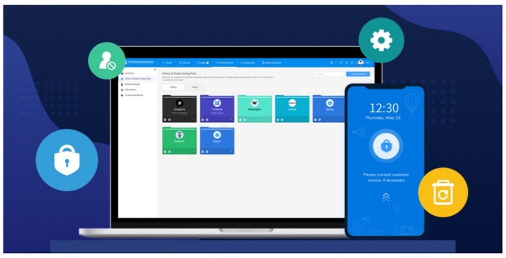

verizon MDM Policies Best Practices Instructions

Home » Verizon » **verizon MDM Policies Best Practices Instructions**

MDM Policies Best Practices Instructions

MDM Policies Best Practices

MDM Policies
Best Practices
Guide to crafting a strong
mobile device management (MDM) policy

- **Enforce software updates**
  Ensure that users follow this crucial security requirement, as updates often contain patches for vulnerabilities that could be exploited by bad actors.
- **Allow only approved applications**
  Make sure that installed applications meet certain security standards, to provide better control over your device environment and minimize potential threats.
- **Install mobile threat defense (MTD) software**
  Help detect and prevent malicious activities, including malware, ransomware and phishing attacks with software that evaluates and mitigates threats as they are encountered.

- **Require lock screen passcodes**
  Help prevent unauthorized access to devices, to aid in safeguarding of sensitive information.
- **Schedule regular password expirations**
  Mitigate the risk of unauthorized access through compromised passwords.
- **Restrict password sharing**
  Limiting shared passwords helps avoid the risk of unauthorized individuals gaining access to your personal or business data.
- **Require two-factor authentication**
  Add an extra layer of security to your online accounts by requiring a second form of verification, to reduce the risk of unauthorized access even if your password is compromised.
- **Set block/allow application lists**
  Block or allow certain applications to help create a safer, more efficient and controlled digital environment.
- **Enforce acceptable use policies (AUP)**
  Create and enforce AUP to promote a secure, compliant, and productive environment within your organization.
- **Set up remote access**
  Help enhance workplace flexibility, productivity and resilience, while supporting talent management strategies and potential cost savings.
- **Disable factory reset**
  Contribute to a more secure and managed device environment by preventing factory reset of your devices, to enhance data security, theft prevention, corporate compliance and control policies.
- **Distribute workforce apps through private stores**
  Help improve security, customization, management, deployment and compliance by utilizing private stores dedicated to workforce apps.
- **Create a sandbox environment or secure container**
  Enhance security, testing, data protection, resource management, and application compatibility in mobile environments.

It shouldn’t take a compromise to step up your game.
Read the Rise of Social Engineering and Cost of Personal Devices: A Security Perspective white paper at
verizon.com/business/resources/whitepapers/the-rise-ofsocial-engineering-and-the-cost-of-personal-devices.pdf

Learn more.
Contact your Verizon Business Account Manager to discover how Verizon can help protect your business.
www.verizon.com/business/products/security/mobiledevice-endpoint-security/

verizon business

Documents / Resources

MDM Policies Best Practices

Guide to crafting a strong mobile device management (MDM) policy

- □ **Enforce software updates**
  Ensure that users follow this crucial security requirement, as updates often contain patches for vulnerabilities that could be exploited by bad actors.
- □ **Allow only approved applications**
  Make sure that installed applications meet certain security standards, to provide better control over your device environment and minimize potential threats.
- □ **Install mobile threat defense (MTD) software**
  Help detect and prevent malicious activities, including malware, ransomware and phishing attacks with software that evaluates and mitigates threats as they are encountered.
- □ **Require lock screen passcodes**
  Help prevent unauthorized access to devices, to aid in safeguarding of sensitive information.
- □ **Schedule regular password expirations**
  Mitigate the risk of unauthorized access through compromised passwords.
- □ **Restrict password sharing**
  Limiting shared passwords helps avoid the risk of unauthorized individuals gaining access to your personal or business data.
- □ **Require two-factor authentication**
  Add an extra layer of security to your online accounts by requiring a second form of verification, to reduce the risk of unauthorized access even if your password is compromised.
- □ **Set block/allow application lists**
  Block or allow certain applications to help create a safer, more efficient and controlled digital environment.
- □ **Enforce acceptable use policies (AUP)**
  Create and enforce AUP to promote a secure, compliant, and productive environment within your organization.
- □ **Set up remote access**
  Help enhance workplace flexibility, productivity and resilience, while supporting talent management strategies and potential cost savings.
- □ **Disable factory reset**
  Contribute to a more secure and managed device environment by preventing factory reset of your devices, to enhance data security, theft prevention, corporate compliance and control policies.
- □ **Distribute workforce apps through private stores**
  Help improve security, customization, management, deployment and compliance by utilizing private stores dedicated to workforce apps.
- □ **Create a sandbox environment or secure container**
  Enhance security, testing, data protection, resource management, and application compatibility in mobile environments.

It shouldn't take a compromise to step up your game.

Read the Rise of Social Engineering and Cost of Personal Devices: A Security Perspective white paper at verizon.com/business/resources/whitepapers/the-rise-of-social-engineering-and-the-cost-of-personal-devices.pdf

Learn more.

Contact your Verizon Business Account Manager to discover how Verizon can help protect your business. www.verizon.com/business/products/security/mobile-device-endpoint-security/

verizon business

verizon MDM Policies Best Practices [pdf] Instructions
MDM Policies Best Practices, Policies Best Practices, Best Practices

References

- **User Manual**

Manuals+, **Privacy Policy**

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.