MangoApps System & Information Security Policy

January 2013

Description of the MangoApps System & Information Security Policy

MangoApps customer data and information security is our highest priority. Our own success rides on the confidentiality, integrity, and availability of customers' information. For that very reason, MangoApps is designed with an industry- leading policy for system and information security that addresses the needs of enterprise. The policy is supported by key security measures including:

- Security in the Data Center
- Application-Level Security Measures
- Logical Separation between Networks
- Data Backup and Disaster Recovery
- Thorough Vulnerability Testing
- Firewall and IP Range Protection
- Increased Password Strength Policies
- Separated Browser Session Settings

MangoApps Product Deployment Options Q&A

The following questions regarding the differences between MangoApps deployment options address the security considerations for each deployment type. Businesses can then better decide between Shared Cloud SaaS, Private Cloud SaaS, and On-Premises deployments.

Shared Cloud (SaaS)

What is a Shared Cloud?

Sometimes referred to as multitenant software architecture, MangoApps in a share cloud runs a single instance of the core software and is able to serve multiple client organizations' domains. Each organization's data and configuration runs in its own logically partitioned instance of MangoApps.

How is My Data Protected in a Shared Cloud?

MangoApps Shared Cloud servers are hosted in the Amazon Web Services (AWS) infrastructure. AWS services are certified and have third-party attestations for:

- **ISO 27001**
- HIPAA Compliance Capability
- FISMA, DIACAP, and FedRAMP
- SOC 1/SSAE 16/ISAE 3402
- SOC 2
- PCI DSS Level 1
- International Traffic In Arms Compliance
- FIPS 140-2
- CSA Questionnaire
- MPAA Best Practices

Amazon Web Services (AWS) deliver a highly scalable cloud computing platform with high availability, reliability, and flexibility. Read more about AWS security and compliance at: http://aws.amazon.com/security/

MangoApps performs the following regular security audits on its systems:

- Full daily backups
- Ensure that all systems that store or process your data are properly configured and adequately hardened
- All sensitive user-data (like password, credit card etc.) is encrypted
- Protect your data during transmission across the network by using SSL.
- Track and monitor access to your data
- Restrict physical access to your data
- Security policies, procedures, guidelines and standards that address information security for all employees, contractors, and third parties

In addition to system level security, there are multiple options for application level security within MangoApps that domain administrators can take to enhance the security of their domain.

- **IP Range Restrictions:** Limiting the IP Range from which users can connect to the MangoApps domain is configurable by domain administrators. Multiple IP Ranges can be set to handle distributed organization's needs.

- **Password Strength Requirement:** When user account passwords are set, they must adhere to the enhanced password strength settings enforced by the MangoApps domain. Administrators can enforce password strength in their MangoApps domain based on password length, alpha-numeric character and special character settings.
- **Enhanced Security Features for Mobile Devices:** Suspend a lost or stolen device, and even wipe it out remotely, without disabling the entire user account. Make your connection from mobile secure over HTTPS just like web and desktop clients. Secure your mobile devices with a PIN in addition to a password. This will ensure that the information on your device is kept secure if lost or stolen.
- **User Management:** MangoApps allows domain members and administrators to invite users to the domain by default. Administrators can enhance security by changing the default setting such that only administrators can invite members to the MangoApps domain.
- **Authenticated User Accounts:** Users must authenticate through the configured authentication server to log in to MangoApps. Authentication is handled by default in MangoApps through user emails and assigned passwords. To enhance security, MangoApps allows administrators to require authentication through an existing Active Directory or LDAP authentication server.
- **Device and Client-type Restrictions:** MangoApps allows domain administrators to restrict specific mobile devices from connecting to the domain. Additionally, the Desktop Client can be prohibited from connecting to a MangoApps domain.

Private Cloud (SaaS)

What is a Private Cloud?

In a private cloud deployment a single customer's domain is hosted in its own virtual machine provided by our virtualization environment. This ensures that your data and computing resources are separate from other MangoApps customers.

What Advantages and Enhanced Security does a Private Cloud Deployment provide?

Private cloud deployments offer all the desired advantages and security of the public cloud including AWS hosted security while extending functionality and enhancing security for your company. Since AWS servers are available worldwide, your data can be deployed in a Private Cloud environment in your preferred region.

Advantages of private cloud over public cloud deployment include protection from latency interference of other domains hosted in the same partition. Security is enhanced by the private partition of the MangoApps core backend. MangoApps additional features for private cloud deployments include:

- Regional deployment options
- Ability to require VPN-only domain access.
- Support for Vanity Domain URLs.
- Support for integration with custom systems.
- Ability to apply CNAME forwarding.
- SSL Authentication certificate integration.
- Ability to encrypt data at rest.
- Control over when a new version of the software is deployed.

On-Premise (Self-Hosted)

What is On-Premise?

On-Premise deployments give you full control over the hardware and software required to run MangoApps. Everything is behind your corporate firewall and you have complete access to MangoApps underlying processes and data stores. All applicable shared cloud and private cloud security benefits carry over to On-Premise

What Advantages and Enhanced Security does an On-Premise Deployment provide?

With full control over the hardware, network, and software environment running MangoApps, on-premise have the greatest performance potential for the largest social business networks.

- Apply your proprietary security requirements.
- Full control of software and hardware architecture.
- Optionally close off external access to MangoApps systems.
- Schedule upgrades and maintenance on-demand to minimize interruption.
- Direct, low-level administrative access to MangoApps.