



McAfee SafeBoot Endpoint Encryption Information (UTD Users)

What is SafeBoot Endpoint Encryption?

McAfee SafeBoot Endpoint Encryption is a tool used to fully encrypt the physical drives in computers, prohibiting access to the data without proper credentials. Encryption is a secure method of protecting confidential and sensitive data. This protection exists even if the computer is lost or stolen.

Why do we need Encryption?

The University of Texas at Dallas requires the encryption of all confidential and sensitive data based on UTS-165 and Security Practice Bulletin #1. This data includes: research, student information, and personally identifiable health information.

When do I get SafeBoot Endpoint Encryption?

We are going to be deploying SafeBoot Endpoint Encryption in phases based on departments, prioritizing the most critical data first.

How is SafeBoot Endpoint Encryption installed?

Information Resources and Departmental Techs will be installing SafeBoot Endpoint Encryption on each computer. It will immediately begin encrypting the drives and will take approximately 2-4 hours to complete. During the encryption process, you are able to login and use your computer. **It must remain powered on (does not have to be logged in) to complete the encryption.** You can check on the progress by right-clicking on the icon on the bottom-right corner and going to Show Status.

What are the risks with SafeBoot Endpoint Encryption?

Due to the possibility of hard disk failures, a backup of the computer is recommended. Please contact your responsible Technical Support Department to discuss backup options if you do not have any readily available to you.



McAfee SafeBoot Endpoint Encryption Signature Page

This must be signed by the user prior to installing SafeBoot Endpoint Encryption on the user's computer. This must be filled out for each computer that is going to be encrypted. Please return completed form to Information Security.

I, _____, understand that the possibility exists that McAfee SafeBoot Endpoint Encryption can cause irrecoverable errors involving my computer.

Please check one box:

In preparation for this possibility, I have taken the appropriate and recommended steps to protect my data from being lost. These steps include taking a backup of all important data and storing that backup in a separate location, making it possible to, in the event of an irrecoverable error, recover all important data.

I have reviewed the files on my system and determined that no backup is necessary. Encryption can be done without a backup of the data. If files are lost, I do not need to recover them.

User Signature: _____ Date: _____

NetID: _____

UTD Asset Tag: _____

Location of Computer: _____ (Building Name and Room Number)

For Technical Support Personnel Only:

Tech Signature: _____ Date: _____

Computer Name: _____ (Fully Qualified DNS Name)

Machine Group: _____ (According to SafeBoot)