SECURITY

MathDATA hosted products provide the security infrastructure necessary for customers to feel confident about placing sensitive information online for secure collaboration amongst employees, suppliers, customers and partners. Security and reliability are accomplished through careful planning at every level of the service: physical security, network monitoring, system architecture, hardware redundancy, data backup, application integrity, and the use of secure communication protocols.

Physical Security

MathDATA uses two facilities. One is located within a carrier-class data center operated by GNAX, and located in Atlanta, Georgia, USA. The other is InterNap within the Equinix data center in Chicago, Illinois. Both facilities use multiple control mechanisms to ensure the highest level of physical security. These include 24/7 security guards, biometric scanners, and full video surveillance. Environmental conditions are kept optimal through sophisticated power conditioning systems, redundant air conditioning units, UPS battery backup, diesel generators, and gas-based fire suppression systems. All servers are housed in locking cabinets within locked cages.

These facilities are state-of-the-art data centers that provide a highly secure physical infrastructure, including the latest in biometric authentication, video surveillance, and around-the-clock security officers. The center is engineered to eliminate any single point of failure, with multiple layers of redundancy in power systems, HVAC, and fire detection and suppression. All systems are monitored 24x7 through a Network Operations Center (NOC).

Specific security measures include multi stage key card access and then hand geometry readers to prevent card key theft. The data centers also have state of the art CCTV recorded 24x7 with certain cameras available to our customers via the Internet for their own monitoring for maximum security. All visitors to the datacenters must check in and out of the facility. The goal is to provide maximum redundancy in every facet of the datacenter environment to facilitate 100% uptime for our your entire hosting infrastructure

User Authentication

Each user must select a unique user name and password that is re-validated upon subsequent visits. At the server level, the passwords are stored in an undecryptable format. (SHA2) Password policies can be modified to ensure internal security policies are enforced. Dynamic htaccess files are located in each and every directory within a customer account. These htaccess files contain a single entry which is "deny all". Once a user is logged in, permissions are checked against the database. As the user enters a specific area, the system will rewrite the htaccess file with appropriate permissions for that specific user for as long as that user is accessing the data. Once the user browses to another area of the site, that htaccess file is rewritten to deny all. Basically, permissions exist only as long as required for a user to obtain the authorized data.

External users may only view and download data where you have granted access to specific files. External users may also upload data. However, once uploaded, the data is no longer accessible to them. This prevents any attempted modification of files and also prohibits users from sharing passwords to exchange files with each other.

Uploading data types which we deem to be a security risk is prohibited. This includes files such as html, php, bat, htaccess, exe, and others. Some of these file types are filtered at upload. Others are destroyed upon arrival.

Permissions within the MathDATA are file and user based. We do not use "group" permissions. Although you may add users to Teams, and you may also create folders to organize data, the actual permissions are user based. Folders that you create are "virtual" folders and do not really exist on the server. Therefore, attempting to access a file through its apparent location, such as http://somedomain.com/folder1/file1 serves no purpose as this location does not exist. If it did exist, the htaccess file would deny access anyway.

Lastly, users cannot "see" one another. When users login they are totally isolated from each other. Even if you add several users to a "Team" for group access to a given set of files, the existence of other team members within the application is hidden.

Access Control & Security
Users see only what is specifically granted to them. External users cannot see other users nor can they see files other than what they have specifically been granted. The User List and User Manager area provides a powerful and automated method to track and review users and permissions. Only Administrators may view user lists.

Further, all user activity is logged to a permanent secure file for review at any time. Comprehensive file and action tracking is available both on-line and as printable hardcopy reports. User Authentication is accomplished via IP verification and dynamic htaccess. No configuration or personalized information is stored in a location which is accessible over the internet.

User Activity & File Tracking Logging
Every user, inclusive of all user classes (regular users, Operators, and Admins), and every transaction is recorded to the History record. Typically, your MathDATA account will record, all logins, all uploads and downloads, file viewing, folder creation, file movement from folder to folder, user creation, IP addresses, and numerous other activities. Optionally, you can have notifications automatically sent to your Administrative staff upon each user login. Activity records are permanent and cannot be altered or removed. Not even by your administrative staff. If a MathDATA customer requires the History record be removed or emptied, there is a verification procedure in place that only the in house MathDATA security officers may perform.

Administrative Security Options
As a MathDATA customer you are provided an Options panel that includes variety of tools that allow you to set a security level that is specific to your account. Some of these include:

Enforcement of password Rules.
Enforcement of Customer defined Security Policies
Require Signatures on Electronic Non Disclosure Agreements

Security levels may be set to Weak, Medium, or Strong depending on your policies. MathDATA services include a Rich Test Editor where you may modify a generic preformatted Non Disclosure Agreement. You may require users to login and electronically sign the NDA or any other document such as a Terms of Service Agreement. All signatures on these documents are recorded to the users Activity record.

Secure Communications

Full 128-bit SSL (Secure Socket Layer) encryption is employed during all communications with your MathDATA account. SSL protects passwords and data during transmission across the public Internet by never transmitting data in “clear” text. Alone or in combination with SSL, IP-based restrictions can also be applied to ensure only identified computers or networks can access a specific MathDATA® implementation.

MathDATA uses two types of SSL certificates for our services:

1. Code Signing Credentials (Java Uploader)

   GeoTrust Code Signing Credentials for MathDATA provide you with assurance we have enabled secure delivery to PC's over the Internet or to mobile devices. Our customers can be sure of the identity of the person who developed the software and that it has not been tampered with or changed. Further, our uploader applet is encrypted and compiled at the source level. It is not human readable.
2. SSL Certificate (Site)

   GeoTrust SSL certificates allow us to encrypt the code for secure online transactions. All of our SSL certificates enable up to 256-bit encryption although we currently use 128bit.