Information Security

emSigner

TABLE OF CONTENTS

A GLIMPSE OF EMSIGNER.COM

emSigner.com is a SaaS based document signing and transaction management platform for Individuals and Businesses. emSigner.com is run by eMudhra Ltd, a licensed Certifying Authority in India and Mauritius issuing Digital Signatures, National ID (AADHAAR) based eSign, SSL certificates and Authentication Solutions to Government, Banks, Financial Institutions etc.

eMudhra is an ISO 27001, 9001 and 20001 certified organization and hosts a Tier III state of the art Data Center in Bangalore, India which hosts emSigner.com apart from a whole host of critical infrastructure for eMudhra's operations.

Our cloud offering emSigner.com is supported through a multi-layer security framework comprising of physical, application, network level security backed by failovers, disaster recovery, uninterrupted power, data backups, 24x7 physical support to provide a high performance solution to our customers.

This is achieved through

- ✓ 24x7x365 in house support manned by trusted personnel
- ✓ Performance, surveillance monitoring 24x7x365
- ✓ Tier III Data Center with physical, network partitioning
- ✓ Restricted Access – two factor and two person authentication to key systems
- ✓ Clear Screen and Clear Desk Policy
- ✓ CCTV Cameras
- ✓ Audit Logs
- ✓ Data Backup
- ✓ Multi-tenant data architecture
- ✓ Security Auditing through regular Vulnerability Assessment and Penetration Testing
- ✓ CMMI Level 3 accreditation software development practices (in progress)

INFORMATION MANAGEMENT

Information Security Program

eMudhra's Information Security Programme is broken down into specific stages as follows:

- ✓ Adoption of a security policy
- ✓ Security risk analysis
- ✓ Development and implementation of an information classification system
- ✓ Development and implementation of the security standards manual
- ✓ Implementation of the management security self-assessment process
- ✓ On-going security programme maintenance and enforcement
- ✓ Training

Information Management

eMudhra has put in place an Information Management policy which is based on sensitivity of information. Access Control are determined by System Administrator only on need to know and need to do basis with periodic reviews of access rights conducted to ensure compliance with the policy.

SECURITY

Applications Security

eMudhra's development team has been trained in secure coding practices and use numerous framework level protections to prevent web application vulnerabilities. These include

- ✓ Logging of security events such as User Logins, Configuration Changes
- ✓ Complete Document Audit Logs
- ✓ Encrypted Password Storage using Symmetric Keys
- ✓ Periodic Vulnerability and Penetration Testing
- ✓ Web Server Surveillance and Event Monitoring

Data Security

eMudhra takes the security and sensitivity of its customers data very seriously. eMudhra production support team does not access data on production servers, unless requires for troubleshooting or support. The access control is also restricted to only users authorized for production support. The development team at no point has access to production data. Environments are clearly delineated with access rights provided based on role and responsibility. eMudhra follows a stringent process for development, changes and release management.

The data of each customer is isolated in application level, and is protected with application architecture. For certain clients, emSigner.com follows a multi-tenant architecture that isolates database instances completely. emSigner.com maintains two kinds of backup logs – application logs and data backup.

The data backup policy of eMudhra includes daily and weekly data backups. At this moment, eMudhra does not have shorter backup span other than above. However, work is in progress towards more frequent cycles.

Backups are stored in isolated instances, as well as secure offsite storage (fire retardant). The backups are tested with restoration testing programs under eMudhra security policies.

At an event where customer opts out of emSigner.com or migrates to 'on premise' platform, the online data is purged against a written request from the customer.emSigner.com uses a PCI DSS certified payment gateway and does not store payment data.

Physical and Operational Security

eMudhra employs a strong physical and operational security to regulate and manage controls at the data processing facilities and environment of eMudhra. This is done to avoid any service outage caused by environmental hazards or by physical unauthorized access.

eMudhra has controls in place to prevent loss, damage or compromise of assets and interruption to IT Services. This includes identification and access to computing facilities based on staff role and responsibility and thorough vetting of Data Center staff to add them to the Trusted Personnel list.

Data Centre Operations

eMudhra's data centre is a Tier III data centre with 7 layers with restricted access control, monitored by CCTV cameras, 24x7x365 physical security and data centre support staff with uninterrupted power supply and multiple internet and connectivity failover options. The primary site is well supported by a Disaster Recovery site with the above connectivity and security provisions.

Network Communication and Connectivity Security

It is extremely important to maintain confidentiality, integrity, and availability of information transmitted over communication channels. eMudhra ensures this through a thorough management of its network communication links including Access Lists, IP Address Schema, Link Backup, Packet Loss Analysis, Protection of network communication devices such as Firewalls, Modems and Routers.