LOK-IT ENCRYPTED USB –
Hacking Prevention and Drive Recovery

LOK-IT USB Drives are supplied by the University as a method to safely transport data. They are not intended to be used for primary data storage. The LOK-IT drives are the property of the University of Texas at Arlington. Loss or theft of these devices should be reported to the Information Security Office at 817-272-5487 or email Security@uta.edu.

Features
LOK-IT USB drives are encrypted drives that are protected by a 7 to 15 digit key entered on the USB’s keypad. The USB functions equally well on Windows, Mac, Linux, and other systems.

Your user “PIN,” or password, must be between 7 and 15 digits and cannot contain repeating numbers (1-1-1-1-1-1-1, etc.) nor sequential numbers (1-2-3-4-5-6-7, etc).

The LOK-IT USB drives will auto-lock when the drive is disconnected from the attached computer, or when it loses power. The drive contains a rechargeable battery that is charged when inserted into a USB port.

To prevent hacking and data loss, after 10 consecutive failed attempts to enter a PIN, the drive is wiped and all data will be lost. It is the user’s responsibility to remember their PIN. The drive is NOT intended for primary storage.

Hacking Detection and Prevention
After ten (10) consecutive unsuccessful PIN entry attempts to unlock the drive are detected, the following occurs:

1. The current encryption key is removed/zeroized.
2. Existing data becomes inaccessible
4. New User PIN must be set
5. Drive will require reformatting due to the creation of a new encryption key
6. Existing data is deleted
Each time hacking is detected, the current encryption key is zeroized and a new PIN must be set. Resetting a new User PIN will require a reformat of the drive due to the creation of a new encryption key which will delete all data on the drive.

**How to Recover Use of the Drive (Forgotten User PIN)**

If the User PIN is unavailable, there is no way to recover data, unless you have made arrangements with the Information Security Office to set a Master PIN. If no Master PIN option has been set, the only option is to reformat your USB Drive and all data will be lost. To Reformat and Set a new User Pin, see instructions on “Setting the User PIN.”

The use of the drive may be recovered by consecutively entering ten (10) incorrect PIN numbers which will activate the “Hacking Detection and Prevention” feature of the drive which will zeroize the encryption key and clear the user’s PIN. **The resetting of a New User PIN’s after this will require a reformat which will delete all stored data.**