Improve your threat protection with a strong acceptable-use policy and mobile security.

Continue >

verizon

Overview

An acceptable-use policy (AUP) is a set of guidelines for acceptable ways an employee is permitted to use the internet, a network or a connected device. AUPs can help drive appropriate use of resources, limit exposure to online threats and protect organizations against security compromises. Yet many companies don't have formal policies in place. In fact, only 43% of mobile security professionals surveyed reported having an established AUP.

Not having these types of policies in place can result in litigation. When employees have no guidance on what is prohibited, organizations may struggle with legal recourse.

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

The Verizon Mobile Security Index

The stats in this piece come from our 2021 Mobile Security Index, a unique report that provides detailed insight into today's mobile threats and best practices for mitigating them.

01 Don't even go there.

Set the criteria for appropriate and inappropriate websites.

02 You do you.

Decide what behaviors you want to encourage or discourage.

03 Take control.

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

04 Keep private from going public.

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 Protect the home front.

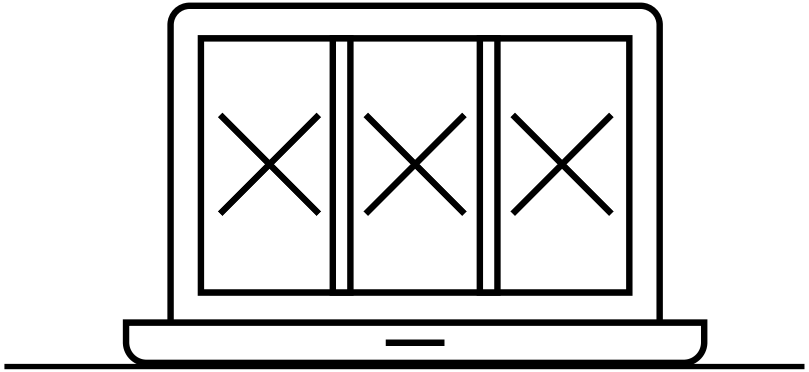
Flag the risks of working remotely.

09 Boost your security fortifications.

Keep your frontline defenses up.

Set the criteria for appropriate and inappropriate websites.

When employees visit an inappropriate site, they may be accidentally 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.

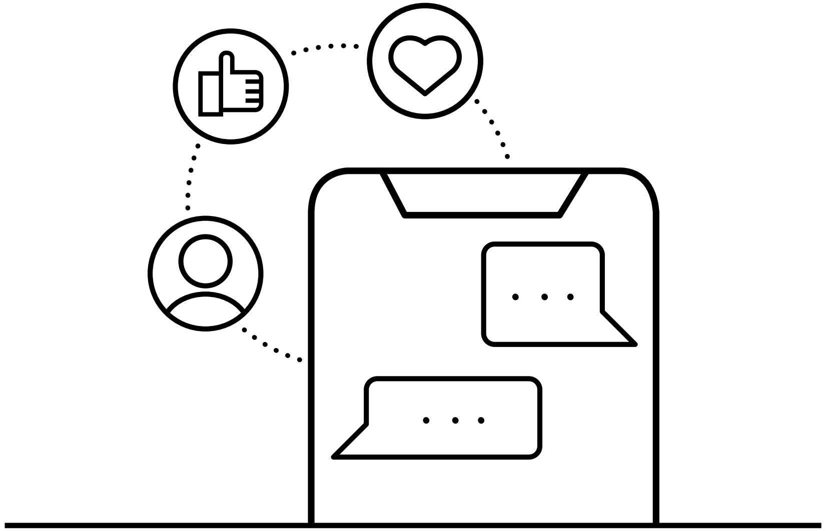


600% increase in the number of visits to websites hosting adult content

– Netskope, August 2020

Decide 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.

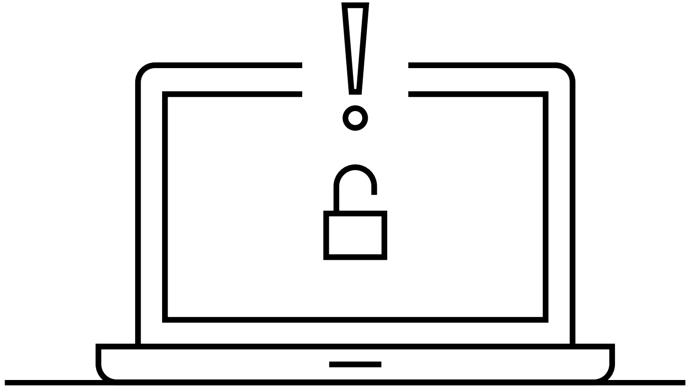


45% of companies that prohibit the use of social media are aware that employees use it anyway.

– Verizon Mobile Security Index 2021

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. Mobile device management (MDM) can help you balance usability and control.

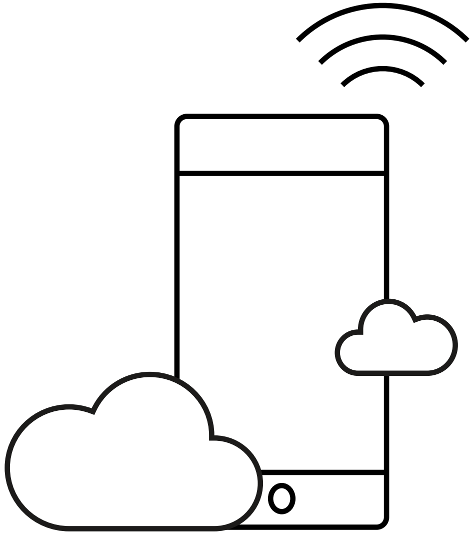


36% In response to COVID-19, more than 1 in 3 (36%) organizations opened up access to corporate resources and systems to employees using personal devices – that's on top of those that already allowed it.

– Verizon Mobile Security Index 2021

Promote LTE and limit public or unapproved 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 public Wi-Fi risks.



71%

Relying on trust is a questionable policy: Nearly three-quarters (71%) of respondents said they personally used public Wi-Fi for work tasks – even though 26% said it was prohibited.

– Verizon Mobile Security Index 2021

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.

28%

Policy isn't enough. Among those organizations that ban the use of apps from outside approved app stores, 28% are aware that employees use them anyway.

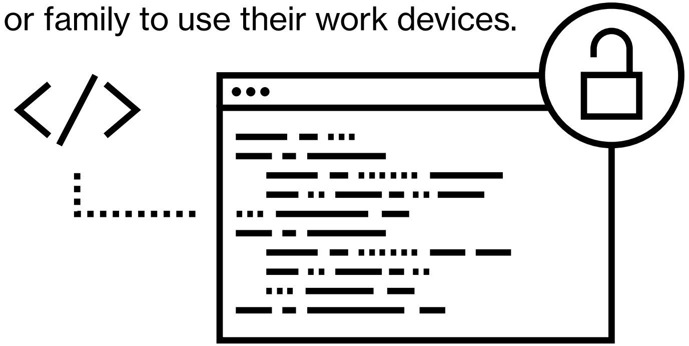
–Verizon Mobile Security Index 2020

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.

61%

of U.S. workers have allowed friends or family to use their work devices.

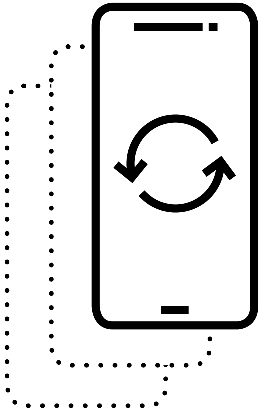


– State of the Phish, Proofpoint, January 2020

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, you can implement a policy 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 204 billion app downloads in 2020 alone.[1] Keeping apps up to date is challenging but important.

[1] Verizon Mobile Security Index 2020



29% iOS

93% Android

29% of iOS devices and 93% of Android® devices are running an out-of-date OS. (Data from January 2020, four months after last major update of each OS.)

– Data from Lookout (represents enterprise devices only)

Flag the risks of working remotely.

With record numbers of employees working from home, helping your workforce understand potential security risks is critical. Give them guidance on what internet connections are most secure when accessing company data and systems. Help them know the risks of public Wi-Fi, especially when using their mobile devices.

97%

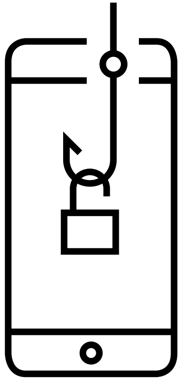
Nearly all (97%) security leaders consider remote workers to be exposed to more risks than office workers.

– SDP report, NetMotion, June 2020

Keep your frontline defenses up.

Having a strong AUP in place is just part of the battle. To win the cybersecurity war, it's critical to train the front line. Having regular training sessions about your AUP and growing risks like phishing will help your workforce help your company stay secure.

Conclusion >



364%

There was a 364% increase in the number of mobile phishing attempts in 2020 versus 2019.

– Lookout, analysis of all enterprise users covering January 2019 to December 2020

From AUP to A-OK

A well-thought-out AUP can go a long way toward 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.