CSSi SA - "Securing Tomorrow, Today"
Waterfall Office Park, 28 Augrabies Rd Vorna Valley, Midrand, 1685
Generated: 2026-11-07 19:40



Kingston Technology IronKey 32GB Vault Privacy 50 AES-256 Encrypted, FIPS 197

Model: IKVP50/32GB

Manufacturer: KINGSTON

EAN: 740617329056

Product Code: 974322

R3,071

Kingston IronKey™ Vault Privacy 50 series are premium USB Type-A and USB Type-C®* drives that provide enterprise-grade security with FIPS 197 certified AES 256-bit hardware-encryption in XTS mode, including safeguards against BadUSB with digitally-signed firmware and against brute force password attacks. VP50 has been penetration tested***** (pen tested) for enterprise-grade security. Because it provides encrypted storage under the user’s physical control, the VP50 series is superior to using the internet and Cloud services to safeguard data.

The product information provided is for reference purposes only. Technical specifications, photos, descriptions and prices may change without prior notice. The manufacturer and seller are not responsible for possible data discrepancies or typographical errors. We recommend checking the current information before purchasing.

Vault Privacy 50 supports multi-password options (Admin, User and One-Time Recovery) with Complex or Passphrase modes. This enhances the ability to recover access to the data if one of the passwords is forgotten. Traditional Complex mode allows for passwords from 6-16 characters using 3 out of 4 character sets. The new Passphrase mode allows for a numeric PIN, sentence, list of words or even lyrics from 10 to 64 characters long. Admin can enable a User and a One-Time Recovery password, or reset the User password to restore data access. To aid in password entry, the “eye” symbol can be enabled to reveal the typed-in password, reducing typos that lead to failed login attempts. Brute force attack protection locks out User or One-Time Recovery passwords if 10 invalid passwords are entered in a row, and crypto-erases the drive if the Admin password is entered incorrectly 10 times in a row.

To protect against potential malware on untrusted systems, both Admin and User can set Read-Only mode to write-protect the drive; additionally, the built-in virtual keyboard shields passwords from keyloggers or screenloggers.

Organisations can customise and configure VP50 series drives with a product ID (PID) for integration with standard endpoint management software to meet corporate IT and cybersecurity requirement through Kingston’s Customisation Programme.

Small and medium businesses can use the Admin role to manage their drives locally, e.g. use admin to configure or reset employee User or One-Time Recovery Passwords, recover data access on locked drives and comply with laws and regulations when forensics are required.

Vault Privacy 50 offers fast dual-channel performance on all capacities. The drive is waterproof with IPX8 rating****, TAA compliant and assembled in the USA.

Hardware-encrypted USB drive for data protection

Safeguard important data with FIPS 197 certified XTS-AES 256-bit encryption. Built-in protections against BadUSB, brute force attacks and pen tested for enterprise-grade security.

Multi-password option for data recovery

Enable Admin, User and One-Time Recovery passwords. Admin can reset a User password and create a One-Time Recovery password to restore User’s access to data. Brute force attack protection

The product information provided is for reference purposes only. Technical specifications, photos, descriptions and prices may change without prior notice. The manufacturer and seller are not responsible for possible data discrepancies or typographical errors. We recommend checking the current information before purchasing.
shop.cssi.co.za | sales@cssi.co.za | +27 (11)541-9950

locks out User or One-Time Recovery passwords if 10 invalid passwords are entered in a row, and crypto-erases the drive if the Admin password is entered incorrectly 10 times in a row.

New Passphrase mode

Select between Complex or Passphrase password mode. Passphrases can be a numeric PIN, sentence with space characters, list of words or even lyrics – from 10 to 64 characters long.

Dual read-only (write-protect) settings

Avoid malware attacks with a forced Read-Only mode set by Admin for User, or a session-based Read-Only mode set by Admin or User.

Locally manage drives for small and medium businesses

Use Admin role to locally manage employee User and One-Time Recovery passwords, recover data access on locked drives, and comply with laws and regulations when forensics are required.

Additional security features

Reduce failed login attempts and frustration by enabling “eye” button to view the password typed. Use virtual keyboard to shield password entry from keyloggers and screenloggers.

The product information provided is for reference purposes only. Technical specifications, photos, descriptions and prices may change without prior notice. The manufacturer and seller are not responsible for possible data discrepancies or typographical errors. We recommend checking the current information before purchasing.
shop.cssi.co.za | sales@cssi.co.za | +27 (11)541-9950