Information Security Policy

Policy

Top Management endeavours to support the establishment of Information Security Management system, set a clear policy direction and demonstrate support for, and commitment to information security to cater to all stake holders requirements through the issuance and maintenance of a ISMS Policy across the organization and user groups.

The purpose of Information Security policy is to guide establishment of an Information Security Management System is to ensure a consistent, comparable and reproducible systems which would ensure adequate protection to the information and supporting infrastructure. This includes information assets critical to the operation of the business used within the locations covered under the ISMS deployment and the associated external information assets, belonging to customers, suppliers and business partners in the operation of Organization.

We are custodians of information provided by our partners. We have legal, contractual and moral responsibility to secure all associated information. This is one of the most critical responsibilities we have towards our partners and is important for our existence in business.

The implementation of this policy is a testimony of Organizations continued commitment to maintain and improve the organization's Information Security initiatives and provide confidence to our Stake holders in the conduct of business with Mindfire Solutions.

It is the policy of Mindfire Solutions:

To preserve Confidentiality:

That is to protect Information Assets against unauthorized disclosure.

To maintain Integrity:

That is to protect Information Assets from unauthorized or accidental modification ensuring the accuracy and completeness of the organization's assets.

To ensure Availability:

That is to ensure that Information Assets are available as and when required adhering to the organization's business objectives.

The above policy:
1. provides framework for establishment of functional objectives to achieve planned results.
2. provides commitment to satisfy all applicable requirements related to ISMS.
3. provides commitment to continual improvement and, is communicated and displayed throughout the organization.
4. Reviewed for suitability in each management review meeting.

It shall be made available to interested parties as appropriate.

Mindfire's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions. Mindfire shall ensure that all information that are disbursed or produced by Mindfire has absolute integrity. Mindfire shall guarantee that all relevant information are managed and stored with appropriate confidentiality procedures. The implementation of this policy is important to maintain and demonstrate our integrity in our dealings with all our Stake holders.

It is the policy of **Mindfire Solutions** is to ensure:

- Information Assets are protected against unauthorized access
- Confidentiality of information assets shall be maintained
- Information is not disclosed to unauthorized persons through deliberate or careless action
- Integrity of information is preserved through protection from unauthorized modification
- Availability of information to authorized users is on a need to know basis only
- A formal, structured and comprehensive risk assessment approach ensuring comparable and reproducible risk assessment results shall be developed and deployed to cover all information assets at the organization within the scope.
- Risk Assessment shall be periodically re-reviewed to closely monitor the Residual Risk accepted by the management
- All applicable Contractual, Regulatory and Legislative requirements shall be adhered under Normal, Abnormal and Emergency Conditions

- Business continuity plans are produced, maintained and tested as far as practicable to ensure continuity of business or else speedy resumption of the process shall be ensured, in case of any business disruption
- Information security training shall be given to all Employees, including Sub-contact and temporary employees to ensure that they are aware of their responsibility and authority towards ensuring safety to the Information Assets
- All incidents & weakness within our established Information Security Management System shall be formally reported, investigated and acted upon promptly to ensure effective resolution.
- Learning from these events shall be integrated in existing processes to avoid their reoccurrence

Revision History

Date of Change	Responsible	Summary of Change
28-Nov-2019	SMG	Created

Soumya Mishra
COO/CISO, Mindfire Solutions