

ThinkTank Security Statement

June 2008

Purpose

The purpose of this security statement is to describe the security precautions taken by GroupSystems to safeguard data of customers using the company's hosted ThinkTank environment.

Hosting Partner

GroupSystems has contracted with a hosting partner for the operations of all of GroupSystems's ThinkTank servers. Our partner, [Rackspace](#) operates secure data centers in the United States and the United Kingdom.

The Network Operations Center (NOC) is staffed 24x7 and maintains high levels of security. Since the ThinkTank servers are managed and secured by Rackspace, GroupSystems does not have physical access to any of ThinkTank servers. The Rackspace facility employs the latest in fire detection and suppression equipment. Power can be provided by backup batteries or diesel-based generators. Communications are provided by no fewer than three independent telecom providers.

Security Hardware and Software

GroupSystems recognizes that data security is of the utmost importance. Therefore, GroupSystems offers varying degrees of security depending upon customer needs. GroupSystems provides the following:

- Secure Socket Layer (SSL) Security over HTTPS

Customers may opt to connect to ThinkTank using SSL. This ensures that all transmissions between the client and server are encrypted using 128-bit encryption. Security certificates are provided by Thawte.

- IP Spoofing

The ThinkTank deployment environment employs algorithms to prevent users from IP spoofing.

- Firewall Security

All ThinkTank servers are located behind a reliable firewall appliance. The firewall only allows HTTP (port 80), HTTPS (port 443) traffic and remote desktop ports (remote

administration). Rackspace monitors the firewall 24x7 for unauthorized intrusions. Furthermore, the firewall software is constantly upgraded when security patches become available.

Should customers desire additional levels of protection, both hardware- and software-based VPNs are available at an additional cost.

Disaster Recovery

All ThinkTank servers are backed up on a nightly basis. Full system backups are taken once per week and incremental backups on a daily basis. Nightly backup routines are monitored both by GroupSystems and Rackspace. Backup media is stored in a Rackspace tape vault.

Security Questionnaire

1. What kind of vulnerability scanning is performed on the infrastructure, including how often?

Port scanning and vulnerability scanning are performed quarterly.

2. What is the process to resolve any vulnerability discovered during scanning?

Issues are reviewed by the security team and addressed.

3. What is the process to assess patches/hot fixes, validate/test a patch, and apply a patch?

GroupSystems program upgrades are provided on a regular basis. We follow a defined upgrade process to uninstall and re-install all patches and program upgrades.

Rackspace has a very stringent patch/hot fix policy for operating system patches. Upon the release of the patch the patch is analyzed to determine what problem the patch will remedy as well as the methods for doing so. Once that is understood the patch is applied to several patch testing servers and then re-analyzed. If the patch has no ill effects it is scheduled (approximately 3 days later) for release across the shared infrastructure. During the time between deployment on the patch test servers and the shared infrastructure searches are performed for other users experience with the patch to assure against other issues that may be experienced with patch deployment. The patch is then applied across shared servers. Once the effects have been analyzed in the shared infrastructure, a patch is scheduled for deployment in groups across dedicated server infrastructure at a time/day that has been pre negotiated with their end customer (GroupSystems, in this case).

4. What is the process to monitor compliance of their IT security processes?

GroupSystems has designated a very small number of individuals to access the hosting server. These people also developed our security processes.

Our hosting provider, Rackspace, has a security team that consists of members from Network, Systems and Facilities personnel. The security team meets monthly to discuss new security threats, the validity and action items for non-emergency type issues. Emergency issues are handled by each individual department with real time input from the other groups via conference call and or electronic communication.

5. What is the process to communicate to our customers the status of the IT security compliance?

Important issues are regularly posted on the GroupSystems support website. Any issues directly affecting Client will be communicated with a direct phone call.

6. When and how often can our customers perform periodic reviews to ensure compliance?

The customer may contact GroupSystems and arrange for compliance review.

7. What level of background checking is completed for both employees and contractors?

GroupSystems performs background checks on all employees.

Rackspace does full background checks on all employees. This is not dependent on job role or responsibilities.

8. What are the physical security requirements? This includes things like controlling and monitoring access (e.g. video), what kind of locking is used (e.g. card access system), do they have guards, and how do they manage the process for employee turnover. How do they log access to the site(s)?

Each Rackspace primary facility is manned 24/7 by Rackspace staff. Each facility also has camera deployments at all access points as well as in the interior of the facility. Customers as well as employees who have access to the facility are issued a Rackspace badge that has a photo of the individual on the badge. Magnetic readers are at each entrance both exterior and interior. Each time the magnetic card is passed by the reader, the picture is displayed in the Network Operations Center and the individual can be identified via the camera system and picture on file. In addition, each card has an individual 4 digit pin code that must be entered to gain access to raised floor areas. Logs are created and backed up for each card swipe at each reader. Video is stored for 30 days on disk and then backed up on to tape for 90 days.

9. What is the process to restrict access to network hardware and telecommunication/wiring closets?

Only authorized Rackspace personnel are granted access to wiring cabinets and or telecommunications rooms. Each room has additional security parameters and video surveillance.

10. What is the backup strategy and process?

Full backups are performed weekly and incremental back up are performed daily during off peak hours. Two weeks of data is held on the tape array before data is erased and media reused.

11. How is obsolete data erased before backup media is recycled or disposed?

The media is erased before it is recycled.

12. What is the change management process (this includes both the application and the infrastructure)?

New releases of GroupSystems are packaged roughly every 2 months. These upgrades are placed on the hosting server.

13. What is the firewall strategy?

The firewall used is from a respected provider of network equipment and has hardware and software support as well as 24x7 monitoring. The operating system of the firewall is patched as needed after the patch has been carefully analyzed.

14. What are the strategies to mitigate a Denial of Service attack?

Null route traffic or add ACL's to transit providers border routers based on size and type of attack.

15. How are the Domain Name Servers (DNS) protected?

DNS resolvers sit in front of protected DNS clusters. Other information will be held confidential for security purposes.

16. What is the password management process for ThinkTank?

Passwords are case sensitive. No one can view a password as entered by a user. Workspace administrators can reset a password.

17. What authentication mechanisms exist?

Login and Password are required for session leaders. Participants must know the session-specific passkey assigned by the session leader.

18. What is the process to manage admin/super user access to the system(s) (this includes not only direct staff but also external service personnel)?

Customers are given workspace level access to administer their own sessions. GroupSystems provides System Administration capabilities.

19. What is the process to manage accounts on the system(s)? This includes account creation, periodic re-verification and disabling of accounts.

GroupSystems creates a separate workspace for each customer after signing a hosting agreement. An administrator is assigned to a named individual provided by the customer. That person sends leader information to GroupSystems. GroupSystems creates the unique session leader IDs as part of our licensing agreement.

20. What processes are in place to control remote access?

All system administration can be done through remote access. Server maintenance requires VPN access from the GroupSystems network.

21. What are the Disaster Prevention Recovery Procedures?

Our hosting provider, Rackspace, spares all hardware and keeps hot live boxes that are installed and networked and can be immediately used for restoration from tape backups in event of a full server failure. Servers all have local RAID configuration and additional parts are spared on site.

22. What are the Business Continuity Plans?

In the event of a disaster, the hardware, software and data would be restored to the date of the last daily backup. Hot site recovery is available for an additional fee.

23. How do they ensure the availability of the application (which would include the infrastructure)?

Network is fully redundant and engineered for failure. All layers (Core, Boarder, Aggregation, and Distribution) are redundant. Five fiber providers and three transit providers connect the facility. Facility has maintained 100% power availability for three years of operation (never lost customer power since Rackspace owned facility). Back up PDU's, UPS's, battery and generator are all onsite, tested, and maintained quarterly. The generator is exercised weekly.

24. What is the security incident and crisis management process?

Mitigate, Manage, Reanalyze and Deploy. The process is led by the security team of Rackspace.

25. What is the process to notify clients if a security incident or crisis occurs that affects a client's information or applications?

GroupSystems will make an immediate phone call to the designated point of contact.

26. What is the virus scanning strategy and process? This includes what tools are used and how virus signature files are kept up to date.

We currently do not use anti-malware software as the restricted users of the server may not browse the web and may not read e-mail. E-mail sent from the server contains only text information and no attachments. Should the functionality of the ThinkTank application change, this policy will be re-evaluated.

27. Describe the security focused resources/organization.

GroupSystems developers have typical awareness of IT security issues. We do not have any dedicated security resources. Our hosting provider, Rackspace has a strong, dedicated security team with extensive experience.

28. What is GroupSystems's privacy policy?

No data is sold or shared with any other entity.

29. What is the security monitoring strategy and processes? This includes clients, servers, and networks.

GroupSystems has designated a very small number of individuals to access the hosting server. These people also developed our security processes.

Our hosting provider, Rackspace, has a security team that consists of members from Network, Systems and Facilities personnel. The security team meets monthly to discuss new security threats, the validity and action items for non-emergency type issues. Emergency issues are handled by each individual department with real time input from the other groups via conference call and or electronic communication.

30. How is a customer's data kept separate from other company's data (this include people without a business need seeing the client information)?

Each account is given a separate workspace. A workspace is a logical separation of data. Only users with rights to a workspace may view users or sessions created for that workspace. Within a workspace, a user may not open a session unless they have been invited to attend by the leader. The data is stored in a database that is behind a firewall.

31. What is the IT security escalation process?

Important issues are regularly posted on the GroupSystems support website. Any issues directly affecting Client will be communicated with a direct phone call.

32. What is the web security strategy?

SSL is optionally used to encrypt all data between the client and the server.

33. What other applications run on the system(s)?

ThinkTank is the only application that runs on the system.

34. Are all applications running on the system(s) enclosed to prevent access to applications for which the user is not authorized?

Yes

35. What are the operating system level trust relationships with other systems?

Our application operates on a standalone server.

36. What is the process to revoke privileges whenever an employee or contractor leaves the company?

Privileges are revoked immediately for all employees and contractors who have left the company.

37. How long are the system log records kept?

The system logs are kept for one year.

38. What is the notification process for unauthorized access to customer data?

We will place an immediate phone call to the authorized point of contact if such an event is detected, followed by an email.

39. What is the intrusion detection strategy and process?

Our hosting provider, Rackspace, has Network Intrusion Detection systems at each of its transit points (3) and actively monitors and reports on these systems. Alarms are tied into their main monitoring systems as well as alarms set specifically for GroupSystems based on traffic patterns. If a traffic increase or traffic type alarm or customer request is initiated, traffic is examined for legitimacy and then proper measures are taken to null route this traffic.

40. Is any session data stores or cached on the client computer?



In brief, no data is stored on the client side. The only part of the ThinkTank application that is cached is the client. Here is more detail:

Web Page Caching

Each time you access a web page, it is stored on your machine in a temporary cache. That way, if you go back to the same web page, they are displayed very quickly because all of the images are stored locally; they don't have to be downloaded again. If you want to see what is cached on your machine, the files are stored in the directory C:\Documents and Settings\\Local Settings\Temporary Internet Files. A user may turn off caching in which case no files will be cached. This is NOT necessary for ThinkTank.

ThinkTank Caching

The only part of ThinkTank stored in the temporary cache is the application itself and the web pages used to access ThinkTank. None of this contains any data from previous ThinkTank sessions. In order to get to the data again, users are required to login and access the session.

Being Even More Secure

If your client wants to be even more secure, they can do the following:

1. Change the passkey after running the session. This will prevent users from accessing the data of the session.
2. They can either "Save the Session to Disk" or generate a report and then delete the session. This is extreme, but it will delete all of the data on the server.