CHECKLIST

The Mobile Compliance Revolution is Here:
5 Proven Steps to Outpace Your Competition

In our mobile-driven world, businesses rely on mobile devices and applications to enhance productivity and communication. However, with this convenience comes a host of potential risks, from data breaches to compliance violations. As organizations navigate the complexities of mobile technology, it is essential to implement proactive measures that protect sensitive information while empowering employees.

Below, we outline five critical steps that businesses can take to mitigate risks associated with mobile devices. By establishing strong governance, capturing content effectively, defining supervision protocols, and committing to ongoing employee training, companies can create a secure and compliant mobile environment.

☐ Actively develop mobile device governance

All stakeholders and employees must review existing mobile device communication policies. Having this discussion can reveal whether policies that protect the business are empowering employees – or hindering their productivity. As part of governance, organizations should establish a mobility task force to:

- Assess the existing mobile environment
- Refresh policies per user group
- Update policies as new apps and functionalities are deployed
- Examine the latest trends and benchmarks

☐ Capture all mobile content

Everyone in your organization uses mobile devices and applications daily. It is critical to protect sensitive information and enable compliance. Strict regulatory requirements regarding digital communications are not going anywhere, and neither is mobile. It's crucial to support both. Businesses must focus on ensuring they can capture all mobile-based content, including unique metadata, emojis and GIFs, enabling the firm to adhere to regulatory guidance on digital communications more effectively.

Capture content the right way

It's vital that organizations capture mobile communications in their native form, complete with full context and metadata. In the U.S., this means being able to capture text content directly from mobile carriers such as AT&T, Verizon and U.S. Cellular, to name a few.

Having the ability to capture all the message types (e.g., SMS, MMS, RCS), including encrypted apps like WhatsApp, WeChat, Signal and Telegram, is essential to fully understanding sent and received communications. This applies to both corporate-owned and BYOD policies.

Content that's captured in native format with full context is extremely beneficial during e-discovery. Firms can quickly and easily review records in context rather than taking up resources to sort and compile information. A fast, effective e-discovery process can prevent costly legal fines and penalties

Proactively define supervision protocols

Communications supervision isn't just an ongoing requirement for regulated users involved in the marketing or sales of financial products. Supervision practices can also be used to inspect how business data and information are being shared across different mobile devices and apps.

Businesses should discover employee messages that violate corporate policies long before an investigation occurs. Proactive inspection of messages, including the use of prohibited apps, can help refine protocols and reduce compliance risks.

Train and retrain employees

Training employees isn't a one-and-done session. Businesses must review existing protocols, stay in front of demand for new tools and adapt to additional regulatory guidance. Training and continually retraining employees are integral steps for staying in front of risks.

Enhancing security in a mobile-driven world

Implementing these five essential steps will empower your employees while ensuring compliance and reducing the threat of data breaches or regulatory violations. Embracing a proactive approach will create a secure mobile environment that enhances productivity and allows your business to thrive in the digital age.