With a strong acceptable-use policy and mobile security in place, you're ready.

Continue >

verizon business ready

Overview

An acceptable use policy (AUP) governs what employees can and can't do with their mobile devices. AUPs can help drive appropriate use of resources, limit exposure to online threats and protect organizations against security breaches. Yet many companies don't have formal policies in place. In fact, only 56% of mobile security professionals surveyed reported having an AUP in place.

Want to do better? Here are 10 steps to take to start building your AUP.

The Verizon Mobile Security Index

The stats in this piece come from our 2020 Mobile Security Index, a unique report that provides detailed insight into today's mobile threats and best practices for mitigating them. To learn more, visit enterprise.verizon.com/msi

01 Don't even go there.

Set the criteria for appropriate and inappropriate websites.

02 You do you.

Understand what behaviors you want to encourage or discourage.

03 Take control.

Secure all your mobile devices, whether employee owned or corporate owned.

04 Don't pay for free Wi-Fi.

Promote LTE and limit Wi-Fi use to secure networks.

05 Know what's 'APPening.

Curate company-approved apps and limit the rest.

06 Look beyond the phone.

Address risks across the mobility ecosystem.

07 Stick with the latest and greatest.

Articulate and enforce your patch policy.

08 Watch how much they're watching.

Set expectations on acceptable data volumes.

09 Avoid the penalty box.

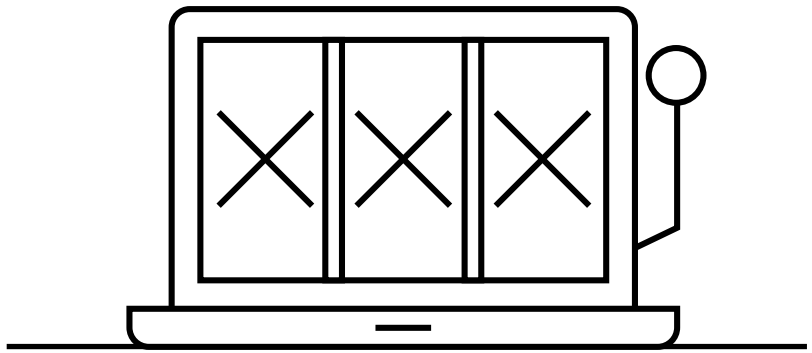
Guide employees on compliance.

10 Be the one that got away.

Provide regular phishing training.

Set the criteria for appropriate and inappropriate websites.

When employees visit an inappropriate site, they may not be just shirking work, they may be putting your organization at risk. The site may contain malicious content. Adult and gambling sites are common vectors for malware. With an AUP, your employees know what is acceptable. Set and enforce clear policies.

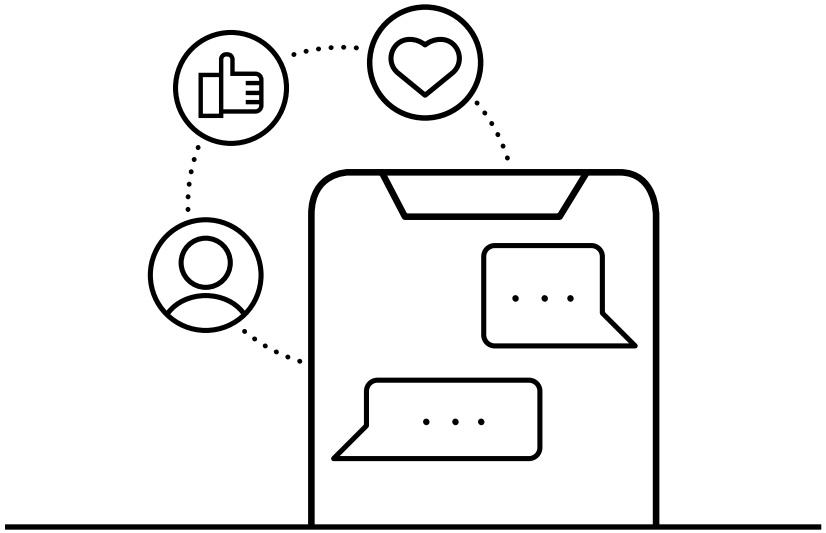


33% of organizations that had suffered a mobile security compromise said that employees accessing adult, gambling or illegal content had contributed to the incident.

–Verizon 2020 Mobile Security Index

Understand what behaviors you want to encourage or discourage.

Your AUP should fit your organization. Social media might be a time-waster – or an important tool for your salespeople. Employees of different ages and cultures might consider online shopping, chatting or gaming while at work completely normal. Your AUP should make it clear to employees what's OK. Even if they can't imagine what's wrong with buying a new clock ... while on the clock.

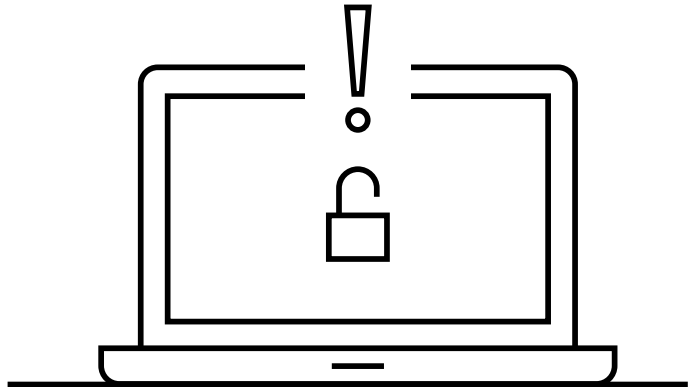


73% of companies either permit or officially sanction the use of social media on company-owned devices.

– Verizon 2020 Mobile Security Index

Secure all your mobile devices, whether employee owned or corporate owned.

In the end, it doesn't matter who owns a device if an employee uses it for business. Whether you adopt bring your own device (BYOD), corporate owned but personally enabled (COPE) or any of the other variations on device ownership and enablement, you need formal policies to govern use. Unified endpoint management can help you balance responsibility, usability and control.



77% of companies saw employees as their greatest security risk.

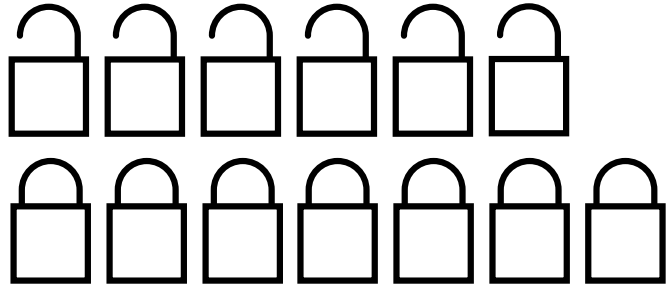
–Verizon 2020 Mobile Security Index

Promote LTE and limit Wi-Fi use to secure networks.

While the potential dangers of public Wi-Fi are well known, just half of companies surveyed have a solution to protect users from a man-in-the-middle attack. This means the more your users travel, the more your organization may be at risk. LTE access and hotspots can help employees stay connected while helping protect your organization's data from "free" Wi-Fi risks.

49%

of companies don't encrypt sensitive data when sending across public networks.



–Verizon 2020 Mobile Security Index

Curate company-approved apps and limit the rest.

It's almost impossible to know who really coded a mobile game and whether a hacker will be leveling up with your company data. Even mainstream business apps can be compromised. The more apps your employees download, the more avenues attackers have. Limit employees to approved apps whenever possible.

43%

of companies prohibit their employees from using apps that aren't from the company or an official app store.

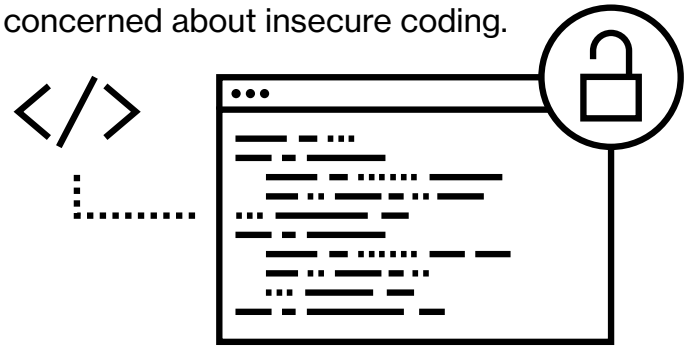
—Verizon 2020 Mobile Security Index

Address risks across the mobility ecosystem.

Your AUP should cover the many ways a mobile device interfaces with the world. Custom apps are just one potential security risk. Bluetooth® connections, public charging cables, SD cards and SIM swapping all carry risks as well. Let employees use what they need to maintain productivity, but use your AUP to open their eyes to the risks around them.

73%

of companies with custom apps are concerned about insecure coding.



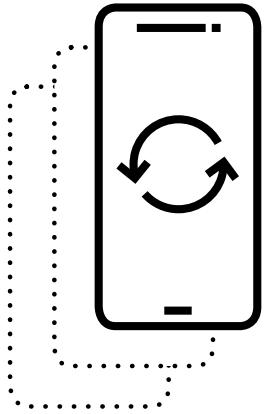
—Verizon 2020 Mobile Security Index

Articulate and enforce your patch policy.

An out-of-date operating system can harbor dangerous vulnerabilities. And if an OS is out of date, apps are likely even further behind. Design and articulate a patch policy to help plug those holes. If possible, implement that policy yourself with unified endpoint management, which can also help you quarantine at-risk devices.

Next, be sure to look at your app patch strategy, too. App downloads are ever increasing, reaching more than 196 billion apps downloaded in 2019 alone.[1] Keeping apps up to date is challenging but important.

1 https://s3.amazonaws.com/files.appannie.com/reports/1901_State_of_Mobile_Main_EN.pdf



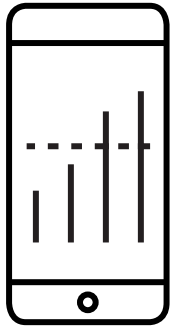
65%

of companies are concerned about the threat of out-of-date operating systems.

—Verizon 2020 Mobile Security Index

Set expectations on acceptable data volumes.

Why not download last year's Oscar winner if someone else is paying for the data? An AUP should make it clear whether video calls, movies, games and streaming music are acceptable or not. Set clear expectations on data consumption and employee usage to avoid putting your business at risk.



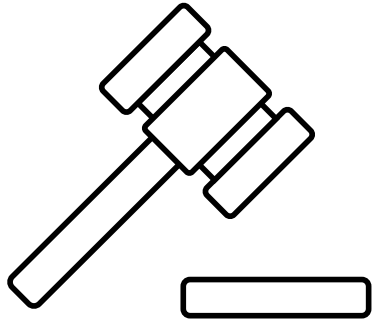
66%

of respondents were concerned about the volume of mobile data being used by their organization.

–Verizon 2020 Mobile Security Index

Guide employees on compliance.

You can't expect every employee to understand the policies governing your communications. Your AUP should list specific activities and behaviors that you need employees to adopt to remain compliant. Let your employees focus on their jobs.



72%

of organizations have reassessed the risk associated with mobile devices in light of new regulations.

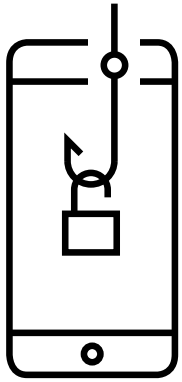
—Verizon 2020 Mobile Security Index

Provide regular phishing training.

Mobile users are three times more susceptible to a phishing attack than others.[1] Consider how many of your executives reply to emails on the go and you'll realize attackers have the chance to land a lot of big fish. Provide regular training and enforce attendance. It should not be optional.

1 https://s3.amazonaws.com/files.appannie.com/reports/1901_State_of_Mobile_Main_EN.pdf

Conclusion >



57%

of organizations reported having experienced a mobile phishing incident in 2019.[2]

2 https://www.wandera.com/mobile-security/phishing/

From AUP to A-OK

A well-thought-out AUP can go a long way to helping keep your organization secure. Combine it with unified endpoint management, mobile threat defense and other mobile security solutions and you can strengthen security and streamline administration.