbers and symbols to create a unique password
- Choose an easy-to-remember password that would be hard for someone else to guess like "swordfishisgood," "iliker0wing!," "@housefriendtreestone," or "G00dVibes!"
- One common password tactic is to use the site or application name with a common secondary word. For example, your email password might be "OutlookC00king!" and your Facebook password might be "FacebookC00king!"
- Do not use your login name or user ID or any variation thereof as your password
- Your passwords should not all be the same
- Do not share passwords
- Do not transmit passwords through an unsecure method such as email
- Do not write down, record or store passwords with corresponding account information or usernames unless secured through password protection, encryption or other reasonable means