A Checklist for BYOD in the Enterprise

Ready or not, bring-your-own-device (BYOD) is here to stay. And enterprise IT must determine if it's a valuable strategy for their organization, as well as the most effective approach for its implementation, management and long-term growth. Use the following checklist as a guide in determining the right BYOD strategy for your environment.

USERS

Understand which employees are interested in/would benefit from utilizing BYOD, and develop their list of specific needs.

- ❑ For which business functions and processes might they use BYOD?
- ❑ Are user needs limited to email, or do they extend to mission-critical systems and applications?

DEVICES

Today's market offers a wide selection of mobile devices and operating systems. Get employees and enterprise IT on the same page by determining which will be allowed into your environment.

- ❑ Which devices do your employees want? Which devices will your organization allow?
- ❑ What are the unique security and management characteristics of these platforms? Can those features be leveraged in your environment? Are there any security features that can or cannot be enforced?
- ❑ What constraints should enterprise IT implement and enforce?

APPS AND SERVICES

Many apps and services leave devices vulnerable to external threats. Understand which apps and services will be necessary for workers to conduct business, and set guidelines for users so they know which apps may put at risk the corporate data on their devices.

- ❑ Which apps may currently be in use by both the business and the users, and which may soon be added (either by users or the organization)?
- ❑ Can you identify and block any risky apps?
- ❑ Which cloud-based storage services may currently be in use? Which cloud-based services will be allowed (if any) in the future?

INFRASTRUCTURE

Ensure resources—for both IT and users—are well managed by determining how BYOD will be supported and monitored within your organization.

- ❑ Will you support BYOD with full-time IT staff, newly hired, dedicated resources and/or via managed services?
- ❑ Will you manage BYOD centrally (e.g., a dedicated console and system to manage policies and all of the devices from one location) or use a decentralized approach (e.g., push out per-device policies via smartphone utility configurations)?
- ❑ How will you provide secure mobile access to internal systems where required?

Apple-ization of the Enterprise

enterpriseappleization.com | @appleization

Brought to you by Code42.

A Checklist for BYOD in the Enterprise

SECURITY

The ability to secure incoming devices and protect corporate data is one of the biggest concerns for enterprise IT. Be sure to address IT's security concerns before allowing users the freedom and flexibility of BYOD.

- ❑ How do you prevent and remove malware from BYOD devices?
- ❑ To which rules and regulations must you comply?
- ❑ Will users co-mingle personal and company data?

It's important to remember that the answers to the above will help shape and drive the decision regarding the devices and apps supported in your environment; the resulting BYOD strategy should serve both long- and short-term needs and goals for the business. As important, ensure your BYOD strategy enables (not restricts) your workers.