Application Security Policy & Procedures

This Security Procedures document is aimed to define the security requirements for the proper and secure use of the Respond.com web application. Its goal is to protect the Organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

This document is reviewed annually and new guidelines added accordingly to handle new vulnerability, threats and risk. Following persons are responsible to manage application security.

Roles	Responsibilities
Chief Technology Officer	• Accountable for all aspects of the Application's information security.
AWS/IT Administrator	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Users	• Meet Security Policies. • Report any attempted security breaches.

1. General

- IT assets must only be used in connection with the business activities they are assigned and / or authorized.
- Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
- All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.
- Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.
- The Local IT Technical Teams are the sole responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
- Special care must be taken for protecting laptops and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields and falls.
- Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen.
- All laptops/desktop to be formatted before handling over to new user.

- All computers and devices with access to the Organization network must have an antivirus client installed, with real-time protection.
- All application servers on AWS must have approved antivirus software.
- All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.

2. Data Classification

Application data to be classified as per their use and sensitivity.

a. Information owners must ensure the security of their information and the systems that support it.
b. Information in the Organization is classified according to its security impact. The current categories are: confidential, sensitive, shareable, public and private.
    i. Information defined as **confidential** has the highest level of security. Only a limited number of persons must have access to it i.e. Performance Dashboard.
    ii. Information defined as **sensitive** must be handled by a greater number of persons to perform their daily jobs duties, but should not be shared outside of the scope needed for the performing of the related function i.e. Advisor Information like Credit card.
    iii. Information defined as **shareable** can be shared outside of the limits of the Organization, for those clients, organizations etc. who acquire or should get access to it i.e. Investor Information. This information not be shared with third party for marketing purpose. Investor should have the option to unsubscribe the Service at any point of time.
    iv. Information defined as **public** can be shared as public records, e.g. content published in the Web Site.
c. Information deemed as private belongs to individuals who are responsible for the maintenance and backup i.e. Buyer/Advisor Portal.
d. All credit card and password related information to be encrypted format.
e. All customer's sensitive information like Credit Card to be deleted after 6 month of account deactivation.
f. Information sharing to be through following mechanism only
    i. Authorized company Email/SMS account
    ii. HTTP Post on secured channel
    iii. Via S3 bucket or file upload via secured channel

3. User Access Control & Password policy:

All web application should be able to handle following kind of users.

- Investor/Buyer – Access through lead submission process and grant access to Buyer portal section.
- Advisor – Granted access through Advisor Registration process. Advisor get their user-id and password to access to Advisor Portal.
- Employees – Role based access given to user to access the Admin section to perform day to day operations i.e. Lead review and its processing as well as Advisor coordination. All employees are made aware about application security policies.
- IT Admin – Role based access to manage the infrastructure

Procedure:

1. A central User Management system to be used to create application User and grant/revoke access.
2. All business information should be protected with a password-based access control system and users to be assigned a strong password.
3. Password must be alphanumeric with minimum 8 characters long.
4. All employee and IT staff password should be expired after 90 days. The same password may not be used again for at least one year.
5. Account lockout mechanism to be in place for all account after 5 password retries?
6. Sharing of passwords is forbidden. They should not be revealed or exposed to public sight. Whenever a password is deemed compromised, it must be changed immediately.
7. Monthly audit of Employee and IT admin access to remove access for those people who no longer need it.
8. All system-level passwords (e.g., root, application administration accounts, etc.) must be changed on at least a quarterly basis.
9. All user-level passwords must be changed at least every six months. The recommended change interval is every four months.
10. Passwords must not be inserted into email messages or other forms of electronic communication.
11. User's access should be based on their roles and responsibilities.
12. Application should maintain an audit log for all business-critical changes performed by Users.
13. All access control to be reviewed half yearly to minimize security breach.
14. All IT Admins to be assigned an individual IAM account with minimal access permission to perform their duties.
15. Any development team's user to be granted permission after review and access through security group with IP whitelist for specified period. This exception to be recorded in incident log.
16. In order to prevent spreading viruses to the Internet, Users shall scan for viruses and other malicious code when
    - Any diskette or other storage medium is transferred from an Internet connected workstation
    - Upon downloading files from the Internet, particularly executable programs and other files at risk such as documents containing macros, and applications which may be downloaded and executed automatically such as JAVA applets
    - Before uploading any files to the Internet
    - Upon receiving or sending Internet e-mail attachments

4. Infrastructure Security & Audits

All applications are hosted in AWS infrastructure and following points to be checked monthly/quarterly.

- Network to be divided in public and private subnets so that sensitive data to be kept inside the private subnets.
- Network to be protected with suitable firewall policy.
- All infrastructure i.e. Servers, Database etc. should have suitable security group to control access.

- Services and applications that will not be used on EC2 instances must be disabled where practical.
- The most recent security patches must be installed on the EC2 and RDS instances as soon as practical, the only exception being when immediate application would interfere with business requirements.
- All access to EC2 & RDS instances through secured channel (e.g., encrypted network connections using SSH or IPSec).
- AWS System Manager to be used to identify all infrastructure issues and provide suitable security patch as and when required to avoid vulnerability.
- Periodically inspect/scan the all servers through AWS inspector for vulnerability.
- All applications to be protected behind AWS WAF to protect from DDos attack, bad crawling, SQL injection etc.
- AWS monitoring & security tools like Guard duty, Cloudwatch, Cloudtrail etc to monitor all suspicious activity.
- Access to Network and associated infrastructure should be limited to IT admins.
- Application and associated database can only be accessed by Internal users via secured login through a private network.
- To asses vulnerability check, A 3rd part application like SecurityMetrics.com to be used and suitable reports to be analyzed.
- All sensitive data like user's password, database password, credit card details etc to be in encrypted form at rest including backups
- All of data encrypted in transit upon transmission from applications via HTTPS protocol.

5. **Change management**
   - All applications code should be kept on standard version control i.e. Git
   - Git access to be limited to developers with suitable role and password.
   - All access to Git account to be through secured encrypted channel.
   - All application release should be tested on multiple environments like development, staging and production.

6. **Incident response**
   All kind of security breach incidents should be recorded, reviewed and suitable fix to be applied to protect the integrity of applications and IT infrastructure. Security-related events include, but are not limited to:
   - Port-scan attacks
   - Evidence of unauthorized access to privileged accounts
   - Anomalous occurrences that are not related to specific applications on the host.
   - Vulnerability attack like DdoS, SQL Injection etc.

7. **Application Reliability, Business Continuity and Disaster Recovery**
   As all applications infrastructure is running on AWS North Virginia region data center, IT admin should take suitable backups of applications and database to maintain business continuity with following objectives
   - Systems Recovery Time Objectives (RTO) – Within 120 minutes

- System Recovery Point Objectives (RPO) – 120 minutes

Backups:

- All EC2 AMI/EBS volume to snapshot to be taken daily with one week of retention time.
- All blog RDS DB snapshot to be taken daily with one week of retention time.
- All primary RDS database snapshot to be taken twice daily with one week of retention time.
- Quarterly test the recovery of this data and restoration of system.

Recovery:

Pilot light DR plan on AWS to be configured and tested periodically.

Appendix – A (Security Audit)

Security testing allows you to discover vulnerabilities. This is especially critical for software that stores or handles sensitive information. For audit, we will be following approach.

- **Research**: We start by researching the software system, potential attack vectors, and potential attackers.
- **Planning**: After conducting research, we build a custom vulnerability assessment plan.
- **Testing**: On average, security testing itself takes from 20 to 80 hours depending on the size and complexity of the system.
- **Results**: Receive a Security Assessment Report with detailed descriptions of discovered vulnerabilities and recommendations on potential solutions and prioritization of fixes.

Methodology and Tools

Category	Use Cases	AWS tool	Frequency
Infrastructure Protection	Filer malicious web traffic, bad crawling.	AWS WAF	Monthly
Detection	- Unified security and compliance. - Threat detection. - Server vulnerability check. - Track user activity and API usage. - Record and evaluate configurations of your AWS resources.	- Security Hub - Guard duty - Inspector - Cloud trail - AWS config	- Security hub (Quarterly) - Others (Monthly)
Data Protection	- SSL/TLS certificates - Data encryption	- Certificate Manager - AWS KMS	

Reports:

- Security and compliance reports with recommendations i.e. Security Hub
- Server vulnerability report i.e. AWS inspector