

BYOD Policy – Bring Your Own Device Policy

Everything you need to write your **BYOD policy (Bring Your Own Device policy)** and procedures for **Mobile Devices Security** all in one kit! It can scale to smaller banks simply wanting to take advantage of resources already available (such as Exchange ActiveSync); but it also scales to organizations looking to leverage some of the sophistications of Mobile Device Management applications (MDM.)

As a whole, our **BYOD Policy** kit addresses all **mobile device security** issues, from company-owned portable devices to employee-owned “**bring your own device**” smartphones and tablets. By starting where the FFIEC wants us to start— with a mobile risk assessment—and then ending with real-world device security decisions in the documents we use to help establish security standards. The risk assessment, of course, includes proposed declared controls that are covered by the mobile policy and procedure documents. The documents include inserts to be added to your existing Acceptable Use Policy and high-level IT Governance policy, and the **Portable Devices Security Procedure** also includes an agreement sign-off form that will establish user rights, and warn users of what exactly will happen due to some of the more intrusion security policies such as the potential remote wipe of their handheld device.

Save \$280 when you purchase the entire kit!
Only \$395.00

All templates are [color-coded](#), [updates](#) are free for three years and our boilerplates all come with a [30-day guarantee!](#)

The following are the actual documents themselves:

[Portable Devices Risk Assessment:](#) The FFIEC is clear about the need to conduct risk assessments focused on the deployment of new technologies. This document is an asset-based drill-down risk assessment that can be used to establish inherent and residual risk on vulnerabilities to smartphones (iPhones, Android Phones, Blackberries), tablets (iPads, Galaxy’s, Playbooks, etc.), and laptops. It allows you to declare existing controls and plan mitigating controls for Android and iPhone management as well as laptop management. It includes a handy asset inventory. Only \$145 individually, or purchase as part of the Mobile Devices Security Kit for \$395!

[Portable Devices Security Procedure:](#) (Mobile Devices Policy) The BYOD policy template you’ve been looking for! This user-level document governs how users are to use, secure, maintain, and return a portable device. It covers both authorized (BYOD . . . employee-owned) devices as well as issued (bank-owned) devices. The required controls it establishes are worded as a trade-off: “if you enforce these controls you get to put bank data on your phone.” Only \$145 individually, or purchase as part of the Mobile Devices Security Kit for \$395!

[Agreement to comply with Portable Devices Security Procedure:](#) This agreement is very important so that employees understand their obligations, responsibilities, rights, and vulnerabilities. The warnings in this agreement are paramount for a solid risk management approach, for warning employees of the pitfalls of remote wipe (you will lose your pictures and music), and also to smooth over some of the more unpopular inconveniences of the program (such as the right to audit). Only \$145 individually, or purchase as part of the Mobile Devices Security Kit for \$395!

[Agenda for Configuration Standards Meeting:](#) This document is intended to help your technical team walk through the issues that must be understood before implementing BYOD and MDM (mobile device management)

controls. It includes documentation such as how to tell if a device has been jailbroken as well as establishes discussion topics such as Apple Configurator and Exchange ActiveSync. Only \$145 individually, or purchase as part of the Mobile Devices Security Kit for \$395!

Portable Devices Configuration Standards: This document establishes all the technical security standards that must be met to properly enforce the modified Acceptable Use Policy and high-level IT governance policy as well as, of course, the Portable Devices Security Procedure. Again, it scales from a “poor-man’s approach” to technical control enforcement through the use of sophisticated Mobile Device Management applications (MDM). Only \$145 individually, or purchase as part of the Mobile Devices Security Kit for \$395!

Portable Devices Audit Checklist: This three-part audit checklist for mobile devices allows your technical team (or whomever is identified in your policy statement) to audit both BYOD devices and bank-issued devices. It includes an asset inventory as well as a checklist for smartphones, tablet pc’s, and laptops. Only \$145 individually, or purchase as part of the Mobile Devices Security Kit for \$395!