dcirrus

Advanced Security Features

Every data room comes with following security features -

- **Unique Corporate ID**
- **Session Time-out**
- **Watermarks with personally-identifiable information**
- **Customizable NDA**
- **Two Factor Authentication**
- **Device Level Approval**

Need further information?

Contact Us.

For more information about DCirrus, please visit:

dcirrus.com

Security Parameters

DCirrus Virtual Data Room platform comes with multi-layer security to keep your confidential data safe and secure.

Data Protection

All our Data Rooms comes with in-built security to ensure that your Due Diligence process remains secure at all times and only authorized users can access the same.

Encryption of Data	256-bit encryption of all data, both in transit and at rest.
Secure Connections	All connections are protected using TLS 1.2, 1.3 with a 256-bit symmetric encryption.
Password Protection	Passwords are masked with one way encryption, seperate salt and encrypted with MD5 and on top of that another level of encryption.
Data Center Protection	While at the data centers, all data remains encrypted using 256-bit AES, which is certified for use by governments and security agencies.
Disk Encryption	Data disks are encrypted with 256-bit AES encryption
Offsite Backup for Disaster Recovery	We store all information in multiple data centers, which are located in any geographic region selected by the customer themselves. We take daily backup of data disk to prevent data loss in case of any disaster.
Privacy	DCirrus never accesses your confidential data and all access of data is properly logged

dcirrus

Data Protection

DCirrus leverages the power of Amazon Web Services (AWS) data centers to run its infrastructure and to protect user's confidential data in their own geographic region complying with local data protection laws.

Secure Data Center Location	Locations all over the globe where AWS provides their data centers.
Network Security	AWS takes a diversified approach to ensuring network security, such as segmentation, firewalls, and intrusion detection, among others.
Third-Party Examination Reports	Service Organization Control (SOC) Reports 1, 2, & 3.
ISO 27001 Certified Data Centers	Security measures include; electronic key-cards, pin codes, biometric hand scans, and onsite security officers 24 hours a day, 365 days a year.

Additional Security Features

Our default additional security features gives you confidence to exchange your confidential data with full control

Multi-Factor Authentication (MFA)	DCirrus offers both SMS, email and Microsoft Authenticator for secured login
Permission Based Access	Folder and file based access to ensure only authorized users have access to the specific information.
Audit Trail	Track system activity by user, date, time, and action taken.
Device Level Permssion	Device approval process by mapping the unique ID of the device
IP Address Control	User based unique IP address login
Digital Rights Management	Prohibition of printing, copying, sharing and setting up of expiry date of the downloaded files

Additional Questions?

If you have additional questions about DCirrus security, please email contact@dcirrus.com