{e}mazzanti® technologies
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

Cell Phone Best Practices Empower Work from Home

Now, more than ever, the lines between work and personal life have blurred. And for the millions of employees working from home, the cell phone represents the ultimate connecting point. More than ever, we use personal cell phones to conduct business. The following cell phone best practices help protect both the organization and the employee.

Understand the Risks

Allowing (or encouraging) employees to use their personal cell phones for business can benefit both the workplace and the employee. Employees benefit from the convenience of using a single, familiar device. Meanwhile, businesses save money on company phones while enjoying greater employee productivity.

However, that convenience comes with a price. Employees who make business calls from their personal cell number lose privacy. They also worry about inadvertently giving their employers access to their personal messages, photos and more. Meanwhile, personal devices accessing corporate networks and data present a significant security and compliance risk.

Despite the risks, BYOD (bring your own device) is here to stay, particularly with a significant percentage of the population working from home. Employers can achieve a win-win scenario with strong BYOD policies, supported by appropriate technology and training.

Start with a Solid BYOD Policy

BYOD policies define the responsibilities of both the company and the employee regarding personal devices for business use, providing the framework for BYOD best practices. A strong policy should include at least the following:

- Acceptable use – Indicate items such as what company resources employees can use from their personal cell phones, a list of approved cell phones and appropriate methods for storing and sharing files.

- Guidelines for support – Specify what maintenance the company IT staff will provide and when the employee should contact their carrier for support. For instance, IT will typically install and maintain items such as security and productivity tools. The carrier should provide support for the phone itself.
- Ownership – Specify whether the company or the employee owns the applications and data on the cell phone.
- Lost or stolen phones – Outline notification procedures for employees to follow if their cell phone disappears. Also specify actions the company will take in the event of a lost phone, including remote wipe, if applicable.
- End of employment – Detail the procedure to follow to separate personal and business data when an employee leaves the company.
- Cell phone end of life – Specify procedures to dispose of old cell phones in a way that does not compromise sensitive data.

- Security policies – These should include policies for passwords, security updates, connecting to corporate networks, and so forth.
- Reimbursement – Indicate whether the company will reimburse employees for a portion of the cell phone costs. California law, for instance, mandates that employers provide reimbursement to employees who conduct business on personal cell phones.

Support Policies with Technology

Policies on paper do little without supporting technology and training. Where possible, automate policies. Additionally, take advantage of available technology solutions to help alleviate privacy and security concerns.

For example, mobile device management (MDM) solutions allow organizations to control which devices connect to the network. They also provide the capability to restrict access by job function and enforce application whitelists or blacklists. And if a cell phone with sensitive data becomes lost or stolen, the MDM provides remote wipe capabilities.

Containers, often in combination with an MDM, partition the cell phone, keeping personal and business operations separate. Thus, an employee’s personal applications cannot access business data, and vice versa. Additionally, when an employee leaves, containerization allows IT to remotely remove just the business data without affecting personal applications.

In addition to device management, various technology options allow employees to use multiple phone numbers from a single phone. This keeps personal numbers private and reduces confusion.

Deliver Timely Training

To get the most out of your BYOD policies and tools, supplement them with periodic user education. For instance, ensure that employees know how to protect their devices with strong passwords and multi-factor authentication. Teach them to recognize and appropriately respond to social engineering. And make sure they understand the policies and how to apply them.

Protect Employer and Employee with Cell Phone Best Practices

Navigating the BYOD landscape can prove challenging. eMazzanti will help you choose and configure the technology options best suited to your organizational needs. We understand the fine balance between convenience and security, and we have the tools you need to put cell phone best practices into place.