

# Security and Management

Brainloop's Document Compliance solution enables companies to work on and share strictly confidential documents both internally and with other companies. It provides strong encryption and protects all documents from unauthorized access by internal or external attacks, creating a high-security collaboration environment. The solution also provides traceability, logging every access and action, to meet compliance requirements. Typically, it is used for board-level communications, for collaboration with external partners, and in financial and contract management.

## Your benefits at a glance:

- › Consistent protection from unauthorized access by system and application administrators
- › Restrictive access control
- › End-to-end encryption throughout the document lifecycle
- › Audit trail for complete traceability of all actions
- › Security categories for consistent implementation of enterprise security policies
- › Integrated rights management technologies to protect documents after they reach users and their PCs
- › Available as a SaaS service – hosted in a high-security, certified data center
- › No installation necessary on the client side
- › Servers are available in several different countries to comply with regional data protection laws

## Protecting confidential documents with Document Compliance Management throughout the enterprise

A company's security and compliance requirements with regard to document protection can only be met with a secure solution that can be implemented across all departments. A particularly high level of protection is required for confidential documents such as financial information, personally identifiable information, and strategy papers – especially if they are being shared with external third parties or need to be safeguarded from unauthorized access.

## SECURITY DELIVERS DOCUMENT COMPLIANCE

### Operator shielding

The Brainloop Server is an application platform where multiple tenants and their virtual data rooms coexist while being completely shielded from one another. Every data room has its own keys and security configurations and can be managed independently of the application itself. A key feature of this architecture is the consistent segregation of data room management, application administration and the system and infrastructure administration tasks. From a technical perspective, it is a Microsoft .NET application that uses MS SQL to store configuration and

system data. The documents to be protected are not stored in the database. Instead, they are encrypted and stored on a NAS server.

### Data room Center

A dataroom center is an encapsulated, logical tenant with separate administration and which contains several data rooms. The data room center facilitates consistency in user management, security policies, templates, style sheets, reporting and accounting across all the datarooms.

### Integrated user management

Each data room has its own user management functions. Users are identified by their email address



and a password they have chosen themselves. Requirements concerning password length and aging can be set using the Password Policy, and additional authentication methods can be configured for each data room.

### Managing security categories

Companies can define individual security categories that directly implement their own information protection policies. This makes permissions management much easier. The authorized manager simply clicks on the relevant category to select it and apply it to individual documents or to entire folders. Typical security categories include Internal Use Only, Secret and Strictly Confidential. Permissions can be defined and attached to the categories. An example of how these are used is to set the properties of a Brainmark document version for a specific user.

### Access control and password protection

To avert manual or automatic testing of passwords and tokens, each failed attempt is logged together with the IP address and this information is provided to the application administrator. A user account can also be blocked for a limited configurable time period if the user fails to enter the right password after a predefined number of attempts.

### Two-factor authentication

A further option is to activate token-based authentication. A one-time password is sent by text message to the user's cell phone. The user then enters it immediately for authentication. This option can be activated for every data room or for a single critical operation, such as a user registering

for the first time or to access a data room's security configuration. Settings are available that define how often users must re-authenticate with the token – every time they log in, once a day, once a week etc. Using text message tokens is useful when working with other companies, as most people have a cell phone and usually notice very quickly if it has been lost, enabling it to be blocked. Users who do not have a cell phone can receive their token by email instead.

### Certificate-based authentication

Companies with an existing certificate-based infrastructure for authentication can integrate it seamlessly into the system. Both software and hardware-based certificate systems (chip cards etc.) are supported.

### Session timeouts

To avoid intrusion via an unattended computer, sessions are automatically terminated if there is no activity. The length of the timeout is freely configurable.

### URL hashing

URL hashing allows the application to detect whether a URL has been generated by the system or externally. This prevents attacks via manual or automatic URL testing.

## DOCUMENT PROTECTION ON THE SERVER

### Strong encryption for document storage

Confidential documents can be stored on the server in a strongly encrypted format, giving them consistent protection from unauthorized access.

The documents are encrypted using the Advanced Encryption Standard (Rijndael algorithm) with a key length of 256 bits. Every data room has a separate key, and as the keys are managed by the application itself the process is transparent to users.

### Encryption invisible to service providers

Encryption and key management are completely invisible to the service provider or operator. Personnel from the internal or external provider can monitor the system and ensure that it works properly, and can back up and restore data. However, they never have access to confidential documents or individual keys. The strict segregation of application and system administration duties, along with dual control for security-related administration functions, ensure the highest levels of confidentiality. This naturally also applies to servers operated in an external data center by an external service provider.

### Permissions system

Brainloop's flexible, role-based permissions system enables the precise definition and monitoring of roles and permissions for every data room user. Also, permissions are only assigned within a data room. As a result, application administrators never have access to confidential documents. Access rights can be allocated with a high level of granularity, making it easy to define exactly what each person may or may not do with a document. The permissions system also enables the configuration of a "Chinese wall" that blocks off groups of users so that they are invisible to each other, even



within a single data room. Rights can be inherited throughout a folder hierarchy, making allocation easier. In addition, complex permission schemes can be created as a template, then stored and reused at a later date.

#### Protection of data integrity

Document fingerprinting is used to identify a specific version of a document's content. As soon as a document is modified, the fingerprint changes in parallel. This enables the system to check that the document content has not been altered outside of the Brainloop application – for example after a document has been downloaded or as a result of an external attack. Other database entries are protected in a similar way using cross-references and checksums. This prevents unauthorized access by an attacker with database privileges.

#### Tamper-proof audit trail

Every activity, whether on an application, data room or object level, is time-stamped and logged in a tamper-proof audit trail. These activities include configuration changes as well as document access, downloads, changes, uploads, and opening within the Secure Document Viewer. Users can only see the information for which they have the relevant permissions and access to the audit trail can be limited. Also, the application ensures that the audit trail cannot be altered at a later date.

#### Document protection during transmission

The system provides encrypted data transmission that protects every transfer of data between the local browser

and the server (document upload and download, views of data room content etc.). Data is transmitted over HTTPS and encrypted with 128-bit standard SSL. This also applies to the communication of files and file names via the Web DAV interface.

Operating a Brainloop Secure Dataroom Server requires a fixed IP address, a DNS name, and a valid SSL certificate, for both the web browser and the WebDAV interface.

#### Sending documents securely

A user can send a document to other people without it leaving the protection of the data room, as addressees simply receive an email containing a link. In addition, the user can select only the recipients with permissions for that document.

The addressee simply clicks on the link in the email to open it. This function is also available for sending documents to users who are not members of a data room. This is achieved by sending a temporary link that can be disabled within the data room at any time. Authorized users can create a security policy that defines how a document should be provided to external users and the level of granularity of the access log.

#### Secure email

Users can send each other encrypted emails from the data room to facilitate communication and collaboration. Users with a client certificate (X.509 v3) will then receive their emails in encrypted form. Recipients without an appropriate certificate in their profile will simply receive a substitute email that refers to the original message. In

this case, the original message is added to the user's personal inbox in the data room. This prevents unauthorized users from accessing confidential information. The same type of protection is also used for emails that the system sends to a user.

#### DOCUMENT PROTECTION ON THE RECIPIENT'S COMPUTER

#### Brainmark for secure document delivery

As an alternative to sending the original format, users can specify that a document can only be downloaded with a Brainmark on it. This type of secure download delivers a version of the document to the client that is generated and protected automatically. Security policies are used to define whether a Brainmarked download delivers the document as a simple but clearly-marked print version with all edits and annotations removed; whether it should include a personalized watermark; and whether it should be read-only with no permission to print or forward it. PDF is used as the basic format for a Brainmarked document. The application adapts automatically to the specific capabilities of the client PC and determines whether appropriate client certificates, Microsoft RMS or Adobe Live Cycle can be used.



**Brainmark**

A Brainmarked download delivers a version of the document that is generated and protected automatically. The user can choose between different security levels.

**Examples**

- › The document can be delivered as a simple but clearly-marked print version with all visible edits and annotations removed.
- › The delivered version can include a personalized watermark if required
- › The document can be delivered as a read-only version with no permission to print or forward it

**Clearly marked printouts**

Brainmarked documents are protected against changes and include a clearly visible identifier. This unique number enables the document to be tracked, even after it has been copied, printed or forwarded.

**Watermarks in documents**

Watermarks personalized for each user can be configured in the data room and included in the document view when the document is downloaded via the secure viewer. This makes it more difficult for recipients of a confidential document to intentionally or unintentionally copy the document by making a screen shot of it.

**Document display with the Secure Document Viewer**

The Secure Document Viewer opens a document in the browser for reading only and with no way of saving it. This type of display is available to any

user with a browser. The server-side rendering breaks up the document content and displays it as tiled images in the browser, so the user never sees the whole file. This makes it very difficult and time-consuming, if not impossible, to print or forward the file.

**Document display with Information Rights Management (IRM)**

Companies with very stringent security requirements can use IRM to ensure that users can only download a document on their own PC in order to read it. A security policy embedded in the document can trigger the conversion of an Office document to PDF, add a watermark if required, and apply Adobe LiveCycle Rights Management to it. The file is then encrypted and stored on the client PC with explicit information regarding what the user is permitted to do with the document. When users open it on their PC, they must authenticate themselves on the IRM server and prove that they have a temporary viewing license. This process is usually invisible to users as it is executed directly by Acrobat Reader 9.0 or higher. Users with an older version of the Acrobat Reader can only view the document in the Secure Document Viewer.

Adobe LiveCycle's IRM protection can also be configured to allow a user to open a document offline for a limited period of time. However, this function requires a certificate generated by Brainloop to be added to the user's profile. The certificate is used to confirm to the IRM server that the user has a license to read the document.

**Secure revisions with Information Rights Management technologies**

The integration of Microsoft Windows Rights Management Services (RMS) and Adobe LiveCycle Server extends the protection of confidential documents to the desktop. IRM technology enables permissions to change, print or forward a document to remain active even after the document has been downloaded. A document protected with IRM that is no longer in the Brainloop Secure Dataroom is encrypted and stored on the authorized user's computer and can only be opened by that person. The combination of Brainloop Secure Dataroom and IRM technology supports the Microsoft Office, XPS, and PDF formats. If the appropriate security category has been configured, IRM protection is activated automatically when a document is downloaded. Client-side Microsoft RMS functions are included in newer Microsoft Windows versions. No other client software is necessary. The server delivers the certificates and permissions needed for authentication directly to the client.

**SECURE OPERATION****No client software**

There is no need to install any plug-ins or OCX modules that could be used by attackers to compromise security. No objects in the browser cache with the appropriate browser settings, no unencrypted objects are stored in the browser cache on the local computer, eliminating the risk that they could be retrieved and read later.



### IP limits for administrators

Access to application management, dataroom center and dataroom administration functions can be limited to certain networks or IP areas.

### Application administration

Application administration tasks are dependent on permissions, enabling different types of administration to be set up (such as for monitoring and analysis, changes, configuration tasks, software upgrades etc.). This also allows the tasks to be divided between different people or groups. The system logs every change made by the application administrator. In addition, hardware fingerprinting is used to ensure that changes to the system configuration are detected immediately.

### Application monitoring

A monitoring component oversees the application and generates alerts about any changes to permissions, the file system, and security-critical database content, and about any tampering with files on the file system. The application administrators define their own preference regarding how they receive the alerts, such as by text message or email.

### Encapsulated user management

Applications administrators cannot change any critical user data such as email addresses or cell phone numbers. As a result, they cannot change an account to give themselves access to the user's documents. Users are informed by email of any changes to their profile made by an administrator.

### Data room center administration

The administration of a data room center consists of creating and configuring data rooms and provisioning user licenses. Other management functions are carried out within a data room in the data room administration section. The dataroom center administrator has no access to the documents in a data room.

### Data room administration

The management of a data room's configuration and content is usually the responsibility of the project or department manager. This person decides – independently of the application administrator – whom to invite to the data room and who has which permissions.

### Virus scanner integration

Customer- or operator-specific virus scanners can be integrated into the system. Any infected files are isolated and the application administrator notified by email.

### Protection of the key infrastructure

The data room keys are encrypted using a master key. This master key is generated during the system installation and is itself encrypted and stored. Once the master key has been created, it can be divided up into parts which can then be distributed to different people. To restore the master key after a total system breakdown, for example, at least one user per key part must be available. It is recommended to divide up the key into 2-3 parts and distribute these to 4-6 people.

### Moving data rooms

Special keys are also needed when data rooms are moved, and these are divided between the application administrator and the data room manager. Both keys are needed to restore the data room in a new system.

### Database administration

Passwords and similar elements are not stored as legible text in the database. Built-in data integrity checks ensure that any attempts at manipulation are detected quickly and the data room is locked immediately. The database administrator is not given a system login for the server machine. Access to the database from the network is also blocked.

## DATA PROTECTION

Various levels of backup are provided to ensure high data availability.

- › **System backup:** Executed regularly and after every software update. A system backup is only used for complete system recovery purposes. Individual files in a data room cannot be restored by the system backup.
- › **Database backup:** Runs continuously.
- › **Server's data area:** Should be run at regular intervals. Differential backup using backup software is also available.
- › **Data room backup:** To allow an individual data room to be reconstructed, the application provides the option of backing up data rooms at fixed intervals and keeping several versions of them. The backups are encrypted and



stored together with the data room key in the server's file system. The application administrator handles the parameterization tasks (maximum period since last backup; number of backups to be kept; backup times; backup schedule etc.).

### Integration in the existing IT infrastructure

The server can be seamlessly integrated into existing network infrastructures such as firewalls and intrusion detection systems as well as into system and application management infrastructures.

### COMMUNICATIONS CONFIGURATION

The firewall in front of the Brainloop system can be configured very restrictively because the system uses very few communications protocols. Minimum requirements include:

- › **HTTPS access:** Normal communications between the client and server use HTTPS. If required for security reasons, HTTP can be turned off.
- › **Email:** The system sets up its own external connection to send notifications to users.
- › **Text message:** The system sends text messages via a web service. The server therefore needs access to an external server via HTTPS. Terminal server access may also be necessary for software updates and maintenance work. This can be protected using IP restrictions or other common protection mechanisms. Software updates for the operating system and its components must be loaded via the Microsoft Update Service or via a solution within the data center.

### High-availability configuration

Very high availability can be provided by clustered database servers and distributed application servers with the appropriate support for system management and system monitoring. The disaster protection components can be distributed geographically.



## CONTACT

**Brainloop**, with offices in Boston and Munich, is the leading provider of Document Compliance Management solutions that enable customers to share confidential documents in a highly secure and traceable environment.

For more information please visit [www.brainloop.com](http://www.brainloop.com)

**Europe**  
**Brainloop AG**  
 Franziskanerstr. 14  
 81669 Munich · Germany  
 T: +49 (89) 444 699 0  
[info@brainloop.de](mailto:info@brainloop.de)  
[www.brainloop.de](http://www.brainloop.de)

**USA**  
**Brainloop Inc.**  
 One Broadway, 14th floor  
 Cambridge, MA 02142 · USA  
 T: +1 (800) 517 3171  
[info@brainloop.com](mailto:info@brainloop.com)  
[www.brainloop.com](http://www.brainloop.com)