



AMACOM

DATA LOCKER

PIN Protected AES Encrypted USB 2 Hard Drive



With the increase in mobile workers and data portability, there is an increased risk that your sensitive and confidential data could fall into the wrong hands. Make sure your data is secure with the Amacom Data Locker.

The Data Locker is a portable USB 2.0 hard drive that is 128 or 256 Bit AES hardware encrypted ensuring that all your data is secure whilst on the move.

By utilising hardware encryption that is integrated into the Data Locker, there is no performance decrease in read and write operations. Hardware based encryption combined with the unique LCD Touch Screen authentication system also means that the Data Locker is platform independent, requiring no device drivers or software to be installed.

The Data Locker's LCD Touch Screen allows you to enter up to an 18 digit PIN which gives you access to your data. Because the authentication is carried out on the Data Locker and not your computer, keyboard loggers, brute force attacks and viruses cannot give third parties access to your data.

Benefits:

- **Highest Level Of Protection**
- **No Drivers Or Software**
- **Quick & Easy To Use**
- **Secures All Your Data**
- **PIN Entered On Data Locker**

Hardware Encryption

The Data Locker is designed using industry standard AES Cipher Block Chaining hardware encryption, with either a 128 Bit or 256 Bit key length. This level of encryption is the same high level encryption standard used by Government departments to secure highly sensitive data. The encryption chipset used in the Data Locker is certified by the NIST to fully comply with the FIPS 197 certification standard and FIPS 140-2 certification has been applied for. Additionally the Data Locker's level of security is enhanced further by the use of an encryption key which is user generated and unique to each unit.

Self Destruct Mode

Should your Data Locker be lost or stolen you can be sure that your data will remain secure. If someone attempts to guess your PIN and gain access to your data, the Data Locker's Self Destruct Mode will count the number of times it is entered incorrectly and after each third incorrect attempt will shutdown requiring the Data Locker to be turned off and on again. Should the number of times the PIN is entered incorrectly reach a total of nine the Data Locker will permanently erase the encryption key. With no encryption key to decrypt the data stored on the Data Locker your data will become permanently unrecoverable by the person attempting to gain access to it or by yourself.

Platform Independent

By utilising an integrated hardware encryption chipset and the unique LCD Touch Screen authentication system the Data Locker provides users with a truly platform independent, secure portable hard drive. Users enter their 6 to 18 digit PIN directly into the Data Locker by using the numeric keypad on the LCD Touch Screen, only once the correct PIN has been entered can the Data Locker be seen by the computer and your data accessible. As all of the encryption and authentication is carried out within the Data Locker there is no need for users to install any device drivers or software on their computer, which means that the Data Locker can be used on both PCs and Macs. Threats from infected systems, keyboard loggers or brute force attacks are also eliminated because there is no interaction with the computer during authentication.

Origin Storage Limited
2-4 Rutherford Centre
Rutherford Road
Basingstoke, Hampshire
RG24 8PB, United Kingdom

Tel: +44 (0)844 288 6868

Origin Storage Limited
B.C.Sittard
Dr. Nolenslaan 157
6136 GM Sittard
Nederland

Tel: +31 (0)467 111 201

Malware Protection

Some of the latest Viruses and Trojans have the ability to attack the boot sectors and file allocation tables of hard drives, which can cause data to be lost. The Data Locker helps prevent these types of malware from causing data stored on it from being lost by implementing a hardware based Malware Protection system. When an attempt is made to delete or modify areas of the Data Lockers hard drive that could cause data loss the user is prompted for confirmation on the LCD Touch Screen that the actions are to be allowed. This means that automated processes, such as malware, cannot erase your data.

Administrator Control

The Data Locker can be used by an individual user without any central administrator intervention before deployment. However for organisations which have central security policies which need to be complied with the Data Locker Enterprise edition allows the organisations IT Manager or Security Officer to configure the Data Locker with an Administrator PIN. Once set the Administrator PIN allows security or IT departments to access a users data without knowing the users PIN, allowing them to recover data should the user forget their PIN or leave the organisation. The Administrator PIN can also be used to quickly and easily redeploy a Data Locker to a new user by allowing them to erase the encryption key and reset the Data Locker to its defaults, all whilst ensuring previous data stored cannot be accessed by the new user.

Technical Specifications

Capacities:	160GB, 320GB & 500GB
Drive Specifications:	2.5 Inch SATA, 5400 RPM, 8MB Buffer
Interface:	Hi Speed USB 2.0
Bus Transfer Rate:	Up To 480Mb/Sec
Operating Temperature:	5 to 55 degrees C
Operating Shock:	2,940m/s ² (350G) 2ms
MTBF:	>300,000 power on hours
Dimensions:	127mm x 76mm x 20mm
Weight:	256 grams
OS Compatibility:	Compatible With All

www.datalockerdrive.eu