Audit Trail Policy

- All client activity logs are being maintained in Odin manager and the backup are maintained for the same.

- Log records are being viewed on biweekly basis.

- Weekly audit are taken regarding the record of system activity both by system and application processes and by user activity of systems and applications.

- Biweekly audit are conducted in detecting security violations, performance problems and flaws in applications.

- Audit work is performed in concert with logical access controls, which restrict use of system resources. Granting users access to particular resources usually means that they need that access to accomplish their job.

- Users cannot be prevented from using resources to which they have legitimate access authorization; audit trail analysis is performed to examine their actions.

- Audit is conducted to reveal that an individual is printing far more records than the average user, which could indicate the selling of personal data.

- If a system or application is deemed to be critical to an organization's business or mission, real-time auditing may be implemented to monitor the status of these processes.

- Audit Trail Review after an Event. Following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem, the appropriate system-level or application-level administrator reviews the audit trails. Review by the application/data owner would normally involve a separate report, based upon audit trail data, to determine if their resources are being misused.