awarathon

Security Overview Paper

At Awarathon, we realize the importance of protecting the information which you have shared with us and we are absolutely committed to making sure that we are able to meet your every security need and concern. We as an organization adhere to the highest level of data protection and data security. Our efforts to protect integrity and confidentiality of your data not only ensures compliance with the laws and directives applicable to us, for the time being in force, but also form the basis of an advanced and progressive information security program designed to protect all information provided to us.

This document's primary objective is to protect you from unauthorized access and to protect it from accidental loss of information. This document aims to outlay various security measures / protocols we as an organization take to safeguard your information and data.

Outline:

1. Administrative Controls
2. Authority and access control policy
3. User Permission and Roles
4. Infrastructure Security
5. Application Security
6. Privacy and Confidentiality
7. Data support and operations policy
8. Responsibilities, rights, and duties of personnel

1. Administrative Controls

We realize that security is not only a technology issue but a personnel management issue as well. In that background, we have put in place robust administrative controls to ensure a more comprehensive approach to protection of customer data.

This policy applies throughout the organization as part of the corporate governance framework. It applies regardless of whether or not employees use the computer systems and networks, since employees are expected to protect all forms of information asset including computer data, written materials/paperwork and intangible forms of knowledge and experience. This policy also applies to third-party employees working for the organization whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

As an organization we share best IT security policies with your staff, conduct training sessions to inform our employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification. We also place a special emphasis on the dangers of social engineering attacks (such as phishing emails) by making employees responsible for noticing, preventing and reporting such attacks.

2. Access control policy

Access to information must be specifically authorized in accordance with Awarathon's Access Control policy. Access to information will be controlled on the basis of business and security requirements, and access control rules defined for each information system. All Awarathon users must be allowed to access only those critical business information assets and processes, which are required for performing their job duties. Access for our clients, temporary employees, or vendor personnel to Awarathon's critical business information assets will be provided only on the basis of a contractual agreement.

Username and initial passwords may only be provisioned by your company's administrators. Usernames and passwords are encrypted and authenticated by the system prior to logging in. Account passwords are hashed. Our own employees cannot view them. If you lose your password, it can't be retried, it must be reset. Only those users with a valid user name and password combination are granted access. Once a user has been authenticated he/she is granted functional authority based on the permission levels set by Awarathon administrator.

3. User Permissions and Role

Awarathon's implementation of security does not end once a user has been authenticated by the system. Your Awarathon administrator can also designate roles and permission at the user and folder levels. At Awarathon we follow a hierarchy pattern access to the system as mentioned below, which is done to ensure data security and prevent eavesdropping.

a. **Super Admin**: The Super Admin user is the person who looks after all the user data management. A super admin user has the ability to:
    i. Manage the access and level of responsibility of all users across our systems
    ii. Assign roles to other users to that of a manager or to that of a representative.
    iii. Access all the Super Admin menu items via the Admin dashboard
b. **Manager:** A manager is responsible for all the user management. A manager has the ability to track progress of all the users across our systems
c. **Representative:** A representative is an end user that can view and use our system.

4. Infrastructure Security

The infrastructure is designed to ensure the confidentiality, integrity, and availability (CIA) of information. In particular, the protection of systems and information against unauthorized access, against unauthorized modification or disclosure, and protection of systems against denial of service. Information security roles and responsibilities are defined within the organization. The security team focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of the Awarathon infrastructure. The security team receives information system security notifications on a regular basis and distributes security alert and advisory information to the organization on a routine basis after assessing the risk and impact as appropriate.

Our infrastructure servers reside behind firewalls and are monitored for the detection and prevention of various network security threats. Firewalls are utilized to help restrict access to systems from external attacks and

between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need.

Awarathon has put in place all the relevant guidelines and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data (onsite and offsite). Period tests are conducted to test whether data can be safely recovered from backup devices.

High-quality antivirus and malicious code protection is already integrated. Malicious code protection policies automatically apply updates to these protection mechanisms. Anti-virus tools are configured to run scans, virus detection, real-time file write activity and signature file updates. All Amazon instances, workstations and laptops run such protections.

5. Application Security

At Awarathon we maintain a proper information security policy which our employees comply with. As an organisation we make our employees sign documents indicating that they have read and thoroughly understood the security terms and implications before proving any access to our system. To access any of our internal systems our organisation's domain email and secure password is required which is only given to an employee once he has completed all the formalities. All the company's important communication is done using our organization's domain email id which ensures information security for us and for our clients as well. Once an employee is terminated his/her email id is revoked with all the important information / data safely stored in our system.

Security assessments are done to identify vulnerabilities and to determine the effectiveness of the patch management program. Each vulnerability is reviewed to determine if it is applicable. HTTPS encryption is configured for customer web application access. This helps to ensure that user data in transit is safe and available only to intended recipients.

6. Privacy and Confidentiality

The confidentiality policy states that only individuals with authorization can access data and information assets, we also ensure that the data is intact, unaltered and safely stored in our databases. Our system is available 24/7 which ensures that all the information is accessible when needed. Therefore, the confidentiality policy ensures data confidentiality, integrity and availability.

Using the confidential policy we prevent the following:

a. Use confidential information for any personal benefit or profit
b. Disclose confidential information to anyone outside of our company
c. Replicate confidential documents and files and store them on insecure devices
d. When employees stop working for our company, they're obliged to return any confidential files and delete them from their personal devices.

7. Data support and operations policy

The data stored at Awarathon meets the organizational standards, best practices, industry compliance standards and relevant regulations. All the data like passwords and other confidential information that is stored is well encrypted, our cloud servers are protected using firewalls and with anti-malware softwares inplace. All the important data is well backed-up in the cloud in case of an emergency or in case of data loss.

8. Responsibilities, rights, and duties of personnel

We appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy.

Conclusion

At Awarathon we give utmost importance to you and your company's data. This whitepaper intends to highlight some of the security mechanisms that we undertake to create a safer experience for you. Awarathon provides a highly secure infrastructure for your company's data stored with us. In addition to security we also maintain privacy and integrity for the same.

If you have any questions regarding to any information in this document then please reach out to us info@awarathon.com