SECURE DRIVE

SecureDrive® KP Best Practices

SECUREDRIVE® KP

Your SecureDrive KP is shipped ready to use straight out of the box. Follow these steps to get started:

FIPS LEVEL 3 VALIDATED 140-2

1. Unbox the drive and find the appropriate included cable for your system – either USB-A or USB-C.
2. Connect the drive directly to your system, avoiding the use of adapters or hubs.
3. Adjust your USB power settings to prevent the drive from losing power and locking due to power-saving features. (See documentation for more information: https://www.securedrive.com/documents/Power-Management-in-Windows-and-macOS-for-SecureDrives.pdf)
4. The drive comes pre-formatted to NTFS. If you're using a Mac, reformat the drive to macOS or exFAT. Note that Mac OS can read NTFS but cannot write to the drive.
5. Once power is connected, the red lock will be on and steady.
6. The factory default PIN is 11223344. Press the Key button, enter the PIN, and press the Key button again. The red lock will flash during PIN entry.
7. A green lock indicates the drive is unlocked, while a blue light signifies the drive is connected. You may need to use Disk Management to assign a drive letter.
8. Change the user PIN as instructed in the manual (https://www.securedrive.com/wp-content/uploads/2017/03/SecureDrive-KP-User-Manual-20190228A.pdf).
9. Make sure to press the keys firmly, and be deliberate, do not rush
10. If providing the drive to an employee, it's highly recommended that you create an Admin PIN.
11. Refer to page 8 for instructions on Admin functions. Setting an Admin PIN grants an additional 10 attempts to unlock the drive if the user enters the wrong PIN 10 times.
12. Admin can also set Read Only Mode so the drive cannot be written to
13. We recommend setting up antivirus protection, one year license for DriveSecurity(r) included with drive purchase https://www.securedrive.com/product/drivesecurity

Care and Use Instructions:

- Take care when handling
- Do not write PIN on the drive with a sharpie or use a sticky note
- Keep the drive safe from water and damage when carrying by keeping the drive in the provided splash-proof case when not in use
- Avoid sudden drops or rough handling, as abuse can harm the internal drive
- Please remember you only have 10 attempts to unlock the drive
- The drive is crypto-shredded after 10 failed attempts
- Admin will have 10 additional attempts to unlock if feature is set
- Data recovery is impossible after the data is shredded
- User will need to reset drive and create new PIN and format to use again
- Use safe eject to disconnect the drive

Bluetooth Options:

- SecureData also offers a Bluetooth version, allowing you to manage drives remotely.
- Admins can remotely unlock, wipe, and reset PINs.
- Contact us for more information on the Bluetooth version at sales@securedrive.com

MORE ONLINE

For more features and for troubleshooting, see the SecureDrive KP Model User Manual on our website: **https://www.securedrive.com/documents/user-manual-securedrive-kp.pdf**

REGISTER YOUR DEVICE

To register your drive on your SecureData account, go to **https://www.securedrive.com/register**

www.securedrive.com
support@securedrive.com

USA: **1-800-875-3230**
International: **+1-323-944-0822**

SECURE DATA

Rev. 20190930_EN