RampedUp BYOD Policy

The purpose of this Bring Your Own Device (BYOD) policy is to establish guidelines and procedures for the use of personal devices at RampedUp. This policy aims to balance the benefits of using personal devices for work-related purposes while maintaining security, confidentiality, and productivity within the organization.

This policy applies to all employees, contractors, and any other personnel who may access RampedUp information or resources using their personal devices. Employees may use their personal devices (smartphones, laptops, tablets, etc.) for work-related tasks if they meet the minimum-security requirements outlined by the company's IT department.

- Personal devices must have the latest operating system and security updates installed.
- Devices must have a password, PIN, or biometric security feature enabled for access.
- Employees must install and maintain up-to-date antivirus/anti-malware software.
- RampedUp does not require any company or customer data to be stored on personal devices. All data storage is through our cloud hosting tools.
- Employees are held responsible for the security and confidentiality of company data on their personal devices.
- Personal devices should not be used to store highly sensitive company information.
- Employees must report any lost or stolen devices, security breaches, or unauthorized access to company information on their personal devices immediately to the IT department.
- RampedUp reserves the right to monitor and manage any device connected to its network for security and compliance purposes in which case we use Miradore MDM software.
- Non-compliance with this policy may result in the revocation of BYOD privileges and potential disciplinary actions.