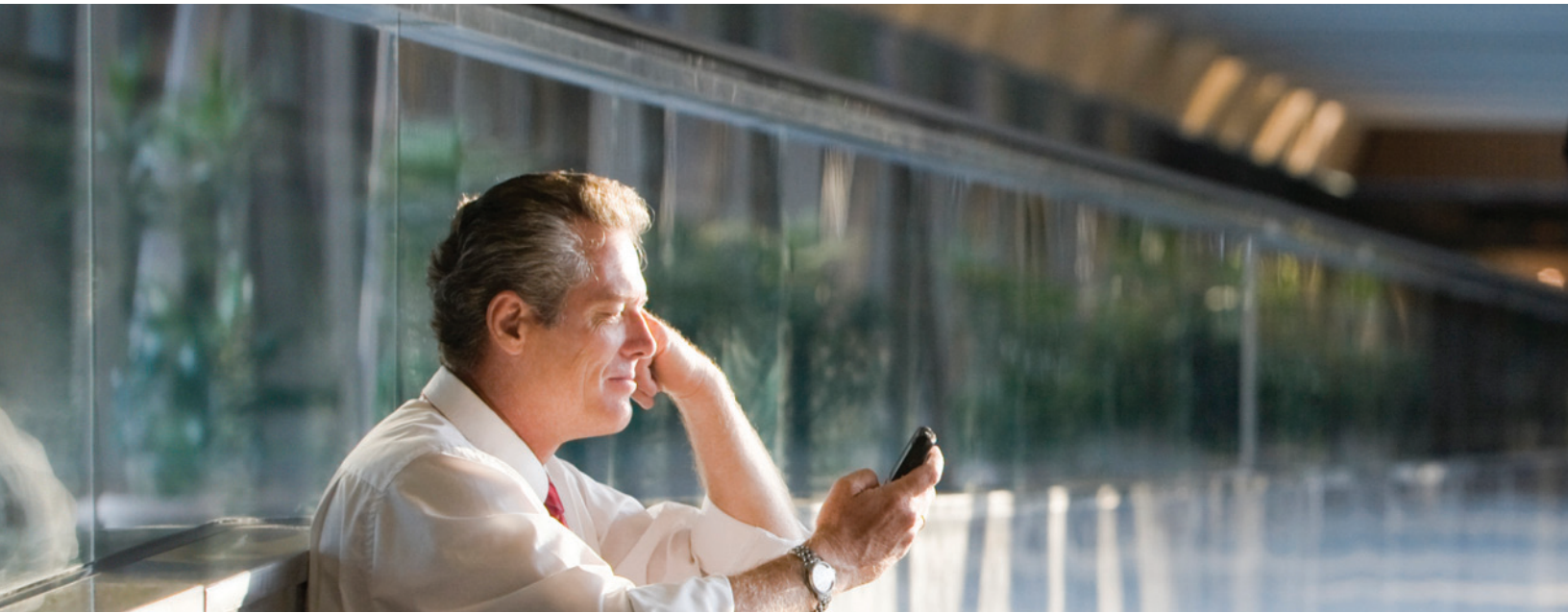




WHITE PAPER

AN IT MANAGER'S GUIDE TO  
**Managing Personal  
Devices in the Enterprise**

SYBASE®



Allowing personal smartphones does not have to be mob rule. Consider establishing these seven steps to creating a more secure and manageable mobile enterprise.

#### AN IT MANAGER'S GUIDE TO MANAGING PERSONAL DEVICES IN THE ENTERPRISE

Developing a strategy for managing and securing employees' personally owned mobile devices is no longer avoidable. iPhone and Google Android devices are joining BlackBerry, Symbian and Windows Mobile smartphones in the workplace, and their numbers are only going to increase in the coming months. Regardless of whether corporate policy allows mobile devices to access the corporate network, workers are still bringing them into the office.

According to a recent Forrester Research report, almost half of U.S. and European businesses surveyed are embracing the notion of allowing personally owned devices access to a secure corporate network. One-quarter of businesses surveyed do provide full support to at least some personal devices, and another 21 percent provide at least limited support.

What these companies are realizing is that if they allow employees with personally owned devices to access corporate email and other resources, these employees will be more productive. In addition, in today's economic times, enabling personal devices helps companies offload some of the cost because users are paying for these devices themselves.

Corporate IT departments naturally are cautious about opening up the network and allowing full access to any device. IT needs control over how and under what circumstances mobile devices can access corporate systems. Finding just the right balance—maintaining the integrity and security of the network while allowing easy access to the applications users need to be more productive—will give organizations a competitive advantage in the coming years.

## SETTING THE GROUND RULES

IT can secure the network for mobile devices without endangering corporate assets. These seven best practices will help protect your environment and provide employees the flexibility to use their personal devices without compromising critical enterprise resources.

### 1. Discover mobile devices on the network.

A good starting point for IT managers is to definitively identify who is accessing – or trying to access the network. Frequently this can be accomplished by auditing existing systems such as your Exchange Server, Microsoft ISA logs and desktop/laptops for the presence of local synchronization software.

If you don't think any mobile devices are on your network, consider this example. A large national retailer implemented Exchange server gating software from Sybase at its corporate headquarters, and within just a few days its IT department determined that the company had more than 1,000 unauthorized Windows Mobile, Palm, iPhone, and Symbian devices on the corporate network.

### 2. Determine the back-office systems employees want to access.

Every user shouldn't automatically get access to everything on the network – not by a long shot. Take the time to survey your departments and employees to determine what they hope to gain from mobility. The trends towards personal devices are being driven by “information workers,” those employees who are often in the office or travel occasionally, and see mobile devices as productivity tools.

Do these users simply need access to enterprise email and intranet sites, or do they want access specific applications? For example, you can provide sales reps with access to their sales applications, executives with access to sales dashboards and purchasing approval systems, while information workers only have access to enterprise email.

### 3. Formalize user types and set policies.

Based on what you learned in step 2, evaluate users, create groups of users and determine governance policies for each group. These policies will define the “like to have access” and “need to have access” for each group of users. IT can set up management and security protocols that conform to those policies. Varying device management tasks and levels of security can also be applied to each group.

### 4. Get ready to take action.

A good place to start implementing more security is to add a filter to control access to your backend systems. A filter is a piece of software that collects data and analyzes it so you can evaluate personal mobile devices coming into the network. One option is to monitor who is attempting access and to block access unless a management client is installed on the device. Sybase provides an Exchange ISAPI filter that can identify and deny access to back office email unless each device meets a predefined set of criteria.



**5. Add password and encryption policies plus remote wipe capabilities at a minimum.**

The bare minimum to consider for securing personally-owned devices is password enforcement and on-device data encryption. Other critical areas include the ability to remotely wipe lost devices, as well as inventory management that identifies which devices are connected to the network at any given time.

**6. Consider separating personal data from business data.**

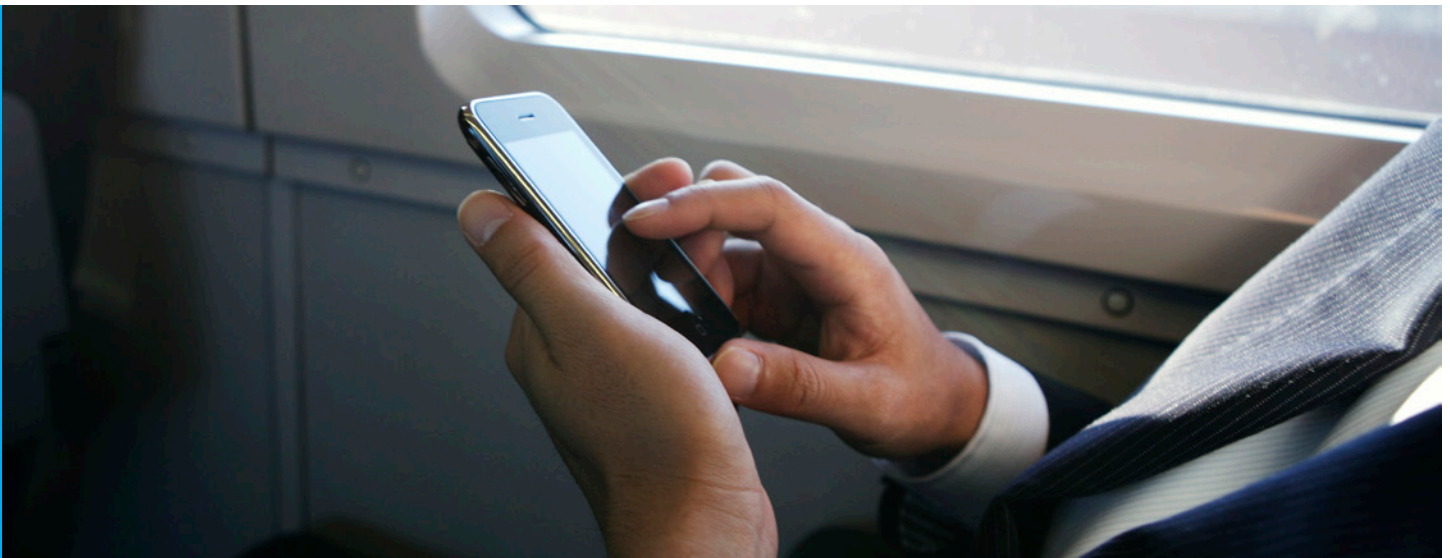
One security strategy that many companies are adopting is a “sandbox approach.” This approach involves storing enterprise data, including email and applications, in a distinct area of the device, and encrypting and password protecting only that data. All other files, including personal music, videos, photos and so on, are available to the user without logging in to the device.

**7. Enable users to be self-sufficient.**

Because most IT departments are spread very thin, the best strategy for making all of these adjustments to corporate policies is to keep things as simple as possible. Rather than adding another screen to the bank of displays that IT managers already need to look at for network status and the like, it makes sense to give users a measure of self-sufficiency to comply with company policy.

For example, instead of flipping a switch and barring personal devices entirely, why not direct users to where they can download a management client application that will bring their device into compliance. This self-help policy frees IT staff from spending precious time tending to personal devices, and it helps keep the network secure.

*Sybase customer Baloise Insurance was faced with the challenge of personal devices coming to work. The company decided to install a self-service portal to enable users to locally set up and maintain corporate data on a variety of mobile devices including iPhones and Windows Mobile devices. After implementing Sybase software, the company has cut the number of help desk calls in half, reduced engineering time and support and improved overall satisfaction and productivity of end users.*



## SYBASE MAKES THE MOBILE DELIVERY

For all of the best practices discussed, IT managers can confidently turn to Sybase and its range of enterprise mobility products. Sybase offers the industry's most powerful, flexible and secure solution for managing mobility across the entire enterprise. The wide range of mobile operating systems and the constant introduction of new devices make managing and securing mobile devices a major challenge. Sybase simplifies this complexity by providing infrastructure that allows enterprises to take full advantage of the vast benefits of mobility today and into the future. Sybase ensures the management and security of mobile devices over any network for any deployment size.

For the growing number of organizations that are deploying Apple's iPhone as part of a mobile strategy, Sybase provides these capabilities:

- Device management via over-the-air provisioning, including establishing network and security settings to minimize IT resource requirements in managing the mobile device population;
- Security through lockable configuration and security policies that are consistent with IT standards;
- Pre-built and custom-built applications that isolate enterprise data to comply with enterprise security requirements, while leaving the user's personal data untouched and easily accessible

## TIME TO EMBRACE MOBILE DEVICES

For IT professionals facing the onslaught of personal devices in the workplace, smartphones don't have to be viewed as a violation of corporate security policies. As the Forrester report cited earlier states, because the vast majority of employees are using personal devices at home, harnessing that trend and turning it to the advantage of your company makes sound business sense and will go a long way to keeping employees happy and productive.

## ABOUT SYBASE

With more than 20,000 global mobility customers, thousands of leading mobility partners and 20 years of enterprise mobility expertise, Sybase is committed to offering device-agnostic solutions that support a broad range of operating systems. Whether your workers are using personally-owned consumer devices or task-specific ruggedized devices on the frontlines, Sybase empowers you to manage mobility with complete confidence. By providing a mobile platform that offers capabilities for device management, security, applications, messaging and development, Sybase provides a solid foundation to mobilize your business and provides the tools for a long-term strategy that helps to protect your valuable IT budget.

