AUDIT TRAIL POLICY

Audit Trails are maintained for both systems as well as application process by user activities and applications.

The series of records of computer events about the operating systems. The applications and the user activities. The different audit trails are required to be maintained and audit trails provides information about computer systems and helps to audit of the computer system.

The audit trails is used to establish individual accountability which has helped the user proper behavior.

Any events to circumvent security policy will be revealed immediately and the appropriate actions are taken immediately.

Any specific problem is always investigated by use of audit trails and system activity to find out what exactly happens.

The event is reconstructed at appropriate level and it is analyzed to find any misuse or mischief created by any user and also to prevent unauthorized use of the system and the network on real time basis. It has also helped the virus attack and it has prevented the unacceptable system performance. The identification process immediately detects the unauthorized access

was attempted and resultant damaged is assessed and controls which were attacked.

System maintains several audit trails on concurrent basis which are recorded and saved.

Further such records are reviewed on regular basis which also includes keystroke monitoring. These logs are preserved in the system.

The review of audit trails has been utilize to find tune the system performance and to avoid any flow violations of security policy committed in application, this helps the misuse of the system by any individual user and all users remains accountable.

The audit trails also examine the access control and its violation.

The record of email application logs and its logs prevents the data pilferage the appropriate action after establishing the misuse and ate\tempt of accessing the data in unauthorized way.

System administrator is required to record the logs of user activities. The sensitive server applications and accessing the network is required to examine regularly.

The attempts of log-in and unsuccessful log in are been checked.

Application level audit trails are monitored and records are been maintained to examine the confidential information is not available to any unauthorized user.

User audit trails the commands directly initiated by the user and also any unauthorized attempts and files and resources access any attempt to delete the log is viewed and noted very seriously.

There is this audit logs are preserved for minimum 1 year and they are not available for review, access or monitor by anyone other than CEO or system administrator they are confidentially preserved.

The audit trails are reviewed after any events or any software malfunctioning.

The periodic review of audit trail data is being carried out by system administrator and under directions from CEO.