

# DealRoom Security



A photograph showing a close-up of a business meeting. Several people in business suits are seated around a table. One person's hands are visible typing on a white laptop keyboard. Another person is holding a pen over a document. The scene is brightly lit, suggesting an office environment.

# DealRoom Security

At DealRoom, we understand the importance of data security and maintaining confidentiality during deals. Our software was built and designed with security as a priority.

Dealroom not only meets industry security standards, but goes the extra mile to ensure all information is kept secure and documents are protected. Our platform's security measures provide clients with controls, reporting, and procedures required to keep all their data and operations safe. We go above and beyond industry standards to reduce risk and eliminate security fears.

We take a comprehensive, multi-faceted approach to secure online files. Several complex layers work together to create an all-encompassing barrier against potential risks and threats.

This PDF goes over DealRoom's security features in detail including:

- Physical security
- Application Security
- Infrastructure Security
- Data Center Certifications
- Auditing and Compliance
- and more

# 01. Physical Security

## 1.1 Modern Multi-Layered Security System

### **| Uptime Over 99.9%**

At DealRoom, we take customer service just as seriously as security. We have consistently met or exceeded 99.9% uptime. We extremely rarely have scheduled maintenance, and if we do, users are notified well in advance, and maintenance occurs at off-hours.

## 1.2 Continuous Data Backup

All our servers and customer data are automatically backed up daily. If hardware failure or an AWS outage should occur, all customer data can be fully recovered.

# 02. Application Security

## 2.1 Data protection

All data is encrypted and protected in transit and at rest, which prevents unauthorized data visibility.

## 2.2 Role-Based Access Control & Data Sharing

DealRoom offers flexible data access control setup by allowing admins to configure Customized Access Roles, which offer the choice of more than 20 different permissions for user actions in DealRoom, and can be used to specify user or group access levels to certain folders, projects, and tasks. Selective sharing can be enabled to not follow the default of inheriting sharing settings, giving greater access control over specific subfolders and Subprojects. DealRoom's Audit Logs allow administrators to holistically review user access to sensitive data.

A DealRoom account administrator manages and controls individual user rights by granting specific types of user licenses.

Customer data, including tasks and folders, can only be accessed by other users within your DealRoom account if those items were specifically shared with them, or if the items were placed in shared folders.

Users can personalize allowances for access and permissions, and the software supports existing workflows and processes. Admin teams can also set controls across all users.

## **2.3 Dynamic/Static Watermarking**

Decide what documents need a watermark with the click of a button. Watermark text and transparency can be adjusted.

## **2.4 Data Siloing in private cloud servers**

Data can be stored in private cloud servers. This allows for data to be stored and accessed by the appropriate parties.

## **2.5 Multi-Factor Authentication**

Utilizes strict, single-user ID and password protocol – Strict single-user ID and password protocols protect all your data. Each user has their own unique login.

Two-factor authentication, and adaptive Multi-Factor Authentication (MFA) – MFA reduces the risk of password theft. It requires users and administrations to login with two factors.

## **2.6 Accident Redemption**

Disaster recovery with repeated failover capabilities and data center recovery testing.

## 03. Infrastructure Security

### 3.1 Data Encryption

All data is supported by 256-bit AES data encryption.

### 3.2 Worldwide Network

We have a global storage network of remote data centers that is strategically separated in order to prevent data destruction. This also speeds data recovery should a disaster occur through real-time replication, multiple connections, and alternative power supplies.

All DealRoom personnel are screened and bound by strict confidentiality agreements.

## 04. Data Center Certifications

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2 Type II (formerly SAS 70 Type II)
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

We support our clients' regulatory compliance needs. DealRoom readily adapts to the ever-changing demands of regulatory compliance — so you can always be at the top of your game.

- 21 CFR Part 11 for electronic records
- FINRA
- FISMA
- Gramm-Leach-Bliley Act (GLBA)
- HIPAA
- HITECH
- SEC Rule 17g-5
- SEC Rule 17g-4

## 05. Auditing and Compliance

DealRoom's platform logs all user activity for all documents and provides detailed reports on how users interact with the shared content.

These records create a "paper trail," ensuring that your organization maintains compliance with organizational and industry regulations. You have complete control over each secure document throughout the entire content lifecycle.

## 06. Infrastructure Security

Almost everything within the room can be exported. Users can archive/unarchive things, such as documents and requests, and admins can permanently delete documents from the archive. Changes to the room can also be accessed via the analytics tab.

Even after a user has been removed from a room, the information added by that user can still be accessed.

## 07. Monitoring User Activities

DealRoom enables teams to quickly create reports with real-time account activity data, such as request progress, user activity, and document activity. There is also an exportable audit log tab that tracks all activity by every user in the room.

