LOK-IT ENCRYPTED USB –
User Instructions

LOK-IT USB Drives are supplied by the University to safely allow a method to 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 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 autolock when the drive is disconnected from the attached computer, or when it losses power. The drive contains a rechargable 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.**

Visual Indicators
**RED LED**
1. Red constant = Factory default state. Drive is locked. User PIN is not set
2. Red blink = Drive is locked. User PIN has been set.

**GREEN LED**
1. Green constant = Drive is connected to USB port and unlocked
2. Green single blink = Drive is unlocked in User Mode while powered by battery
3. Green double blink = Drive unlocked in Master Mode. This option is not usually configured by the University, Wait 30 seconds to allow the drive to go into the sleep mode and try again.
**RED LED/GREEN LED**
1. Red/green constant = Change of PIN initiated
2. Red/green single blink = Accepting User PIN input
3. Red/green double blink = Accepting Master PIN input. This option is not usually configured by the University, Wait 30 seconds to allow the drive to go into the sleep mode and try again.
4. Red/green alternating blink = A PIN entry error has been made; retry PIN entry

**BLUE LED**
1. Blue constant = Drive is unlocked and inserted into a powered USB port
2. Blue flicker = Drive is unlocked, inserted into a powered USB port and data transfer is occurring

**BLUE LED/RED LED**
1. Blue blink/Red blink = Drive has been inserted into a USB port while locked. The red LED will stop blinking. The blue LED continues to blink. Remove drive from port and enter PIN.

**NO LED**
All LED indicators off = Drive is in sleep mode

**Setting the User PIN**
The User PIN is clear upon delivery to the customer.

To set a User PIN:
1. Depress once and hold the KEY button for 3 seconds
   a. Only depress the KEY button Once, a double press will enter into the Administrator Master PIN menu which is not usually configured by the University.
2. When both red/green LED’s illuminate, release the KEY button
3. Red/green LED’s will blink once and remain lit for 10 seconds indicating accepting the User PIN is initiated.
   a. If the red/green LED’s double blink, the KEY button was pressed more than once. Wait 30 seconds until the USB Drive goes into the sleep mode, then start over at Step 1.
4. Enter a User PIN between 7 and 15 digits before the drive reverts to sleep mode
5. Press the KEY button
6. Both red/green LED’s will now single blink in unison for 10 seconds before reverting to sleep mode
7. Re-enter the User PIN
8. Press the KEY button
9. A continuous green single blink confirms the User PIN is accepted
10. Insert the USB drive into a USB port within 30 seconds
11. Upon initial PIN setup a format operation is required. Follow on-screen prompts for formatting the drive. The Quick Format option is acceptable. This step will not be required after initial PIN setup or when changing the PIN.
   a. Select “Format disk”
   b. Enter Volume Label if desired
   c. Quick Format option is acceptable
   d. Select “Start” to begin the format.
e. For MAC’s select “Initialize”, select “Partition”, select the “+”, click “Apply”, then “Partition” to Format the drive...

It is recommended that users format with “FAT32” or on a Windows PC if they envision using the USB on Mac’s and Windows devices.

12. If a mistake is made entering the User PIN an alternating red/green LED blink is displayed indicating an error has been made. Start over beginning at Step 1.

Sleep Mode - If the drive reverts to sleep mode at anytime start over beginning at Step 1
How to Unlock Drive with the User PIN

To Unlock the drive with the User PIN:

1. Press and release the KEY button one time.
2. **Red/green** LED’s will single blink in unison for 10 seconds before reverting to sleep mode
   a. If the **red/green** LED’s double blink, the KEY button was pressed more than once. Wait 30 seconds until the USB Drive goes into the sleep mode, then start over at Step 1.
3. Enter User PIN before the drive reverts to sleep mode
4. Press the KEY button
5. **Green LED** will single blink to indicate the drive is unlocked
   a. If an incorrect PIN was entered, the **red** LED will light indicating the drive remains locked. Start over beginning at Step 1.
6. Connection to a USB port needs to be made within 30 seconds.
   a. If no connection is made within 30 seconds the drive will re-lock and enter sleep mode.
   b. If AutoPlay is allowed for windows you may see a pop-up window like the one pictured below.
7. When connected to a USB port the **green** and **blue** LED’s will illuminate in a constant state indicating the drive is ready for use.

Sleep Mode - If the drive reverts to sleep mode at anytime start over beginning at Step 1

How to Change User PIN

To change your User PIN:

1. Unlock the drive with the existing User PIN (see previous section for instructions)
2. With the drive unlocked, depress and hold the KEY button once for 3 seconds
3. When both **red/green** LED’s illuminate, release the KEY button
4. **Red/green** LED’s will blink once and remain lit for 10 seconds indicating accepting the User PIN is initiated.
   a. If the **red/green** LED’s double blink, the KEY button was pressed more than once. Wait 30 seconds until the USB Drive goes into the sleep mode, then start over at Step 1.
5. Enter a User PIN between 7 and 15 digits before the drive reverts to sleep mode
6. Press the KEY button
7. Both red/green LED’s will now single blink in unison for 10 seconds before reverting to sleep mode
8. Re-enter the User PIN
9. Press the KEY button
10. A continuous green single blink confirms the User PIN is accepted
11. You may then Insert the USB into a USB port, and your drive should be available
   a. It is not mandatory to insert the USB Drive
12. If a mistake is made entering the User PIN, alternating red/green LED blink is displayed indicating an error has been made. Wait until the drive reverts to the sleep mode, and start over beginning at Step 1.

Sleep Mode -If the drive reverts to sleep mode at anytime start over beginning at Step 1

How to Lock the Drive after Attaching to a USB Port
1. Disconnect drive from USB port
2. LED’s will turn off
3. Drive auto-locks and enters the sleep mode

Activation from Sleep Mode
1. Press the KEY button (numeric keys will be ignored)
2. Red or green LED will illuminate to show the drive status
   a. Red = Locked
   b. Green = Unlocked

How to Unlock Drive with a Dead Battery
1. Connect the drive to a USB port or extender cable.
2. Follow instructions in ‘How to Unlock Drive’.

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 “Setting the User PIN” section above.

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. **Resetting of a New User PIN’s after this, will require a reformat which will delete all stored data.**