PHYSICAL SECURITY POLICY

KEYNOTE FINANCIAL SERVICES LIMITED

K E Y N O T E

31ST JANUARY 2025

(DATE)

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

Document Control

Document Title **Physical Security 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)	Physical Security Policy	(Date)	1.0

Distribution

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

1.0 PHYSICAL SECURITY POLICY

1.1 PURPOSE

Physical and environmental protection of office facilities is of prime importance to KFSL

The purpose of this policy is to build a secure environment that will protect against unauthorized physical access and environmental threats to KFSL facility.

1.2 SCOPE

This policy applies to:

- All staff and stake holders, non-employees of KFSL and other individuals, entities or organizations that have access to KFSL information systems
- All Information assets involving data, applications, network, security devices, servers and other IT system that needs to be appropriately protected from physical and environmental threats

1.3 PHYSICAL SECURITY POLICY STATEMENTS

Information processing facilities must be secured from unauthorized access, damage or interference. Physical security measures must be in place to ensure the security and integrity of information processing facilities and the information assets.

1.3.1 SECURING THE OFFICE PREMISES

- The main entry to KFSL office must be secured with appropriate controls like Access Cards / CCTV Camera
- All offices entry points shall be locked, when unattended, beyond working hours
- Movement of IT Assets must be recorded with appropriate information to track its movement

1.3.2 SECURING PREMISES FROM THIRD PARTY AND VISITORS

- The date, time of entry and departure and the purpose of visit must be recorded during office hours or outside office hours in a visitor's log maintained at reception.
- If separate area for loading or delivery of goods is not available, it shall be done at reception of the office.
- In Visitor's Register, all visitors shall be made to declare their personal belongings. Example: Laptops / Tablets / Camera Phones / Storage Devices.
- Strict access control measures shall be put in place to lockdown unused network points. Network Access to visitors or guests shall be granted upon prior approval by Designated Officer or Technology Committee.

1.3.3 SECURING INFORMATION STORAGE MEDIA

- All information storage media containing sensitive or confidential data shall be physically secured and access must be restricted to authorized personnel only.
- Back-up media shall be stored in fire resistant safes or cabinets and a copy of all backup media shall be maintained at an off-site location.
- Employees, Visitors and third parties shall not be allowed to bring along their personal laptops or any other external storage devices, unless authorized by Designated Officer or Technology Committee.

1.3.4 PHYSICAL SECURITY OF PORTABLE COMPUTING DEVICES

- Official Portable computing devices (Laptops, phones etc.) shall not be left on desk unattended for extended period or any other visible location overnight.
- In the event of a portable computing device being stolen, the concerned employee shall notify Designated Officer or Technology Committee about the theft immediately.
- Access to such portable and physical medias shall be controlled by encryption mechanism necessary to warrant loss of confidential information

1.3.5 CLEAR DESK AND CLEAR SCREEN

- Computer terminals when unattended shall be locked out or password protected.
- Controls like Automatic screen lockout or screen-saver passwords shall be enabled if left unattended for more than ten minutes.
- Files and other papers that contain sensitive information shall be protected from unauthorized access.
- Users shall not leave papers unattended on printer trays, photocopiers or their desks.
- Information classified as 'Restricted (in paper format or storage media like CD's, DVD or Tapes) shall be locked in a fire-resistant safe or cabinet, when not required.

1.3.6 EQUIPMENT SECURITY

- Eating, Drinking or smoking shall be restricted in secure areas where information processing equipment is placed.
- Combustible materials shall not be stored in secure areas where information processing equipment is placed.
- Only authorized maintenance personnel must be allowed to service or perform repairs on equipment.
- The confidentiality and integrity of all information shall be ensured prior sending any information processing equipment for repairs or maintenance.

1.3.7 SECURE DISPOSAL OR RE-USE OF EQUIPMENT

- All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

- Devices containing sensitive information shall be physically destroyed or the information shall be deleted or overwritten using adequate format techniques such that the original information remains non-retrievable in any manner.

1.4 ENVIRONMENTAL SECURITY POLICY STATEMENTS

Adequate environmental security measures must be implemented to reduce exposure to environmental threats.

1.4.1 ENSURING SUITABLE ENVIRONMENTAL CONDITIONS

- The air-conditioning and humidity levels must be monitored.
- Smoking is strictly prohibited inside the office area. It may be permitted in the open designated areas only.

1.4.2 SECURING PREMISES FROM FIRE

- All computer systems must be housed in an environment equipped with fire extinguishers.
- The fire extinguishers must be placed in such a way so that they are easily accessible in all areas.
- Fire safety equipment must be checked regularly in accordance with manufacturer's instructions. A maintenance records must be maintained with the equipment.
- Comprehensive fire and emergency instructions must be displayed in prominent locations.
- Functioning and operations of the fire safety devices / equipment installed by KFSL must be explained to employees and security guards periodically during Internal Training Programs.
- Regular mock drills shall be conducted to ensure effectiveness of the training and instructions to be followed.