NETWORK SECURITY POLICY

Keynote Financials Services Ltd.

KEYNOTE

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

Document Control

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

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

1. NETWORK SECURITY POLICY

1.1 PURPOSE

The purpose of this policy is to ensure authorized and secure access to KFSL network infrastructure internally and from external networks and establish effective management/assured Network services quality and service continuity.

1.2 SCOPE

This policy applies to:

- LAN and WAN network infrastructure at Primary site deployed and maintained by KFSL
- Relevant third-party personnel responsible for administering and maintaining KFSL IT infrastructure
- All Infrastructure Coordinators and Infrastructure Specialists, Section Heads, administering and maintaining the network infrastructure viz. LAN and WAN
- All IT assets used to build the network viz. network devices, communication links and assets that use the network viz. servers, desktops, smart devices owned by KFSL

1.3 POLICY STATEMENTS

- KFSL network infrastructure shall be adequately designed, managed and controlled in order to strengthen security, continuity and quality of its IT assets and services.
- All connections to external networks including Internet, outsourced vendors and partners will be authorized and provided in a secure and controlled manner.
- Any kind of remote access to KFSL network must be first approved based on valid business justification and initial risk assessment done by Head of Information Security.
- Network shall be designed and maintained for high availability to meet the Business Continuity requirements.

1.3.1 NETWORK ACCESS

- All user accesses to the network resources shall be approved and authenticated.
- Administrative access and privileges on servers, network devices and other KFSL' IT systems shall be granted only after necessary approvals from Head of Information Security.
- Prior approval shall be taken from Head of Information Security to connect desktop, laptop, smart phone or any network endpoint to KFSL network (wired or wireless), including the guest wireless access for third party officials working within the wired/wireless network coverage.

- Before porting a new application on KFSL network, Head of Information Security shall study the network usage of application, it's impact to existing infrastructure and provide the report which shall minimum contain the following details:
    - Whether the existing network infrastructure can accommodate the new application without affecting the existing applications
    - Whether there is need to modify the existing network infrastructure in order to accommodate the new application.
    - If there is need for modification, provide the estimated expense involved and the estimated time required for implementing the modification
- Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data shall be blocked and measures taken to secure them.

1.3.2 SEGREGATING SERVER AND USER SEGMENTS

- A list of mission critical servers or servers processing sensitive information shall be prepared.
- List of critical servers shall be periodically reviewed and updated. All critical servers shall be separated from LAN users by creating dedicated server segments on firewalls.
- The user segment and the server segments must be distinct and access between them must be controlled.
- Server's segments shall be segregated and secured from user LAN by firewalls and continuously monitored by Head of Information Security for any malicious or abnormal traffic.
- In addition to firewall rules, all critical servers shall have restrictive access control policies configured on them which provide access to users on "Need to know" and "Need to Access" basis only.
- Internet facing servers and servers accessed by external parties like the Extranet shall be hosted on a separate segment De-Militarized Zone – DMZ Segment.
- Utility servers like AV, Active Directory, Proxy, etc. shall be on a separate segment – Server Segment
- Application and database servers shall be protected by placing them on separate protected segment. This segment shall be accessible to authorized users only.
- Intrusion Prevention System (IPS) shall be strategically installed at network segments to monitor the traffic flowing, to and from critical servers.

1.3.3 SEGREGATION OF DEVELOPMENT & PRODUCTION FACILITIES

- Production systems shall be segregated from development and testing systems to mitigate unwanted modifications to live systems.
- Development and testing personnel shall not have direct access to production systems. If required, such access shall be through strict authorization and access control.
- Development, UAT and Production environment shall be segregated from each other with adequate access rights.
- Demilitarized Zone (DMZ)
- A list of DMZ servers (servers which are going to face Internet or process external requests) and ports / services to be opened for external users shall be prepared by respective administrators and submitted to Management Representative - Information Security Officer (MR-ISO).
- Request to open service or ports shall be supported by valid business justification from respective administrators.
- MR-ISO shall approve the request after adequate review and forward the approved request to Infrastructure Team.
- List of DMZ servers and open services shall be periodically reviewed and updated by the Infrastructure Specialist.
- Demilitarized Zone (DMZ) segment shall be created on firewall for Internet facing servers that hosts services that an organization needs to make available to the general public (such as web server, Mail server, Internet Banking Server etc.)
- DMZ shall be segregated from the internal server segments and LAN users through a firewall.
- Both Incoming and Outgoing traffic shall be continuously monitored for any malicious content.
- All channels connecting to DMZ resources shall preferably be encrypted. (SSL using valid certificates, VPN Tunnels with strong encryptions etc.)
- Event logging shall be enabled for all DMZ resources to send logs to a centralized log server.
- Internal IP address of DMZ servers shall be properly NAT-ed with Public IP address on firewalls.
- Internal IP addresses (Private IP Addresses) shall not be allowed to pass from the internet into the DMZ.(Configure Anti spoofing Rules)

1.3.4 VPN CONNECTIVITY

- Any approval for Remote access via Internet to KFSL IT systems shall be granted by Head of Information Security.
- Remote access to network resources must be done using the SSL / IPsec VPN infrastructure provided by KFSL. SSL must always be used for remote desktop protocol or SSH.
- Head of Information Security shall conduct quarterly audit of the VPN users.

- The use of remote access to KFSL IT systems is strictly prohibited without a reasonable and documented business reason illustrating the necessity to complete job responsibilities.
- The VPN system shall automatically disconnect sessions upon reaching an idle time of 15 minutes.
- Remote access for vendors shall be enabled to the test and development environment upon receiving a written request, with adequate business justification and approved by Head of Information Security
- It is prohibited to copy, move, or store KFSL data into local hard drives and removable media while using remote access to KFSL IT systems.

1.3.5 NETWORK DEVICES – ROUTERS & SWITCHES

- Network devices like routers; switches; etc. shall be configured securely as per the Secure Configuration Document (SCD).
- Each Router & Layer -3 devices shall have the following statement as a banner in clear view:
  - "UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device are logged, and violations of this policy shall result in disciplinary action and will be reported to law enforcement."

1.3.6 NETWORK DEVICES – FIREWALL

Access to the Firewall

- The firewall shall be hardened and secured as per the Secure Configuration Document
- The firewall shall not have any additional services that can be accessed remotely
- The firewall shall be placed in a controlled environment with access only to authorized personnel
- Any unused physical interface shall be disabled/de-activated on the firewall

Firewall Rule Base

- Firewall rule-base shall only allow access to required ports and services on the target machine.
- Access requests for all the opened ports and services with valid business justification shall be documented and maintained
- Rule addition must be approved by Head of Information Security Officer prior to deployment
- All connections from the internal network to external networks shall be approved by the Head of Information Security. All connections to approved external networks shall pass through firewalls
- The rule base shall have a Stealth Rule which is a rule to deny all access requests that are not explicitly allowed

- The placement of this rule in the rule base is critical and shall be placed after all VPN and administrative and access rules to the firewall
- Firewall rule base shall deny all the ICMP Traffic
- Firewall rule base shall deny all the IP spoofing by enforcing egress filtering

Firewall Administration

- Default device password of the firewall shall be changed before deploying the device into the production and follow the Password Security Guideline.
- Unique usernames shall be used by each firewall administrator

Firewall up gradation and Patches

- Firewall shall be updated with latest stable firmware upgrades and patches released by the firewall vendor and follow the Patch Management Policy and Procedure
- Infrastructure Team shall evaluate new version release of firewall, test and verify if the upgrade is required or not before applying it in production
- After any upgrade, firewall shall be tested to verify all functionalities are working as desired

Firewall redundancy

- Redundant firewall in HA (High availability) mode shall be configured so that in case of a firewall failure, the backup firewall shall be switched in order to maintain the security level

Change Control

- Appropriate change control procedures shall be followed when making changes to the firewall system, including but not limited to -
  - Upgrades or modification of the firewall application
  - Addition of new firewall system hardware
  - Physical movement of firewall system components
  - All new user access requests shall be accompanied with business requirement and access details such as the IP address and the corresponding port numbers
  - All changes to the firewall application shall be approved by the Head of Information Security
- Firewall rule base reviews needs to be done on periodic intervals (yearly once).

1.3.7 WIRELESS NETWORKS

- External auditor can perform wireless audit to detect unauthorized access points, at frequency of once a year.

- For any unauthorized access point detected Information Security Specialist should check for existence of any suspicious network. If such access points exist, such access points should be disconnected immediately.
- All unauthorized networks that are detected should be discussed with KFSL senior management and it should be documented in MOM.

1.3.8 CLOCK SYNCHRONIZATION

- Network Time Protocol (NTP) shall be used to ensure synchronization.
- Clocks of all the systems throughout the organization shall be synchronized with NTP server.
- Any changes to time settings on critical systems shall be logged, monitored, and reviewed.

1.3.9 NETWORK LOGGING

- Adequate levels of information to be logged shall be clearly defined and configured.
- Type of log category and log information shall include the following:
    - Users - Login/logout information: location and time of failed attempts, attempted logins to privileged accounts; changes in authentication status such as different privileges etc.
    - Networks - Service initiation requests: name of the user/host requesting the service; network traffic; new connections.
    - Applications - Applications and services specific information: mail logs, ftp logs, web server logs, modem logs, firewall logs, router logs.
    - File Systems - Changes to access control lists and file protections; file accesses (opening, creating, executing, deleting).
- The log files shall be protected from being accessed, modified or deleted by unauthorized users and shall be stored in centralized log repository with restricted access.

1.3.10 RESTRICTION ON FILE TRANSFER PROTOCOL (FTP) SERVICE

- The use of File Transfer Protocol (FTP) shall be restricted on production systems
- The IT administrators for all servers shall ensure that anonymous file transfers (anonymous FTP) into the company system are disallowed
- If needed, then use of SFTP (Secured File Transfer Protocol) shall be encouraged, instead of FTP service
- No inbound FTP shall be allowed from the Internet to the firewall or internal network unless approved

- All files that are downloaded via SFTP shall undergo malware scan

1.3.11 NETWORK ARCHITECTURE DIAGRAM

- Network Architecture diagram shall be kept confidential and shall be made available only on need-to-know basis after the approval of Head of Information Security.
- Network Architecture diagram shall be updated as and when changes are done, latest network diagram shall be aligned with Business Continuity Plan/Disaster Recovery Plan.
- There shall be strict version control for Network Architecture Diagrams, and they will be stored in a centralized configuration register under the custodian of the Head of IT Infrastructure.
- Network Architecture diagram shall be:
    - Reviewed and updated at least annually
    - Shall clearly indicate wireless networks which are used in KFSL
    - Shall clearly indicate the author, approver, date created, date reviewed & version number
    - Shall include all internal and external network devices, endpoint devices, server segments, logical and physical inter connections, WAN locations, LAN, internet and connection to service providers.