Monitoring

Objective

JLI shall monitor its information technology processes to ensure that IT Operations are managed and performed in a controlled environment so that the overall IT and business objectives are met.

Prerequisite

This procedure should be read in conjunction with:

- Information Security Policies, including:
- Access Control Policy

Responsibility

- Group Head Digital, Technology and Strategic Planning
- IT Sectional Manager
- Database Administrator
- Application Administrators
- System Administrator
- Network Administrator

Policy

- Group Head Digital, Technology and Strategic Planning or his designate shall ensure that audit logs are maintained as per Access Control Policy.
- Audit logs shall be protected against unauthorized modifications.
-
- Privileged ID audit logs shall be reviewed as per frequency defined in the Access Control Policy.
- System Administrator, Application Administrator, Network Administrator and DBA are responsible for generating audit logs for their respective applications / OS / Devices.
- In absence of a Biometric device used to secure access to server room, a manual entry logs for server room shall be maintained by Data Center owner / IT Sectional Manager or designated personnel.
- Group Head Digital, Technology and Strategic Planning or his designated resource(s) will maintain all records pertaining to the review of logs so as to demonstrate compliance with JLI's IT Operational policies and procedures for auditing purposes.

Application Level

User level application rights and roles shall be reviewed in accordance with the Access Control Policy.

- Privileged Users rights and roles shall be reviewed in accordance with the Access Control Policy

Database Level

User level database log review shall include, but is not limited to, the following:

- Unauthorized access.

Privileged ID database log review shall include, but is not limited to, the following:

- Any modifications made to core data/schema etc. (insert, update, delete)
- Any modification made to file/data dictionary.

Data Centre / Server Room

- Access logs of employees and third party manual logs shall be reviewed depending on frequency of visits to data center.

Network Configuration / Firewall

- Logs of firewall and proxy server shall be reviewed from time to time to detect access to blocked/banned websites.
- Network configuration changes shall be reviewed to ensure they were authorized.

Operating System

System Administrator activity log review shall include, but is not limited to, the following:

- Patch Updates history
- User administration activities to detect if any unauthorized roles have been granted to users or administrators