It’s no secret that mobile devices and applications are flooding into organizations of all types and sizes. Technology research firm Gartner predicts that by 2016, 40 percent of the global workforce will be mobile, with 67 percent of workers using smartphones.

The drivers are many, but big draws include the potential for greater productivity — giving people anywhere, anytime access to information via devices they’re comfortable with. That means they can readily collaborate with peers and quickly address constituent or customer issues that surface in email or text messages.

What is less clear, however, is how organizations can cope with this mobile onslaught to make it manageable and secure. The answer, according to consultants and mobile technology vendors, is to craft a comprehensive mobility policy.

“My recommendation is to take a step back and create an entire mobile strategy that replaces a series of Band-Aid solutions,” says Vizay Kotikalapudi, group manager for Symantec’s enterprise mobility group. “Once you have the strategy in place, you can avoid always being in reactive mode.”

Here are eight steps for devising and implementing:
a comprehensive mobile policy that’s manageable, enhances productivity and maintains security.

STEP 1: Organize a mobility steering committee.

Experts say it takes a team of stakeholders, representing a cross section of internal experts, to develop an overarching policy for mobility.

Three groups will play an especially pivotal role in these discussions: IT, human resources and line-of-business units. In some cases, hashing out questions about mobility can lead to new ways for these groups, particularly HR and IT, to work together.

“HR comes from an interesting perspective because on one hand it’s responsible for creating and distributing policy, but its job is also to create a favorable employee experience,” says Dan Shey, practice director for M2M, enterprise and verticals at ABI Research. “They have to balance the benefits and risks associated with mobility.”

The IT team can augment this perspective by lobbying for efforts to address security and management risks, while business managers can make sure the policies address the needs of users, Shey adds.

STEP 2: Outline the organization’s goals.

Before the steering committee delves into policy specifics, it must define what challenges and opportunities the organization is trying to address with a modern mobile policy.

“Considerations will range from helping the CEO, who just got a new tablet, to end users, who are pressuring the organization to support Android devices,” Kotikalapudi says. “But then there’s also the line--of-business managers who want to put corporate data in the hands of people in the field, which represents a true business model. A final consideration is the fact that if you don’t have a system in place to support mobility, end users will find their own way.”

Multiple triggers may encourage organizations that the time has come to act. These drivers may include a growing acceptance of the bring-your-own-device (BYOD) model — both as an opportunity for cutting IT costs and as a potential productivity booster.

Other incentives include the ability to better secure an organization’s data and applications, as well as making sure that workers have ready access to the necessary tools to do their jobs.

STEP 3: Define the policy details.

There aren’t any one-size-fits-all templates for mobile policies, but all types of entities, no matter their size and industry segment, need to address some common core requirements. These start with specifying the types of devices covered by the policy.

In some cases, organizations may have to merge old and new policies. For example, most organizations will already have rules in place for managing notebooks. But unless they’ve been updated recently, the policies will likely assume that the devices are provisioned by the entity. That may still be the case, although some organizations are extending BYOD beyond smartphones and tablets to include notebooks and ultrabooks.

The key is defining which types of devices and operating system platforms will be allowed to access data versus those that are restricted from use because of management and security considerations.

“Different areas need different infrastructure and controls,” Shey says. He suggests organizing worker groups into three broad categories. The first segment he calls “organization--liable,” those who use entity provisioned devices and data services to access organization databases.

SHOP APPS CLOSE TO HOME

Enterprise app stores provide a managed portal where workers can download approved and proprietary mobile apps. The research firm Gartner has earmarked such stores as one of the top tech trends for 2013.

Enterprise app stores will turn IT departments into market managers, according to Gartner. The app stores will eventually become the “anchor point” for users to get everything they need.

According to some estimates, the rollout of these resources is still in the early stages. But that may change as senior program and IT managers alike understand the advantages.

Enterprise app stores provide some welcome control over the software that mobile workers run on their devices. End users simply browse a list of available apps. The IT department can also vet the apps to guard against security vulnerabilities.

THE PERCENTAGE OF ORGANIZATIONS EXPECTED TO HAVE MOBILE DEVICE MANAGEMENT PROGRAMS IN PLACE WITHIN THE NEXT FIVE YEARS.

65% SOURCE: Gartner, Inc.
Examples include C-level executives, directors and administrators. “For this group, organizations will need a well-developed policy in place and a management infrastructure to control the devices and keep sensitive data safe from the bad guys,” he says. “That may mean mobile device management [MDM] capabilities, plus data encryption and mobile virtual private networks [VPNs].”

The second group also uses entity devices and services, but they might be authorized to access only the organization’s email system not databases directly. The controls can be somewhat looser, but the organization might still want an MDM solution to track the status and location of devices.

“These users may not have mobile access to databases, but there could still be access to sensitive data in emails,” Shey points out. The third segment comprises BYOD users who tap their personal devices for work-related apps or to email and text other staff members, customers or constituents. Examples include a marketing manager or HR person who may work mostly in an office but wants to stay connected while in meetings or after hours.

Wrapped up in these considerations are rules for whether some applications and data are off limits. For example, a policy might allow all devices to download approved software via a specified portal. But any additional software applications that users want must be on an organization-approved list.

If there are other apps users or groups of users need, then an approval would need to come from the mobile policy overseers. The policy also can state that the organization won’t support user-added software.

**STEP 4: Spell out financial terms.**

There are three basic financial models an organization can adopt.

The first is direct billing, where the organization buys the device and assumes all expenses. The second is to provide a fixed monthly reimbursement for device support. Finally, some organizations choose to reimburse based on worker expense reports.

The model chosen depends on the answers to a handful of important questions. These questions range from whether the organization or worker will pay for all or a portion of the hardware, data access plan and support costs. Other financial areas to spell out include the specific costs for which a BYOD device owner will be responsible and, if applicable, the international calling and international roaming plans that will be offered for voice and data traffic.

**STEP 5: Address liability issues.**

Liability considerations home in on data that’s subject to government security and privacy regulations and the organization’s own best practices. “You don’t want to wind up with a Sarbanes–Oxley problem because of mobile usage,” warns Craig J. Mathias, principal with the Farpoint Group, a consulting firm. But there may be some knotty issues to sort out when it comes to liability. For example, every organization has a right to regulate how its data is accessed and used, but policymakers must decide how to handle users’ personal information, including contacts that are stored on entity provisioned devices. Is that data private? The policy committee must hash out questions such as these to create a system that minimizes the exposure of personal information.

Finally, mobile users should clearly understand the penalties for failing to adhere to any of the required mobile policies. This includes whether different types of violations will carry different penalties. For example, will the consequences for violating eligibility rules be treated differently than security or acceptable-use requirements?

**STEP 6: Lock down security.**

Security will likely require the most time and effort from the mobile policy writers. The influx of new mobile equipment, including personal devices, is adding complexity to security operations while also loosening some of the tight controls the IT department had been able to exert in the past.

“The paradigm has changed. In the past, end users were bound by what the IT department required. But it’s not a one-way street anymore,” Kotikalapudi says. “If you want to put security software on a mobile device, you must first get user buy-in.”

To get users on board, IT managers must accept a couple of ground rules, he adds. “You can’t do anything to mess up the native end-user experience. People buy an Android device, for example, for specific reasons.” That shouldn’t be compromised by security controls.

Hammering out security rules
begins with setting the broad outlines in Step 3 about the data that should be accessible via mobile devices. Follow that rule with having the steering committee drill down into specific security technologies and use policies.

An important goal is to protect internal data when it travels outside the physical boundaries of the organization. Sensitive information becomes particularly vulnerable to cyberthieves as it moves across external networks and may be accessed by unauthorized viewers if devices are lost or stolen.

Technology-based security measures encompass methods for user and device authorizations, device and data encryption, VPNs and sandboxing (the ability to wall off certain data and applications to make them less vulnerable to intrusions). Other basic measures include device-side antivirus software and the ability to manage configurations and patches.

The team also must come up with contingency plans for controlling damages if a breach does occur. Full or selective wiping of data from missing devices is one common approach.

If the organization retains the right to remotely wipe lost or stolen devices, the policy should explain whether a wipe will include removal of personal data or just the information contained in a corporate sandbox.

One way to exert these controls is with MDM solutions that let organizations centrally enforce policies. Some entities extend this approach by focusing their efforts on the data itself with mobile application management systems. With MAM, the organization enforces policies for entity related applications and data, not the devices themselves.

From a mobile policy standpoint, the rulebook can also require mobile users to download a specified MDM or MAM system.

**STEP 7: Manage the rollout.**

The next step is to create a game plan for what is, in essence, a public relations effort. The organization must determine how to communicate the policy and educate workers about what it will mean for them.

It’s advisable to first explain the salient points to group managers and then to groups of staff members. “Do you just send it out via email and say, ‘Here, read this?’ Or do users have to check a box that says they’ve read the policy and agree to follow it?” Kotikalapudi says.

Once the policy is complete and all users are aware, it’s time to put the policy into practice. The best starting point is often a pilot, especially if this is a new policy. Consider enlisting staff members who are already interested in or stealthily using their own devices.

Beginning with a small group that’s representative of various users within the organization will help determine what’s working and what isn’t. It also provides time to collect data to measure benefits and costs.

**STEP 8: Address ongoing changes.**

Experts say there’s one final step for keeping a mobile policy viable: regular reviews and updates to assure the strategy continues to address the latest technologies and business needs.