



SafeBoot Implementation for State Agencies - Frequently Asked Questions

Question 1: Is encryption on all state-owned notebooks mandatory?

Answer 1: Yes, state agencies must encrypt all notebooks. [Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data,"](#) requires state agencies to encrypt sensitive data on all state-owned notebooks, including tablet PCs. Because of the low costs associated with the SafeBoot implementation, state agencies are to encrypt all other notebooks to eliminate human error and the improper placement of sensitive information on unprotected notebooks.

Question 2: Is encryption on all *contractor-owned* notebooks mandatory?

Answer 2: Yes, state agencies must encrypt all notebooks. The requirement in [Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data,"](#) to secure sensitive data on portable devices also extends to contractor-owned notebooks. Because of the low costs associated with the SafeBoot implementation, state agencies are to encrypt all contractor notebooks that store state data. Again, doing so will eliminate human error and the improper placement of sensitive information on unprotected notebooks. State agencies can use a SafeBoot license to secure a contractor's machine, then remove the license file once the contractor is no longer performing a government function. Alternate notebook encryption solutions may be used by contractors if that solution complies with state of Ohio IT policies and standards, and if verification is provided to the state agency that the solution is currently in place.

Question 3: Is encryption on all state-owned desktops mandatory?

Answer 3: Encryption is mandatory for desktops containing sensitive data. Encryption is not mandatory for desktops without sensitive data; however, state agencies are urged to consider this level of security. The majority of state Ohio agencies plan on deploying some form of desktop encryption (full disk or file and folder encryption) and port control.

Question 4: Will SafeBoot encrypt removable storage media, such as CDs, DVDs, and USB drives?

Answer 4: The SafeBoot port control feature gives agencies the ability to set policy controls for removable storage media, including whether end-users may copy – and encrypt, if necessary - information to removable storage devices such as CDs, DVDs, USB drives. Removable storage media does not count as a device under the SafeBoot licensing model.

Silicon.com reports that 70% of company data theft comes from the use of portable memory devices such as USB drives. Implementing SafeBoot's port control functions helps minimize this risk.

Question 5: Is encryption on state-owned Personal Digital Assistants and cell phones mandatory?

Answer 5: Yes, for those devices that can hold sensitive data. [Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data,"](#) requires state agencies to encrypt sensitive data, especially mobile devices with sensitive data, in case the device is lost or stolen and the data risks compromise.

Question 6: Should our agency use Full Disk Encryption (FDE) or File and Folder Encryption (FFE)?

Answer 6: OIT generally recommends implementing FDE.

FDE is a method of encrypting every bit of data on a disk, including the operating system, swap space, and temporary files. FFE is a more selective approach to applying encryption that requires the end-user to actively and accurately identify and encrypt sensitive data. The benefit of FFE is that it minimizes the increase in access time incurred by disk encryption. Conversely, with FDE there is no need for end-users to select data to be encrypted, thereby eliminating the potential for human error. When in doubt, opt for FDE.

State agencies must use FDE on notebooks. The costs associated with a security breach due to a lost, unencrypted notebook are greater than the performance overhead of an entirely encrypted disk, or the cost of losing access to encrypted data due to a mishandled encryption key.

Question 7: My notebook is partitioned into multiple drives. Can I just encrypt the partition containing sensitive data?

Answer 7: No. For notebooks, state agencies must encrypt the entire physical drive, regardless of the number of logical drive partitions.

SafeBoot can be deployed on multiple operating systems such as Unix and Linux, if that is the purpose for the partition. Multiple partitions used to support data recovery solutions will also require encryption, as backed-up data is as equally vulnerable as active information.

Question 8: We use primarily Macintosh computers using OS X, how can we participate?

Answer 8: While a Macintosh OS X client is not available today, a version will be available from SafeBoot in the future. SafeBoot has agreed to include the Macintosh OS X client in the end-user license. As long as a corresponding end-user license has been purchased, Macintosh support will be available once that product ships from SafeBoot. Note that end-user licenses that can potentially be deployed on Macintosh have already been paid for during the offer period to lock in the current pricing.

Question 9: Who should we notify as to whether a SafeBoot implementation is complete?

Answer 9: Please communicate to the Chief Privacy Officer Sol Bermann at Chief.Privacy.Officer@oit.ohio.gov the following information as part of your agency's SafeBoot implementation plan:

- A timeline indicating deployment of the SafeBoot solution for the following devices:
 - notebooks,
 - other mobile computing devices (e.g., PDAs, smart phones), and
 - desktops;
- an update to the agency's report on data encryption implementation as required by [Executive Order 2007-013S, "Improving State Agency Data Privacy and Security,"](#) reflecting the agency's implementation of SafeBoot;
- any other security solution that complements the deployment of SafeBoot;
- whether the agency is primarily using Full Disk Encryption or File and Folder Encryption;
- audit reports from either the SafeBoot Management Center or some other report indicating the current status of SafeBoot implementation within the agency; and
- a statement indicating that all state-owned notebooks have been secured through full-disk encryption.

