REALBOOKS

Adansa Solutions Private Limited
98/7A, Harish Mukherjee Road,
Kolkata - 700 025
West Bengal, India

RealBooks IT Security Policy

RealBooks is hosted on AWS (Amazon Web Services), it's crucial to have a well-defined IT security policy to ensure the security, compliance, and protection of our infrastructure, applications, and data. Here's a high-level outline of what our IT security policy might entail when hosting services on AWS:

Access Control and Identity Management:

- We have defined user roles and responsibilities.
- We have implemented strong authentication mechanisms, such as multi-factor authentication (MFA).
- We have used AWS Identity and Access Management (IAM) to control access to AWS resources.
- We enforceed the principle of least privilege, granting only the necessary permissions.
- All data is hosted on Amazon AWS , Mumbai region in India. Accordingly, no company employee has access to physical servers.
- All access to databases is via SSH connection to EC2 instances.
- Only authorized IP Addresses can access these EC2 instances, and these IP addresses are monitored and updated on a daily basis.
- The SSH key files are rotated once every 6 months.
- Employees have been given individual access keys based on need basis.
- Upon termination of employees - access from such keys are deleted from the servers.
- Audit Policy
    1. All keys are rotated once every 6 months.
- Users and Groups & File Permissions
    1. RealBooks is designed on the micro services architecture.
    2. Only applications are deployed by DevOps team.
    3. Hence we don’t have user wise access and permissions at the OS level.
    4. **Developers don’t have access to Production OS.**

Adansa Solutions Private Limited
98/7A, Harish Mukherjee Road,
Kolkata - 700 025
West Bengal, India

Data Protection and Encryption:

- Data Segregation

  1. RealBooks was built for the cloud from ground up.
  2. RealBooks is a SaaS system with multi-tenancy architecture.
  3. All companies are assigned a company id and all records in every table are required to have this company id that segregates and identifies data of companies within a single database.

- Data Access

  1. All data is hosted on Amazon AWS , Mumbai region in India. Accordingly, no company employee has access to physical servers.
  2. All access to databases is via SSH connection to EC2 instances.
  3. Production Data can be accessed by two people only for monitoring and maintaining the databases in write access mode.
  4. Only authorized IP Addresses can access these EC2 instances, and these IP addresses are monitored and updated on a daily basis.

- Data Back up

  1. All Data is backed up at least in three ways
  2. Realtime replication for all databases is carried out on a master – slave configuration.
  3. End of day EC2 Snapshot of instances with databases are taken.

- RealBooks Data Governance

  End of day dumps of Database are stored in AWS s3, copied in at least two separate regions - India and Frankfurt.

- Data Security from Application to Server

1. Encryption of all data is carried out by SSL Certificates issued by Trusted Partner – GoDaddy.
2. Algorithm used for SSL Certificate is SHA-256 with RSA

- Application Password
  1. Passwords are required to be changed every 90 days.
  2. Passwords are required to have a minimum length of eight (8) characters.
  3. Required to contain at least 1 capital letter, 1 small letter, 1 numeric character and 1 special character.
  4. Passwords cannot be identical to previous two passwords.
  5. Upon 5 incorrect attempts, captcha is required so that bots dont keep attempting to crack the password

Network Security:

- We have used Amazon Virtual Private Cloud (VPC) to isolate and secure network resources.
- We have configured network security groups and network access control lists (NACLs) to control inbound and outbound traffic.
- We have a Web Application Firewall (WAF) for protecting web applications from common web exploits.

Logging and Monitoring:

- We have used Amazon CloudWatch for monitoring and alerting on resource utilization, performance, and security events.
- Consider using AWS Config to assess resource configurations for compliance.

Patch Management:

- We keep our AWS resources up to date with the latest security patches.

Compliance and Auditing:

- We have used AWS Artifact to access AWS compliance reports and third-party audit reports.

User Training and Awareness:

- We educate employees about AWS security best practices and policies.
- We conduct regular training sessions to keep the workforce informed about emerging threats.

AWS Well-Architected Framework:

- We considered aligning with the AWS Well-Architected Framework, which provides best practices across multiple domains, including security.

Continuous Improvement:

- Regularly review and update your security policies based on changes in the threat landscape and technology.