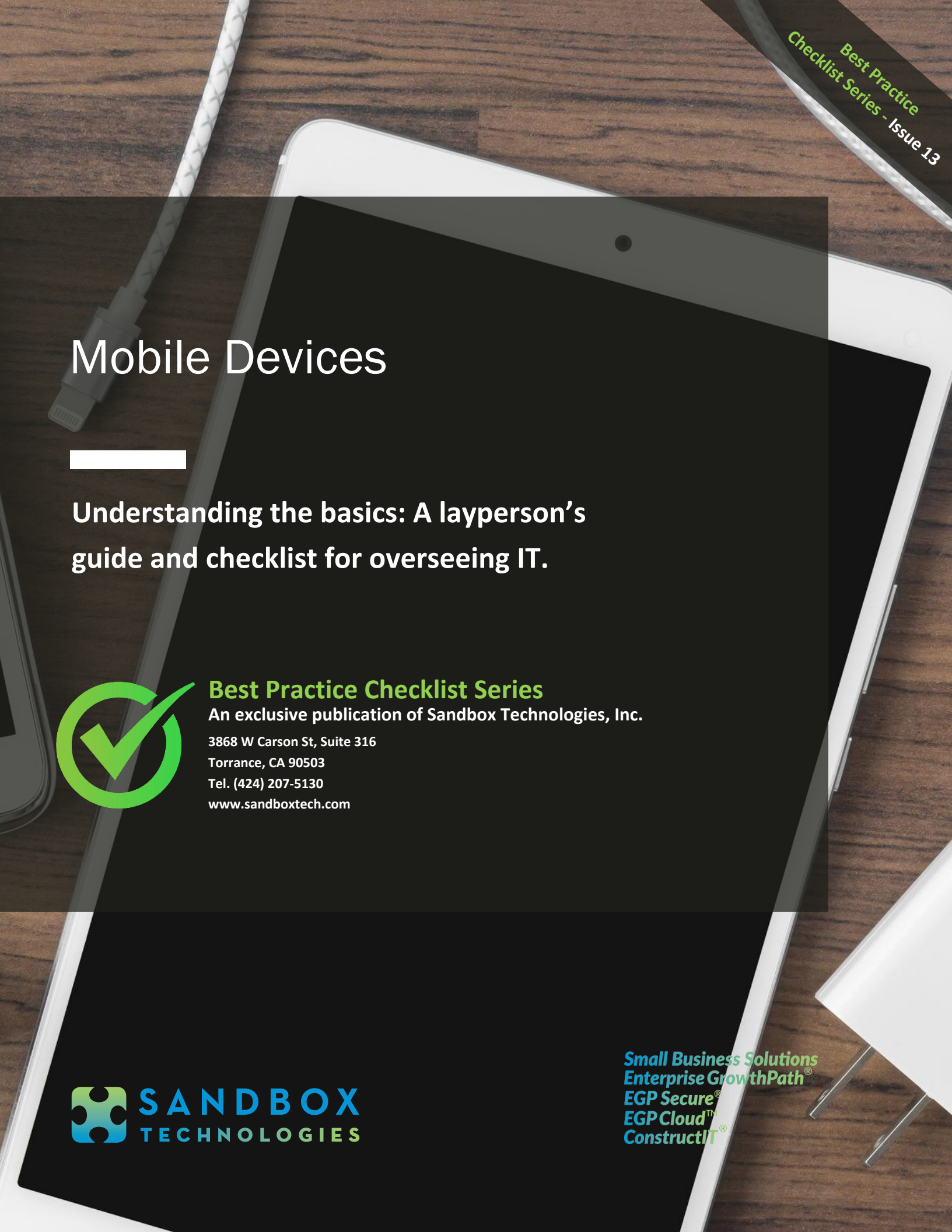


Best Practice Checklist Series - Issue 13

Mobile Devices

Understanding the basics: A layperson's guide and checklist for overseeing IT.

Best Practice Checklist Series
An exclusive publication of Sandbox Technologies, Inc.

3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Mobile Devices

Mobile devices have become an essential business tool for many organizations, however best practices for their deployment and security are often neglected.

In this issue, we'll cover basic recommendations governing the use of mobile devices in business environments. In some cases, particulars may vary from one business to the next. Should you wish to discuss your mobile device practices, your Sandbox Technologies Engineer, Account Manager, or Consulting CIO will be happy to answer any questions you may have.

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Table of Contents

Recommended Practices 4

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Recommended Practices

Company Owned and Controlled Devices

Does the organization allow only company owned and controlled devices to connect to company systems or be used in connection with company business?

Although some organizations may opt to allow the use of employee-owned devices for business purposes (sometimes referred as “Bring Your Own Device” or “BYOD” practices), it is recommended that for the best protection of the company, only the use of devices owned, managed and subject to the its full legal control be permitted.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

BYOD Device Agreements

Although only the use of company owned devices is recommended, if the organization allows the use of other devices, have “Bring Your Own Device” or “BYOD” agreements been obtained governing the use of such devices?

As binding legal documents, BYOD agreements should only be drafted and/or implemented by a qualified legal professional. For reference purposes only, Sandbox Technologies clients may request a sample BYOD agreement to familiarize themselves with what to expect.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Require Approval Prior To Allowing Devices to Connect

Has the organization taken measures to restrict even authorized users from accessing email and other systems via mobile devices without intervention from IT?

In environments using Microsoft Exchange Servers or Microsoft 365 for email hosting, ActiveSync (the mechanism used for communication with mobile devices) by default permits anyone with a valid username and password to connect a mobile device to the associated mail host. Hackers often exploit this vulnerability to circumvent multi-factor authentication protections, because said protections do not apply to mobile devices. When using either of the aforementioned platforms, it is a recommended practice to enable a feature known as “ActiveSync Quarantine”, which requires an authorized administrator to electronically approve new mobile devices before they are permitted to connect.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Mobile Device Management (MDM) Functions

Does the organization have a suitable solution in place for the remote management of mobile devices?

In the event of a mobile device loss, unmanaged devices are at risk of being compromised, leading to the exposure of sensitive data. Unmanaged mobile devices also represent an area of potential exposure for organizations in the event personnel issues arise.

Email/collaboration solutions like Microsoft Exchange and Microsoft 365 provide built-in MDM functionality capable of meeting most organizations' MDM needs at no added cost. Occasionally, companies requiring more robust MDM functionality opt to implement one of several stand-alone solutions on the market. Examples of MDM functions include remote locking capabilities, remote data wiping capabilities, mandatory PIN/password enforcement, data encryption, device encryption, software policies & installation restriction capabilities, and GPS tracking.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Secure Messaging

Does the organization employ an encrypted platform for messaging purposes?

In addition to email, many users make use of mobile messaging platforms to communicate for work purposes. There is a common misconception that such platforms are in some way more secure than corporate email; however, the reality is often quite the opposite. A false sense of security often leads to users transmitting sensitive information (passwords, client data, etc.) via these platforms. It is recommended that companies adopt a standardized platform for secure messaging.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

International Travel

Does the organization maintain policies governing the acceptable use of mobile devices while traveling outside of the United States?

Malicious actors can often embed malware into a mobile device when a user unknowingly roams onto a compromised mobile network, or connects to an unsecured Wi-Fi network. Travel to nations classified as hostile by the U.S. State Department can be particularly challenging. When such travel is necessary, the use of temporary mobile devices that are subsequently destroyed or indelibly marked for use only during return travel to that nation is recommended.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Encrypted Calling Platform for Use Abroad

Does the organization require the use of an encrypted voice calling platform while traveling abroad?

Similar to the previous checklist item, travelers within hostile nations may be exposed to a higher risk of intercepted voice calls. Information obtained may be used to exploit network resources, commit identity theft, fraudulently initiate financial transactions, sell corporate secrets, or even commit blackmail.

It is recommended that an encrypted calling service be implemented for use when traveling outside the U.S., and particularly within nations classified as hostile by the U.S. State Department.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

© 2021, All Rights Reserved. Sandbox Technologies, Inc.