IT INCIDENT HANDLING 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 **IT Incident Management 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)	IT Incident Management Policy	(Date)	1.0

Distribution

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

IT INCIDENT MANAGEMENT POLICY

1.1. PURPOSE

The purpose of this policy is to ensure timely and effective response to IT incidents by restoring service operations to agreed level as quickly as possible.

1.2. SCOPE

- All staff and non-employees and other individuals, entities or organizations responsible for administering and maintaining KFSL Information processing systems.
- All Information assets involving data, applications, network, security devices, servers and other IT system.

1.3. POLICY STATEMENT

To promptly report, investigate, and resolve all incidents that are or may be a threat to secure and effective Information Technology operations and the network.

1.3.1 GENERAL STATEMENTS

- 'Incidents is a term related to exceptional situations or a situation that warrants intervention of specialist help or senior management. An incident is detected in day-to-day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of KFSL
- All users and IT administrators shall be responsible for identifying incidents. Some examples are:
    - Abnormal system resource usage: If the CPU or memory utilization on a system is very high compared to the normal usage, the system could have been compromised. Compromised systems could be exploited by attackers for spreading viruses.
    - Abnormal, slow response of the application: Users could experience extremely slow response times if the application servers or the network has been compromised.
    - Data Corruption: If the user finds that data or files stored on the desktop/laptop has been either deleted or modified without their knowledge.
    - Change in system: If your desktop/laptop configuration looks different in terms of the applications installed, screen savers or icons on the screen, or the system is misbehaving.
    - Changes in password and user-id: Users shall report if they find their passwords have been changed or their account has been locked without their knowledge.

- Virus infection: Users shall report any virus or worm that infected one or more hosts. However, viruses or worms that are detected and cleaned by anti-virus software need not be reported; only those which are not getting cleaned and infecting the system needs to be reported.
- Changes in applications: If the applications accessed by user look different from its normal appearances.
- Security weakness detected: If any weakness in the applications accessed by user that can cause unauthorized access or modification or lead to any kind of compromise.
- Violation by others: Any instance of security violations committed by others like running of malicious tools, trying to break into system or committing IT frauds or thefts, copyright or license agreement violations, user shall report such instances.
- Denial of service or disruption to system activity - Such incidents include:
  - Distributed denial of service attack (D Dos) causing loss of external network connections through packet flooding
  - Causing system to crash
  - Causing system to partially or completely fail
- Changes to system software/firmware, hardware or environment without approval - Such incidents include:
  - Addition of software/hardware with malicious intent (e.g., keystroke logging or backdoor)
  - Unauthorized removal, addition or replacement of equipment
  - Installation of back door code without authorization
- Loss or physical damage to the systems
- Unauthorized activation of suspended / deleted user accounts

The importance of incident detection and analysis shall be propagated throughout the organization and users shall be made aware of the importance of the same and their responsibilities towards reporting of incidents and security weaknesses or any software malfunction.

1.3.2 IT INCIDENT REPORTING AND RECORDING

- All employees of KFSLshall be aware of their responsibility to promptly report any IT incidents.
- All IT related incidents shall be reported to the respective reporting manager, Designated Officer, Technology Committee or HR Head via phone or email.
- The Designated Officer shall evaluate the information, determine the potential for loss and the risk to the, and assign the incident to the Incident Response Handling Team or SOC Monitoring Team.
- The following details shall be recorded initially:
    - Details of the user(s) who reported the incident including contact details
    - Detailed description of the incident including time of incident
    - Asset / service affected
    - Details on how the incident was discovered / detected
    - Supporting evidence
    - Remedial steps taken, if any
    - Incident classification

1.3.3 IT INCIDENT PRIORITIZATION

Incident Management Priority Matrix	
Severity Level	**Description**
Severity 1 **(Major Impact)**	Direct threat or damage to image, reputation or credibility of KFSL Multiple business functional units getting severely impacted.
Severity 2 **(High Impact)**	Severe outage affecting single business functional units, key services or location.
Severity 3 **(Moderate Impact)**	Moderate degradation to business functional units, locations, IT assets. Moderate to high impact to non-critical business units within organization.
Severity 4 **(Minimal Impact)**	Small issue with localized scope. Affecting few resources. Issue can be tolerated for a particular period of time.

All Incidents shall be prioritized based on the severity of the Incident.

1.3.4 IT INCIDENT HANDLING

- Employee should report suspicious incident or event to Designated Officer.
- Designated Officer will assign unique Incident ID
- Designated Officer shall evaluate the information contained on Incident ID to determine the potential for loss and the risk to the Company
- Designated Officer assigns the incident to the Incident Response Handling Team.
- The Incident Response Handling Team shall analyse the incident evidence, develop and test hypotheses regarding the incident, develop a set of findings and conclusions, and resolve the incident.
- The Incident Response Handling Team should perform a post-incident analysis, after an incident has been fully handled and all systems are restored to a normal mode of operation.
    - Analysing what has transpired and what was done to intervene
        - Did detection occur promptly or, if not, why not?
        - Was the incident sufficiently contained?
        - Was communication adequate, or could it have been better?
        - What practical difficulties were encountered?

        - Was the incident caused due to negligence or malicious intent on part of an employee?
    - Analysing the cost of the incident
        - How much is the associated monetary cost/ time?
        - How much did the incident disrupt ongoing operations?
        - Were any data irrecoverably lost, and, if so, what was the value of the data?
        - Was any hardware damaged?
    - If any employee is suspected guilty, the HR should be informed for initiating disciplinary proceedings against the employee.
- The Incident Response Handling Team should discuss actions that were taken, and shall be recorded for future references
    - Workarounds and measures adopted to mitigate incident shall be updated in knowledge base.
    - Lessons learned, recommendations, and deficiencies should be presented to the Senior Management for discussion related security planning.
- The Team should report Incidents to respective exchange on quarterly basis.