5 TIPS for Guest BYOD Use

If your midsize company welcomes guests and their mobile devices, read on!

1 POLICY

Create a BYOD policy for all users, including guests.

When creating a bring-your-own-device (BYOD) policy, consider the following:

- Who can connect to your network?
- What devices can connect to your network?
- What access levels and restrictions are needed to manage services and data? Will access be based on job title, user, or device type?
- What compliance regulations must be met, such as Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI)?

Additional Resources

Webinar: Meraki Secure BYOD and Guest Access
Register Now

At-A-Glance: Cisco Unified Access - The Intelligent Platform for a Connected World
Learn More

2 ACCEPTABLE USE

Create an acceptable use policy for BYOD management.

Work with your legal department to create an acceptable use policy that employees and guests can read before connecting to your wireless network.

- Consider adding the policy to your company's employee handbook.
- Define employee and guest usage of personal devices on the network.
- Document acceptable BYOD procedures when connected to the company network, and when accessing company data.

3 GUEST MANAGEMENT

Identify who, where, and what for guest users.

Define the term "guest" in your BYOD policy.

- Do guests include visitors, contractors, auditors, board members, partners, customers, and others?
- Does guest access also apply to employees' personal devices that are not company owned, or will these devices be on-boarded using BYOD?
- What is the total number of guests that your network can support?
- How will guests connect to the network?
- What services and applications will guests be authorized to access?

4 ON-BOARDING

Manage identities and control devices.

Proactively oversee employee and guest connections to your wireless network.

- On-boarding: Policies and limits need to be applied to devices and users to manage access to network resources and applications based on job titles, roles, or devices.
- Off-boarding: Policies should be in place to uninstall applications and restrict or block network access for selected devices on demand.

5 MOBILE DEVICE MANAGEMENT

Integrate management or add a management module.

Look for a wireless network that includes management so you can easily:

- Deploy applications, secure devices, and manage device access.
- Generate reports on-demand or automatically.
- Lock accounts, devices, or users when needed.
- Wipe business data, information, and applications from devices that are lost, stolen, or owned by employees that have left the company.

CISCO

It's not what we make;
it's what we make possible.

Learn how we can help you grow your business.

Visit our Midsize Website