

White Paper:

Establishing an Effective BYOD Mobility Policy: A Process and Templates for Success



BYOD: A Process and Templates for Success

Mobile devices have become a fixture of our daily lives, both work and personal. We barely remember living and working without constant access to email, contacts, calendars, Google searches, and even the occasional phone call. It's natural to want to extend that to the workplace. But when people link personal mobile devices to enterprise systems, red flags pop up in IT.

What about security? Who will support this? Are there compliance issues? Do we need to update our business applications? A BYOD strategy and effective policy establishes the rules of the road and sets expectations for everyone involved.

If you've written or updated your BYOD policy in the past two years: congratulations! But older policies should be revisited—and if you have no policy at all, it's even more urgent. A fast-moving mobile environment, combined with massive shifts to cloud services, make this an excellent time to review BYOD policies to acknowledge the important role that mobile devices play, and to ensure that a user-focused BYOD policy balances technology and business benefits with careful risk management.

This white paper is broken into two parts:

The first is our seven-step process for writing a BYOD policy. Not everyone will follow this exact path, but the steps we lay out will keep you from forgetting important details.

The second part is a BYOD template, broken into four sections. No one should copy the template word-for-word, but the template can speed the process of policy development and reduce the chance of leaving out important details.



About the Author

Joel Snyder is an internationally known expert in telecommunications and networks, with an emphasis on messaging, mobility, and security. He is currently a Senior Partner at consulting firm Opus One and splits his time between Tucson, Arizona and Rome, Italy. With over thirty years of experience, Dr. Snyder has deployed enterprise-class email and security systems, developed hardware and software products, and helped organizations worldwide with their mobility, networking, and security projects.







7 Steps to an Effective BYOD Policy

BYOD policies can be contentious. They help to define a line between work and home, and can tread on strongly held beliefs on how things should be done and the relationship between staff and the company. That conflict can't always be avoided, but having an inclusive process can help to minimize problems and create a clear path forward. Here are our steps to get things off on the right foot—and improve your chances of success.

1. Don't Try and Do This Alone

In some cases, IT groups will want to drive the BYOD policy process—they may be frustrated with support issues or worried about security. Sometimes, Line of Business leaders will be pushing for BYOD policy development as they discover that the lack of structure gets in the way of deploying new applications. Or it may come from the administrative side of the house, with HR or Legal departments weighing in after a bad experience.

Whoever starts BYOD policy development, though, should make sure that the right team is working on it. Organizations should already have an overall mobility strategy in place, but BYOD is often the place where the rubber hits the road: strategy has to meet reality.

Who	Why
 Line-of-Business	BYOD is about more than giving people access to email; it is about enabling a more effective organization. The use cases that LoB leaders bring to the table help define the structure of mobility.
 Information Technology	IT groups have to support BYOD, and have valuable input on issues related to mobility including potential technical problems. IT can also help make it clear what is, and isn't possible with existing infrastructure.
 HR and Legal	BYOD combines a very personal device—typically a smartphone—with company rules and responsibilities. In the long run, HR and Legal departments will be responsible for enforcing the policy and dealing with violations.
 Risk Management and Information Security	BYOD can increase the risk to the organization if private or financial information is leaked or lost. Some security measures are important in setting a balance between usability and security.

2. Agree on Definitions and Scope First

The term "BYOD" means different things to different people. Before discussing policy, it's important to discuss what you mean very, very carefully. You'll see terms like "BYOD" (Bring Your Own Device), "CYOD" (Choose Your Own Device), "COPE" (Company Owned/Personally Enabled), and more, all thrown around. You can make any definition you want—and the policy may be able to handle more than one case—but you should make it clear what you mean early on.

Defining the term "BYOD" is just part of the task at hand. You should also determine the scope of your policy. Is this BYOD policy for smartphones only? Or are laptops and tablets included? In this document, we're mostly focusing on BYOD for smartphones and tablets, but some organizations use the term to include a much broader range.

Whatever works for your enterprise is fine—just as long as you get the definitions laid out early. This is critical to all discussions going forward.

Try answering these questions to define BYOD:

1

Who Pays



Who pays for, and owns, the device?

Who pays for the monthly service plan?

2

Who Picks



Who gets to pick the device?

What limits are there?

3

Who Controls



Who has most control over the device - the user or the organization?

Can the user run personal applications?

What level of control does the organization have?

4

What Works



What applications are included? Collaboration tools? Or much, much more?

Does the device connect to the enterprise internal network?

3. Set Expectations on Control of Devices

Mobility security policies should be written to acknowledge that most users want a single smartphone, no matter who pays for it. From that point of view, BYOD policies describe a collaboration between the organization and the staff member, working together to ensure that mobile devices don't represent a security vulnerability.

Frequently, the administrative side of the enterprise will overreach, with Legal and IT groups trying to exert unwarranted control over employee smartphones. Having a balanced attitude means really accepting the reality of shared management between the user and the enterprise, with a focus on defining the minimum requirements that make a device acceptable to connect to corporate applications and handle sensitive data.

4. Don't Reinvent the Wheel

Most organizations have existing policies that cover many aspects of mobility, indirectly. Before writing any new policies, you should identify existing policies that already apply. Some those include:

Acceptable Use Policies (AUP)

Define what staff members can—and cannot—do with the IT assets of an organization, including company-owned computers and company-owned networks.

Data Protection Policies

Define how staff members must handle and protect sensitive corporate data, including company confidential, personally identifying information (PII), and financial information.

Regulatory Policies

For organizations that fall under one or more regulatory regime, define the steps and controls that the organization must take to remain in compliance.

Security Policies

Define how physical and network security are established, including access to physical assets and how devices and users connect to the corporate network.

These policies represent areas of work you do not need to do. If an AUP exists, then the BYOD policy should refer to it and accept it without re-stating the policy or changing it. When defining BYOD policies, don't try and second-guess or override existing rules for no reason. If some problem comes up or if

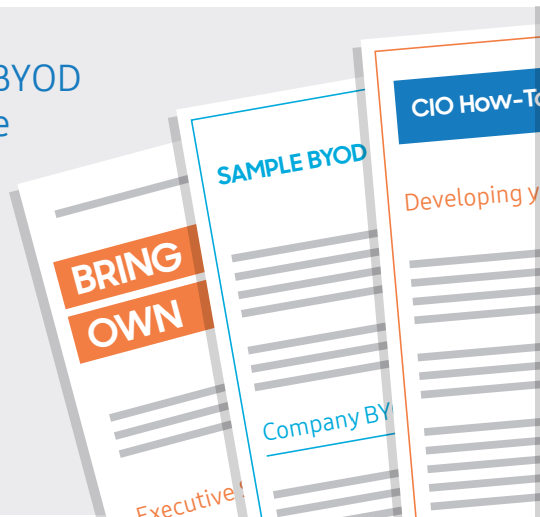
the policy needs to be adjusted with the introduction of BYOD, then it's best to modify the original policy—not build an exception into the BYOD policy.

Identify existing policies that already apply—for example, AUP or data protection. Identify any environmental concerns, such as regulatory or security classification. Do not try to rewrite these policies; if adjustments need to occur because of BYOD, the “root” policies should be revisited. Emerson may have found consistency to be the hobgoblin of little minds, but consistency in policy making is a good thing.



5. Build a Policy Based on Our Template ... and Get Agreement That It Is Realistic

Download the BYOD Policy Template



Sample BYOD Policy



Having the right team in place, a clear definition of what you want to accomplish, agreement on attitude, and good knowledge of existing policies sets you up for the easy part: writing the policy itself.

Our template makes the process straightforward by identifying the most common elements of BYOD policies and giving you an easy way to include them in your final policy. As you're developing the policy, resist temptation to go overboard or get too complicated. Your BYOD policy should be shorter than this white paper!

Before releasing the policy, make sure that you evaluate how the policy will affect technology and other processes within your organization. Policies that are too "blue sky" and won't work in your enterprise aren't much good.

For example, if the policy requires a particular password policy in your Mobile Device Management (MDM) suite, the IT department should confirm that they can actually enforce the policy. Each of the units affected, such as Purchasing, HR, Legal, and IT, should sign-off on the policy to confirm that they can make it work.

6. Establish the Exception Process

Policies always have exceptions. Sometimes it's a very senior executive who insists that they need a different device than everyone else. Or an advanced R&D group may need special access to their devices or configuration for testing and development. In any case, there will be exceptions, and it's good to plan for those exceptions at the beginning. This may sound like you're already undermining the new policy, but it's better to have all the rules laid out at the beginning.

Start by identifying who is allowed to make exceptions to the policy—and it shouldn't be an entire committee. The exception process shouldn't make it easy to circumvent the policy, but it should allow reasonable exceptions when there are clear business requirements. Exceptions should be clearly documented and be subject to periodic review, or come with an expiration date.

7. Decide How You Will Review the Policy

Policies should be long-lived and not need much review. That sounds good, but when it comes to mobility policies, it's easier said than done. Obviously, policies should be written in a technology-independent way, but changes in technology may require (or give the opportunity for) changes in policy. For example, a BYOD policy that doesn't address biometric authentication is leaving a valuable security tool on the table—but a policy written two or three years ago would obviously not have accounted for the rapid spread in facial, iris or fingerprint scanning technologies.

Other environmental changes can also affect your policy, such as changes in the marketplace for mobile devices, evolving budget and support structures in the organization, and shifting importance of mobile devices and mobile workers over time. Don't wait for someone to realize that some piece of the BYOD policy doesn't apply anymore—because that encourages everyone to ignore the entire policy. Make sure a defined process and timetable is given for periodic review at least every two years.



Writing the BYOD Policy

Mobility policies can be short or long, specific or vague, technical or procedural. In our experience, though, BYOD policies that are most effective are ones where the implicit "contract" between the employee and the organization is made explicit. Those should be the first two sections: Organizational Responsibilities, and User Responsibilities. By listing the duties of the organization, and those of the user, the expectations and issues are clarified to all involved.

In our template, we've added two more sections. The third one, called "Security," can even be turned into an Appendix to the main policy, because it is very technical and describes security features and settings that help mitigate the risks of mobile devices connecting to confidential enterprise data. The fourth section, called "Signoff and Consequences," is simply a place for the employee to affirm that they've read and agree with the policy, and they understand that there can be consequences for failing to follow the policy. That section should be short and simple.

Some enterprises will need longer policies. For example, if your organization is covered by a particular regulatory regime, you may need to be more explicit in ensuring that the controls and rules are covered fully. However, the policy should not be overly long. Implementation details can be written separately and incorporated by reference. Some sample policies available on the Internet fill more than 50 pages with excruciating detail that no employee will ever be able to understand (or will care about).

When considering what goes into the policy, and what should be in a separate document, ask yourself a simple question: Will the end user understand what we're talking about? If the information is so technical that it only makes sense to someone in the IT group, then it really doesn't need to be in the main BYOD policy.



1.1 Organizational Roles and Responsibilities

After an introduction and a brief summary, the most important subsections include the scope, eligibility, support, and any stipend or reimbursement. This is also the place to put in any terms and definitions that are needed—and these can be particularly important when defining the policy.

1.1.1 Scope of the Policy and Eligibility

In this subsection, you want to describe exactly what this policy covers. You should be answering questions such as:

- What is the total scope of this policy?
- What do we mean when we say BYOD?
- Who is eligible to participate in this BYOD program, and who is not eligible?

If you have broad groups of people who have different eligibility and scope, then they can be called out here. For example, if full-time staff are handled differently from contractors or consultants, this would be a good place to mention it. Similarly,

if there are major divisions between organizational units, they can be described here. You don't have to go into detail on the differences, but let people know up-front that there are BYOD policy differences between, for example, people at Headquarters and those in Branch Offices, or people in administrative departments compared to people in customer-facing departments such as Sales or Support. If there are other requirements to participate in BYOD, such as particular sign-off by a manager or a training program, this should also be laid out.

Scope and Eligibility also should cover eligibility limits and restrictions: the organization should reserve the right to disconnect a device or remove BYOD privileges at any time. This could include seizing and searching devices enrolled in the program, although that might be difficult to defend in front of a judge, no matter what the policy says.

1.1.2 Support

Support is one of the major costs of any BYOD program, so you need to be very explicit about what is and what is not covered.

In this subsection, you will answer:



What devices are supported?

This should not be so specific that you have to change it every time a vendor releases a new smartphone or laptop, but you will want to cover major operating systems, vendor product lines, and patch levels.



How will technical support be provided, and what support is included?

Consider that the end user will have at least four potential support organizations: the enterprise, the hardware and software vendors for their device, and the carrier they are using for cellular network connectivity.



Are specific carriers being recommended, or required?

This could include requesting access, approval, deployment or initial configuration of the device, connection to the carrier or company network (or both).



How does the user apply to be part of the BYOD program (if there is a clear lifecycle)?

You've already covered eligibility and scope previously, but if there are group-specific issues (such as what level of approval is required for different groups, or what devices are used by different groups) related to participation or device choice, then these should come out here.

1.1.3 Stipend or Reimbursement

This may not apply in all organizations, but any financial aspects of the BYOD policy should be laid out clearly and all in one place. This could include:

- Are devices 100% purchased by end users, or does the organization support a portion of the costs?
- How does this work and how is it approved?
- Are carrier services paid for by end users, or by the organization?
- Are there exceptions to this, depending on physical location or travel requirements?

- Will the organization pay for roaming charges when on official travel?
- What happens when a device is damaged, is lost or stolen, or ends its useful life?
- Who pays for the replacement and under what circumstances is this limited?

As part of this subsection, you want to consider all of the situations in which where there is a financial commitment, either on the part of the staff member or the enterprise. Look beyond initial purchase and setup for issues such as continuing service, replacement, and device loss to be sure you are clear on what your obligations are.

1.2 User Responsibilities

This section is an important place to make clear what you expect of the end user. It can be as simple as a list of specific issues and responsibilities, and should also refer to existing policies.

It's a good idea to try and incorporate existing policy and practice within the company in this section, rather than come up with something new. For example, if the existing Data Protection or Data Classification policy describes how confidential data should be protected, then the BYOD policy should not be re-defining these protections. If the existing policy is too lax to cover BYOD-type scenarios, then the existing policy should be fixed. Similarly, if the existing policy does not permit BYOD-type scenarios, then this should be evaluated for the impact it will have on the BYOD program and what types of data users are allowed to see on their BYOD devices.

We have broken this up into two main subsections. The first deals with the day-to-day use of the device, and the corresponding user responsibilities attached to that. The second subsection deals with the important exception cases of device loss and employee termination. You may wish to re-organize these subsections and add or delete based on your own requirements—this division just makes it clear that there are different responsibilities in the two usage scenarios.

1.2.1 Day-to-Day User Responsibilities

This subsection should cover expectations and responsibilities of the user on a day-to-day basis. These can be divided into three main areas: compliance with existing policies (such as Acceptable Use and Data Protection), mobile-specific safety issues, and mobile-specific physical security issues.



Mobile Responsibilities

Responsibility Area

Elements to Include in Policy

Acceptable Uses for BYOD Devices

Point to your existing Acceptable Use Policy and Data Protection / Classification Policy, as these are the base policies that have the most global scope. Other information security policies, such as anti-malware or phishing avoidance, can also be mentioned here, although most of these will be detailed in the "Security" section of the policy.

Mobile-Specific Safety

Many organizations have specific safety requirements, often going beyond what is permitted by local regulation. For example, use of mobile devices while driving should be strongly discouraged or require use of hands-free equipment – perhaps provided by the organization at no cost.

Mobile-Specific Physical Security

Users should be reminded not to lose their devices, perhaps by pointing out that the organization will not pay them for a replacement. More important security requirements could include forbidding sharing of devices with family members or requiring use of data separation solutions to protect work apps and data. When the BYOD Policy covers laptops, safe use of removable media such as USB drives should be discussed.

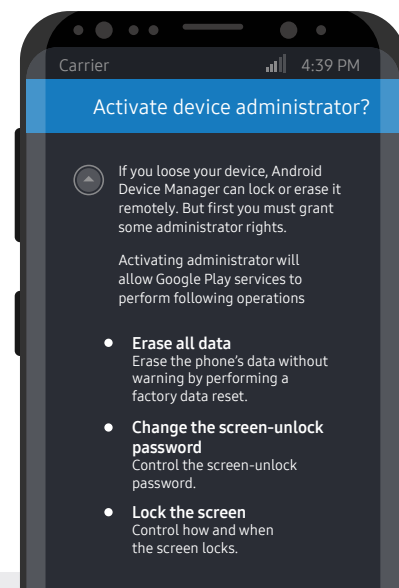
1.2.2 Device Loss and Employee Termination

This subsection of the BYOD policy is important because it deals with specific cases where the organization's rights normally would not be so broad. For example, if a user is fired, the organization often will immediately remotely wipe the user's mobile device. That might also delete personal information, which would normally not be considered within an employer's scope of privileges. For this reason, the final text should be reviewed by your legal department to ensure that the organization is not violating any Federal or local laws here.

Device Loss: In this section, you'll want to describe the responsibilities of the user when a device is lost or accessed without authorization. For example, you may want to require the user to inform the Help Desk within a very short time interval so that they can activate remote wipe, remote lock, and reset any credentials or revoke any digital certificates used for authentication. This section should not only describe what the user must do, but also what the organization will probably do along with the potential loss of personal data stored on the device.

Employee Termination: This section includes responsibilities during employee termination. If an employee is being fired, then the organization can expect little cooperation. However, it

is very important that any steps that the organization plans to take be described here to avoid potential legal issues down the line. The most common post-termination BYOD activities include remote locking and wipe of BYOD devices and disabling access to encrypted data on the phone, all of which affect any personal data on the device.



1.3 Security

Many companies over-specify their security requirements in their BYOD policies by listing every security parameter that needs to be set on BYOD devices. This should be avoided, for two reasons:

- These settings have little or no meaning to most staff members, and they can make the policy needlessly long and complicated. Since the goal of the policy is to lay out roles and responsibilities for BYOD users and the company, adding a lot of IT-only information obscures the core message.
- These settings change with technology changes, and you don't want to have to change your BYOD policy because of a software update on your MDM tools.

In this document, we'll include a list of elements that may be appropriate for IT security teams, but ideally these should be moved to a separate document maintained by the IT team and not be an integral part of the BYOD policy.

1.3.1 Privacy, and Remote Wipes and Backups

A very important part of the BYOD policy is a clear statement about which personal data can be reasonably kept private and what are employee expectations about privacy of their data. Some of this is covered incidentally in the "termination" section above, but having redundant statements about this is a good idea as it makes very clear the issues and implications of

BYOD especially in a shared-device environment.

This section of the policy should answer the following questions:

- How private and secure will personal data be on the BYOD device? For example, will it be backed-up to corporate servers and thus visible to IT staff, HR, or auditors? Will the company be able to remote wipe the device, possibly deleting all personal data? The policy should note that this may happen, even accidentally.
- How private will personal usage data be from the BYOD device? This is a particular issue when endpoint security software is installed, which may log every URL the device uses, including blockages.
- Who is responsible for backing up personal data on the mobile device? For smartphones, this includes private information such as locally stored photos, logs of text messages, and email, address book, and calendar data. (If the user is responsible for backing up corporate data, then this should be stated as well.)
- What expectations does the organization have about its access to the device? Are there other "rights" that the organization reserves (such as seizing a device) and under what circumstances? Note that some of this is covered in the Scope and Eligibility section above, so it should appear only once, either there or here.



1.4 Information Security

This part of the BYOD policy should be kept brief, and many of the settings described here can be put in a separate document maintained by the IT department.

The goal of this subsection is to define the "rules of the road" for security, including how they will be enforced. This typically includes the mandatory activation of a Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) client that controls many security settings.

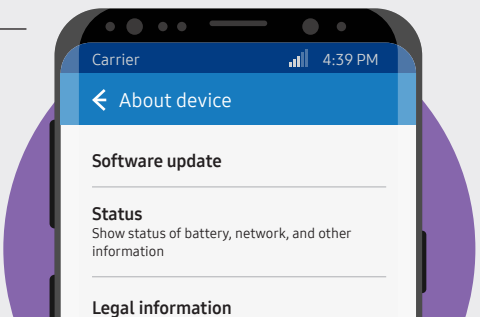
When deciding what to put in this part of the policy, the goal is to inform the user of what is important from an Information Security point of view, not to set the exact parameters for each setting. For example, it's appropriate to say: "BYOD devices will have passwords set to comply with Company Password Policy. This setting will be enforced by the installed MDM client." It's not appropriate to say: "BYOD devices must have a password at least 8 characters with 3 upper case, 2 lower case, 3 special characters, and changed every 117 days, with a history maintained for 2 years. Passwords may not contain English or Dutch words and may not have any part of the username included..." That last chunk might go in an IT policy that is available to anyone who wants to see it, but it shouldn't be in the BYOD policy.

Generally, anything that IT is responsible for enforcing (either directly or through MDM policies) should be described very briefly; only things where the user must make a decision or take an action should have detailed descriptions.

1.4.1 Signoff and Consequences of Violation

The BYOD policy shouldn't just be a list of settings; it really describes an agreement and responsibilities between the enterprise and the staff member. This means it's appropriate to have a mechanism for each side to formally acknowledge that they've read and understand and agree with the policy. Some organizations handle the sign-off by including the entire policy, with a signature line at the end for the employee. Others make a shorter document that says, essentially, "I received and read and agree with the policy" that has to be signed before a device is activated for BYOD access. Whichever you choose, it's a good idea to also include a short reminder that the policy is not just an abstract thing—the enterprise is doing this for a reason, usually security and risk-based, and therefore there are consequences of violating

Some of the areas commonly mentioned in BYOD policies include:

Security Area	Common Issues
<p>✓ MDM/EMM or other client tools</p>	<p>BYOD almost always requires MDM/EMM tools to be installed, and often includes an endpoint security tool. Users should be reminded that these tools are configured by corporate IT and may not be disabled, even temporarily.</p>
<p>✓ Patches and Software Versions</p> <p>The minimum requirements are already described earlier, so here the policy should simply mention that patching and software updates will be controlled by IT using the MDM tool, and that users may not postpone installation of patches or updates.</p>	

Security Area

Common Issues

- ✓ **Containers**

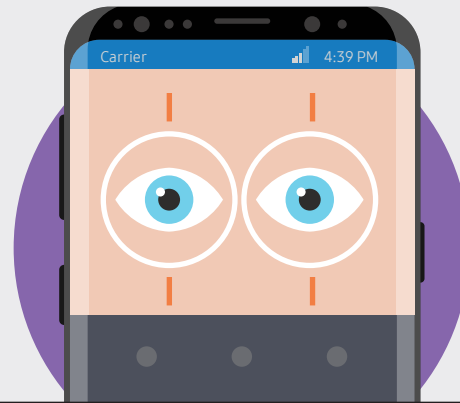
If containerization technology (such as work and personal profiles or more advanced tools) is a part of the BYOD security strategy, it should be mentioned here. Note that the user responsibilities section describes taking care with access to containers, so this does not have to be repeated here.
- ✓ **Network Access**

BYOD devices may be allowed to connect to corporate networks, either directly via Wi-Fi or using a VPN client. Policies and profiles should be controlled by IT and pushed by MDM, so users don't have to know anything other than "network access is controlled by IT."
- ✓ **Storing Sensitive Data**

BYOD devices may have sensitive data limits (such as "no more than 100 Mb of data"). This is more relevant in BYOD laptops than in smartphones, but can apply to both if there are large document libraries that may be cached.

- ✓ **Password Protections**

BYOD devices should comply with company policy. Sometimes biometrics will be required. If two-factor authentication is used, this should also be brought up. Idle locks enforced by MDM/EMM should be mentioned, although not described in detail.



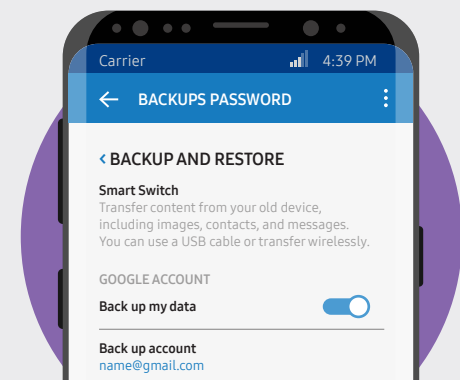
- ✓ **Rooted/ Jailbroken Devices**

This is mentioned earlier, but a brief note that jailbroken or rooted devices will be immediately dis-enrolled from BYOD is appropriate. Any other hardware security measures, such as required encryption or disabling of cameras, could be mentioned here.
- ✓ **Applications and Application Stores**

If an application whitelist/blacklist is in place and enforced by MDM, this should be mentioned. Similarly, if application store restrictions will be imposed, these should be mentioned.

- ✓ **Backups**

Any backup questions or issues not covered above should be mentioned, but usually this is not needed. If there are rules about what can and cannot be done with synchronizing devices to laptops and desktops, these should be described.



How Samsung Can Help

Samsung understands the challenges of enterprise mobility. Beyond our portfolio of smartphones, tablets, wearables, 2-in-1s and laptops, we offer a breadth of device management solutions and expertise to help plan and execute any mobility initiative.

The Samsung Knox Platform and Solutions

Learn more about the defense-grade Samsung Knox security platform and device management solutions, such as Knox Configure, a tool for remotely provisioning and configuring a fleet of mobile devices, and Knox Workspace, for secure containerization of work and personal data.

samsung.com/knox

Samsung Business Services

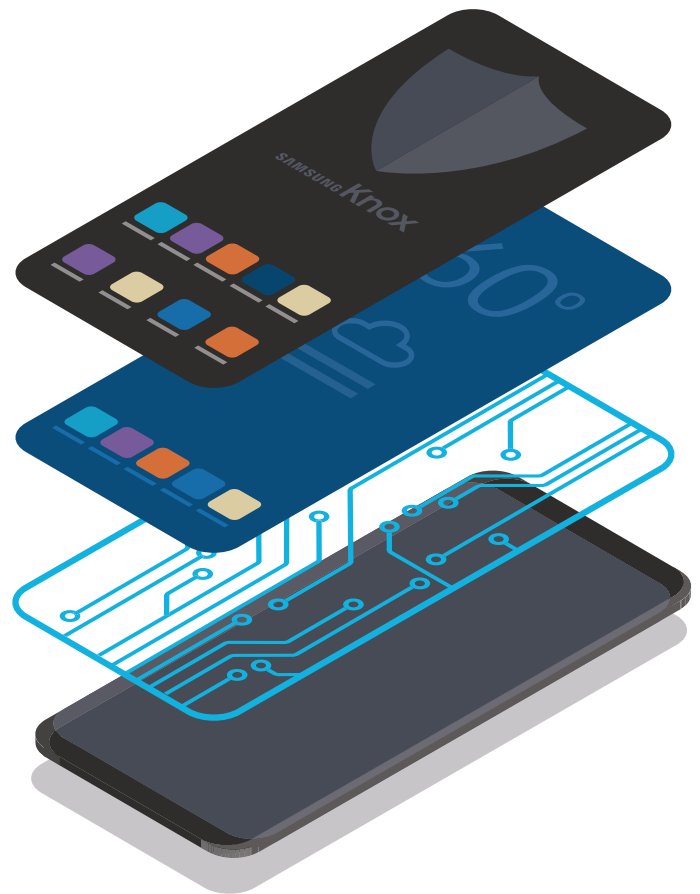
Learn about how Samsung Business Services can help with device deployment and technical support. Get easy access to expert advice and assistance, including EMM assessments, deployment planning and execution, and tech-to-site senior engineers.

samsung.com/us/business-services

The Enterprise Edition

Learn about Samsung's Enterprise Edition of unlocked smartphones can help drive your business. Combining Knox Configure, Samsung E-FOTA, regular security updates, you get the combination of powerful and simple device management, customization capabilities and defense-grade security.

samsung.com/enterpriseedition



Get a Consultation Today

Get an enterprise mobility consultation from Samsung's mobile solutions experts to address your biggest business challenges. [Click here](#)

This template has been created as a starting point for organizations updating or instituting a formal BYOD policy. Organizations are encouraged to modify, customize and amend the template for their own use. Samsung does not accept responsibility for any issues arising from the utilization of this template. Organizations using the template should undertake their own legal review.

Learn more: samsung.com/business | insights.samsung.com | 1-866-SAM4BIZ

Follow us: [youtube.com/samsungbizusa](https://www.youtube.com/samsungbizusa) | [@samsungbizusa](https://twitter.com/samsungbizusa)

SAMSUNG