AUDIT TRAIL POLICY

Scope

The audit trails policy is used to establish individual accountability and secured structure for the organization.

Policy

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

Series of records are maintained about computers, its events, operating systems, updates etc. Systems are check for their functionality by the IT Administrator on a daily basis to verify that all basic operations of the computer are functioning properly and essential applications (such as ODIN, Office, Operating system, Internet, Local Area Network, etc.) are operating without any glitch.

Each computer is installed with a username and password. This allows for authenticated access for every user. Any events to circumvent security policy will are revealed immediately and reported to the management for further decision making. Each system is installed with antivirus program which helps avoid access of unsafe applications onto the system. The antivirus application immediately detects/prevents unauthorized access of threat files. It also maintains logs of files which may have been affected/damaged due to attack.

Every computer is assigned a dedicated IP through which it is connected on the local area network/internet. In case of any unusual activity or heavy bandwidth usage may be tracked on the network. This allows for balanced distribution of connectivity within the office.

Common document database of the organization are segregated division wise and password protected. Unauthorized access to third parties or unknown personnel is thus avoided. Backup of these databases are done by the IT administrator on a weekly basis, any error or unsafe files are segregated from the system and deleted or healed. Copy of the backup databases is maintained at an offsite location for safety purposes. Any unauthorized attempts to access files and resources, any attempt to delete the log is viewed and noted seriously and brought to the notice of the management for further action.

Every division has an installed video camera for visual record of activities taking place within the division. The video cameras are monitored on a daily basis and log is maintained where unusual activity is recorded.

Backup of all important documentation is taken every day and maintained with the IT administrator and senior personnel for safety and security reasons.

IT administrator is required to record the logs of user activities. The sensitive server applications are password protected thus restricting unauthorized access. Logs are monitored for any unusual activities taking place on the servers. Only authorized personnel are allowed to carry out system/operation related activities on the servers.

Any problems arisen are investigated through the use of logs and records maintained by the systems. Loop holes in the system are identified and rectified subject to being bought to the observation of the management. An 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.

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

The reviews/records of audit trail are utilized to fine tune the system performance and to avoid any flow violations of security policy committed in application. The audit trail review process helps avoid the misuse of the system by any user.

Audit logs are preserved and they are available for review only to authorize personnel or IT system administrator.

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

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

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