Information Security Policy

1. Purpose

The aim of this policy is to provide guidelines for ensuring protection of Information that is stored on the end user devices | servers or in Transit.

2. Scope

This policy would be applicable to all the employees and IT Systems administrators, who handle computer systems and Data.

3. Responsibility

The President-IT would be responsible for effective administration of this policy.

4. Guidelines

4.1. Information stored on servers and storage devices at company datacenters as well as on end user machines are of utmost importance. The Data is also required to be protected while in transit through Data networks. This document provides the guidelines and processes that are in place to ensure confidentiality of the information.

4.2. IT Administrators are responsible for ensuring the confidentiality of Information that is stored on Server and Storage Infrastructure.

4.3. Network Administrators are responsible for ensuring the security of data when it gets transmitted over the wireless and wired network of the company. They also need to ensure protection of Information assets of the company through external threats from Internet.

4.4. Users handing IT equipment's like desktop | Laptop | Handheld devices are responsible to ensure security of both the device and data through use of passwords and following the guidelines provided by IT unit. They are also required to refrain from sharing confidential information with other persons when under employment and even after their separation from the company.

4.5. Contractors and Data Entry operators hired by company are also required to follow the information security guidelines and are responsible for maintaining secrecy of information shared with them during and after their association with the Organisation.

4.6. Information security awareness training will be imparted to the end users from time to time and all employees are required to attend the same and. Also training will be imparted in induction programs.

5. Procedure

5.1. Security controls and account privileges for the servers should be governed by specific SOPs viz. Server Administration, Logical Access Management and Password Management.

5.2. Operating system and database security configuration should be maintained as documented in security configuration documents.

5.3. Datacenters should be physically secured with Biometric access control systems and the access should be governed by Datacenter Operations SOP.

5.4. Data communication through Wireless computer networks should be encrypted and only authenticated users should be allowed access of wireless network.

5.5. Computer networks should be protected from external threats by use of Unified Threat Management system and access to Internet should be controlled and should be in compliance with the Corporate Internet Access Policy

5.6. Intrusion detection and prevention system should be implemented to protect unauthorised access of computer networks and to prevent any data leakage.

5.7. End user computing equipment's should be protected from Viruses and Malwares using Antivirus software and such protection should be monitored on regular basis so as to ensure trouble free operations and prevention of data leakage.

5.8. End user should protect their login passwords and should not share the same with anyone. Such passwords forms the first line of defense and it is necessary that the passwords meets the complexity requirement as mentioned in password policy and controlled through active directory group policy.

5.9. End users are expected to lock their devices when not in use and should not leave them open in order to prevent unauthorised access of Information.

5.10. In case of printing sensitive information, user should use the printers providing password protected print feature or should ensure that the prints are collected from printers immediately after printing in order to ensure confidentiality of the Information.

5.11. Handheld devices must have the Pass code set in order to protect against misuse and such pass codes should not be shared with anyone. In order to separate corporate data from personal data and to centrally administer such hand held device Mobile device management software should be deployed.

5.12. The required access of business application should be given after having the approval from the designated business owner in line with the Application Change management process.

5.13. HR should provide employee separation notification to IT as soon as the employee separate from the company. IT administrator should ensure to revoke the account privileges in a time bound manner.

5.14. In the event of a breach happening on account of non-adherence to the guide lines mentioned in the policy document the user accounts of concerned user/group of users responsible for such a breach will be suspended on immediate basis and their access to the compute device as well as business applications will be denied until a final decision is taken by HR unit in accordance with the "Code of Conduct" Guide line. If the offender is an external entity, our

legal department will be requested to take appropriate action as applicable. Business unit will be responsible to ascertain the Business Impact of such a breach and IT unit will provide the relevant system and audit logs as required by the Business function or HR.

5.15. Security breach will be recorded by IT unit as an Incident and necessary counter measures or process changes will be identified and put forward for management approval. Upon approval the same will be deployed in order to prevent recurrence of such breach in future

5.16. IT team in consultation with HR will plan and organise security awareness training for users.

5.17. IT managers handling the information management system will be encouraged to attend training programs | webinars organised by security solution providers in order to hone their skills and for up keeping of their information security knowledge.