IT ACCESS CONTROL POLICY

Keynote Financials Services Ltd.

K E Y N O T E

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

Document Control

Document Title **IT Access Control 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 Access Control Policy	(Date)	1.0

Distribution

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

1.0 IT ACCESS MANAGEMENT POLICY

1.1 PURPOSE

The purpose of this policy is to establish the framework and the rules for controlling logical access of KFSL users to the information processing systems of KFSL

1.2 SCOPE

This policy applies to all staff and non-employees and other individuals, entities or organizations responsible for administering and maintaining KFSL 's IT infrastructure.

1.3 POLICY STATEMENT OF LOGICAL ACCESS

The Company shall control access to its information to help ensure its confidentiality and integrity.

1.3.1 ACCESS CONTROL

- Access shall be provided to meet following two principles of Role Based Access Control:
  - Need-to-know: granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile)
  - Need-to-use: granted access to the information processing facilities
- There must be a formal user access provisioning and de-provisioning procedure for granting access to information, information processing systems and IT services.
- All users shall have controlled access (read, write, modify, execute, full control) to information processing systems, in accordance with the user's functional role and information security requirements.
- For Contract Employees, Interns and Consultants, the validation of the ID must be only for the period of contract and must be automatically De-activated thereafter. There must also be a periodic review of the same.
- A record of disabled accounts must be maintained by the Designated Officer & Technology Committee.
- All information processing systems shall be configured to enable audit logs.

1.3.2 USER ID

- Unique user IDs shall be assigned to each user for the purpose of their job roles and responsibilities.
- KFSL 's IT administrator is responsible for creation of all KFSL 's User IDs.
- All User IDs shall follow a standard naming convention defined as a part of this policy:
    - For KFSL employees (permanent and contractual basis) the naming convention is <First Name>Dot<<Last Name>
    - If the User ID already exists, <First Name>DOT<Last Name><Numeric Value> shall be considered.
- User-IDs and related passwords shall not be shared with any other individual.
- User-IDs must be disabled and deactivated when the user leaves KFSL
- Anonymous user-ids (such as "Guest") must not be allowed.
- Common user-IDs must not be issued to multiple users. In situations where a common ID is required, written permission shall be taken from Senior Management and Designated Officer.
- Default user-IDs and passwords shipped with information processing systems and software applications must be disabled.
- User-ID that is inactive for a maximum period of 60 days shall be disabled after seeking the approval from the user's reporting manager and/or Designated Officer.

1.3.3 PRIVILEGE MANAGEMENT

- All privileges to the users shall be assigned through a formal access provisioning procedure
- Designated Officer shall ensure that no privileges are assigned before access request is approved by his/her reporting manager.
- Privileges that are temporarily granted shall be authorized and tracked. Such privileges shall be revoked as soon as they are deemed not required.
- Designated Officer shall maintain detailed records for all allocated privileges.

1.3.4 REVIEW OF ACCESS RIGHTS

- Designated Officer in coordination with Technology Committee shall review all user access rights at least every 12 months.
- Designated Officer shall review access logs, security logs, etc., on a periodic basis (once in 6 months is recommended). Findings of such reviews shall be reported to senior management for their review and possible action.
- Privileged accounts shall be reviewed by the Designated Officer at least every 6 months, and changes to such accounts shall be logged for periodic review.

1.3.5 NETWORK ACCESS CONTROL

- Access to networks and network services shall be specifically requested by the user's reporting manager and reviewed by Designated Officer.
- Remote user access to KFSL network shall be subjected to appropriate user authentication and Cryptographer controls, for example, use of VPN (virtual private network) connectivity and two factor authentication / security tokens.
- Wireless networks and publicly accessible systems shall be segregated from the rest of the internal network.
- Wireless networks shall be secured by binding each IT asset's physical address (MAC address binding) on wireless access point.
- Groups of information processing systems, services and users shall be segregated on networks based on their sensitivity and classification of information stored or processed, exposure to public networks/users and corresponding risk levels.
- Access between the segregated network segments shall be appropriately controlled.
- Use of Network services shall be continuously monitored.
- KFSL shall formulate an internet access policy on content filtering proxy device to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within their critical IT infrastructure.

1.3.6 SECURE LOG-ON

Secure log-on shall be implemented for systems and applications, as follows:

- Information processing systems shall suspend the user account and prevent user access to the system when an incorrect user password has been entered for specific number of times
- All actions performed by an individual on system programs shall be logged.
- All systems shall be locked, or sessions terminated after a defined time of inactivity.

1.3.7 MEASURES FOR APPLICATION AUTHENTICATION SECURITY

- Any Application used by KFSL containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as “Application” over the Internet shall be password protected.
  - Strong password policy must be followed as per company’s policy.
- Passwords, security PIN s etc. shall never be stored in plain text and shall be one-way hashed using strong cryptographer hash functions before being stored in database.
- For added security, multifactor e.g., two-factor authentication scheme shall be used. In case of IBTs and SWSTs, two-factor authentication is mandatory.
  - In case of Applications installed on mobile devices (such as smart-phones and tablets), a cryptographically secure bio-metric two-factor authentication mechanism shall be used.
- Post multiple failed lo gin attempts into Applications; the Customer’s account should be locked out.
- KFSL hall focus on strong multifactor authentication for security and educate Customers to choose strong pass-phrases.
  - Customers may be reminded within 60 days intervals to update their password.
- Logins attempts to system much be logged for both successful and failed attempts.
- CAPTCHAs can be implemented for limiting the brute force attack and enumeration attacks against logins.