

# Mobile Device Security:

## Bring Your Own Device (BYOD)

---

**Volume A:**  
**Executive Summary**

**Kaitlin Boeckl**

**Nakia Grayson**

**Gema Howell**

**Naomi Lefkovitz**

Applied Cybersecurity Division  
Information Technology Laboratory

**Jason Ajmo**

**Milissa McGinnis\***

**Kenneth F. Sandlin**

**Oksana Slivina**

**Julie Snyder**

**Paul Ward**

The MITRE Corporation  
McLean, VA

*\*Former employee; all work for this publication done while at employer.*

November 2022

SECOND DRAFT

This publication is available free of charge from

<https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device>



# 1 Executive Summary

2 Many organizations provide employees the flexibility to use their personal mobile devices to perform  
3 work-related activities. An ineffectively secured personal mobile device could expose an organization or  
4 employee to data loss or a privacy compromise. Ensuring that an organization's data is protected when  
5 it is accessed from personal devices poses unique challenges and threats.

6 Allowing employees to use their personal mobile devices for work-related activities is commonly known  
7 as a bring your own device (BYOD) deployment. A BYOD deployment offers a convenient way to  
8 remotely access organizational resources, while avoiding the alternative of carrying both a work phone  
9 and personal phone. This NIST Cybersecurity Practice Guide demonstrates how organizations can use  
10 standards-based, commercially available products to help meet their BYOD security and privacy needs.

## 11 CHALLENGE

12 BYOD devices can be used interchangeably for  
13 work and personal purposes throughout the  
14 day. While flexible and convenient, BYOD can  
15 introduce challenges to an enterprise. These  
16 challenges can include additional  
17 responsibilities and complexity for information  
18 technology (IT) departments caused by  
19 supporting many types of personal mobile  
20 devices used by the employees, enterprise  
21 security threats arising from unprotected  
22 personal devices, as well as challenges  
23 protecting the privacy of employees and their  
24 personal data stored on their mobile devices.

---

***An ineffectively secured personal mobile device could expose an organization or employee to data loss or a privacy compromise.***

---

## 25 SOLUTION






26 The National Cybersecurity Center of Excellence (NCCoE) collaborated with the mobile community and  
27 cybersecurity technology providers to build a simulated BYOD environment. Using commercially  
28 available products, the example solution's technologies and methodologies can enhance the security  
29 posture of the adopting organization and help protect employee privacy and organizational information  
30 assets.

### This practice guide can help your organization:

- **protect data** from being accessed by unauthorized persons when a device is stolen or misplaced
- **reduce risk to employees** through enhanced privacy protections
- **improve the security of mobile devices and applications** by deploying mobile device technologies
- **reduce risks to organizational data** by separating personal and work-related information from each other

- **enhance visibility** into mobile device health to facilitate identification of device and data compromise, and permit efficient user notification
- **leverage industry best practices** to enhance mobile device security and privacy
- **engage stakeholders** to develop an enterprise-wide policy to inform management and employees of acceptable practices

31 The example solution uses technologies and security capabilities (shown below) from our project  
 32 collaborators. The technologies used in the solution support security and privacy standards and  
 33 guidelines including the NIST Cybersecurity Framework and NIST Privacy Framework, among others.  
 34 Both iOS and Android devices are supported by this guide’s example solution.

Collaborator	Security Capability or Component
	Mobile Device Management that provisions configuration profiles to mobile devices, enforces security policies, and monitors policy compliance
	Application Vetting to determine if an application demonstrates behaviors that could pose a security or privacy risk
	Firewall and Virtual Private Network that controls network traffic and provides encrypted communication channels between mobile devices and other hosts
	Trusted Execution Environment that helps protect mobile devices from computer code with integrity issues
	Mobile Threat Defense detects unwanted activity and informs the device owner and BYOD administrators to prevent or limit harm that an attacker could cause

35 While the NCCoE used a suite of commercial products to address this challenge, this guide does not  
 36 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your  
 37 organization's information security experts should identify the products that will best integrate with  
 38 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that  
 39 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
 40 implementing parts of a solution.

## 41 HOW TO USE THIS GUIDE

42 Depending on your role in your organization, you might use this guide in different ways:

43 **Business decision makers, including chief information security and technology officers** can use this  
44 part of the guide, *NIST SP 1800-22a: Executive Summary*, to understand the impetus for the guide, the  
45 cybersecurity challenge we address, our approach to solving this challenge, and how the solution could  
46 benefit your organization.

47 **Technology, security, and privacy program managers** who are concerned with how to identify,  
48 understand, assess, and mitigate risk can use the following:

- 49     ▪ *NIST SP 1800-22b: Approach, Architecture, and Security Characteristics*, which describes what  
50     we built and why, the risk analysis performed, and the security/privacy control mappings.
- 51     ▪ *NIST SP 1800-22 Supplement: Example Scenario: Putting Guidance into Practice*, which provides  
52     an example of a fictional company using this practice guide and other NIST guidance to  
53     implement a BYOD deployment with their security and privacy requirements.

54 **IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-22c: How-*  
55 *To Guides*, which provides specific product installation, configuration, and integration instructions for  
56 building the example implementation, allowing you to replicate all or parts of this project.

## 57 SHARE YOUR FEEDBACK

58 You can view or download the guide at [https://www.nccoe.nist.gov/projects/building-blocks/mobile-](https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device)  
59 [device-security/bring-your-own-device](https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device). Help the NCCoE make this guide better by sharing your thoughts  
60 with us. If you adopt this solution for your own organization, please share your experience and advice  
61 with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so  
62 we encourage organizations to share lessons learned and best practices for transforming the processes  
63 associated with implementing this guide.

64 To provide comments or to learn more by arranging a demonstration of this example implementation,  
65 contact the NCCoE at [mobile-nccoe@nist.gov](mailto:mobile-nccoe@nist.gov).

66

---

## 67 COLLABORATORS

68 Collaborators participating in this project submitted their capabilities in response to an open call in the  
69 Federal Register for all sources of relevant security capabilities from academia and industry (vendors  
70 and integrators). Those respondents with relevant capabilities or product components signed a  
71 Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to  
72 build this example solution.

73 Certain commercial entities, equipment, products, or materials may be identified by name or company  
74 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an  
75 experimental procedure or concept adequately. Such identification is not intended to imply special  
76 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it  
77 intended to imply that the entities, equipment, products, or materials are necessarily the best available  
78 for the purpose.