LOGGING AND MONITORING POLICY

Keynote Financials Services Ltd.

K E Y N O T E

(DATE)

Author:	MD(Designation)
Owner:	MD(Name)
Organization:	KFSL
Version No:	1.0
Date:	(Date)

Document Control

Document Title Logging and Monitoring Policy

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	(Date)	MD(Name)	NA

Approvals

Name	Title	Date of Approval	Version No
MD(Name)	Logging and Monitoring Policy	(Date)	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	(Date)	NA

1.0 LOGGING AND MONITORING POLICY

1.1 PURPOSE

- IT infrastructure components forms a crucial part of KFSL operations. IT assets are constantly under threat from malicious users and as a result, needs to be monitored effectively on a continuous basis for any abnormal activities. This policy aims to establish effective system to centrally log and monitor information security controls.

1.2 SCOPE

This policy applies to:

- All staff and non-employees, stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of *KFSL* and other individuals, entities or organizations that have access to and use *KFSL* information processing systems and card holder data environment to perform their daily job-related responsibilities or meet their contractual obligations.
- All Information assets involving data, applications, network, security devices, servers and other IT system

1.3 POLICY STATEMENTS

Logging shall be enabled on all information processing assets. All access to critical applications and *KFSL'* network shall be logged and monitored for suspicious activities or security breaches and adequate response mechanism shall be setup for controlling security breaches.

1.3.1 LOG MONITORING

- Logging shall be enabled for all the critical devices including application servers, network devices and security devices.
- The logs of the applications shall be monitored periodically to ensure proper functioning and policy compliance.
- Some of the following activities and parameters shall be logged and monitored, but not limited to:
  - Access to all audit trails
  - Initialization of audit logs
  - Stopping or pausing of audit logs
  - Remote access activities of vendors
  - All individual access to cardholder data
  - Actions taken by any individual with root or administrative privileges
  - Invalid logical access attempt
  - Identification and authentication mechanisms

- Creation and deletion of system level objects

- Parameters related to audit trails:
  - Ensure user identification is included in log entries
  - Ensure type of event is included in log entries
  - Ensure date and time stamp is included in log entries
  - Ensure success or failure indication is included in log entries
  - Ensure that audit trails are enabled and active for system components
  - Ensure ONLY individuals who have a job-related need, can view audit trail files. Access to audit trail files shall be monitored regularly
  - Ensure current audit trail files are promptly backed up to a centralized server or media that is difficult to alter
- The logs shall be analyzed for the following:
  - Unauthorized access
  - Configuration changes
  - Abnormalities in mail routing events
  - Failed logins
  - Denial of service attempts

1.3.2 INCIDENT REPORTING

- Any incident shall immediately initiate the IT Incident Management Process as per the IT Incident Management Policy.
- Designated Officer shall prepare the “Log Analysis Report”, post any event identified.

1.3.3 BACKUP

- Logs in the centralized server shall be backed up on a periodic basis.
- The backup logs shall be protected from unauthorized access.
- The Retention period of the logs shall be decided by the Designated Officer. Though all logs shall be maintained for minimum period of 1 year.