14

What security measures does REACH CAD implement for collaborative projects?

14 What security measures does REACH CAD implement for collaborative projects?

REACH CAD's security measures for collaborative projects include :

1. Access Control and Authentication

(i) REACH CAD implements robust access control measures, including:

(ii) Multi-factor authentication (MFA) to verify user identities.

(iii) Role-based access controls to restrict permissions based on user roles.

(iv) Password protection for sensitive files and projects.

2. Data Encryption

To protect sensitive design data, REACH CAD uses:

(i) End-to-end encryption for data in transit and at rest.

(ii) Strong encryption standards like AES-256 or RSA-20483.

(iii) Secure Data Storage and Backup

For data integrity and disaster recovery, REACH CAD offers:

(i) Secure cloud storage using reputable providers like AWS or Google Cloud.

(ii) Regular automated backups of project data.

(iii) Data replication across multiple secure data centers.

3. Audit Trails and Monitoring

To track activity and detect potential security issues:

(i) Project audit logs to record user actions and changes

(ii) Activity tracking and monitoring of user behaviors

4. Collaboration Controls

For secure sharing of design data:

(i) Granular permissions to control file/model access and editing rights.

(ii) Secure file sharing capabilities with external partners.

(iii) Version control to track changes and revert if needed.

5. Additional Security Measures

(i) Regular security updates and patches.

(ii) Employee security awareness training.

(iii) Compliance with data protection regulations like GDPR.

These security features of REACH CAD secure collaborative projects and protect sensitive design data.

For more information on how REACH CAD can add value to your business, please email ***info@reach-tech.com*** *and visit* ***www.reach-tech.com***

enabling agile apparel enterprises
for the digital economy

www.reach-tech.com
info@reach-tech.com

RT