Network Security Policy

Introduction:

Networks play an important role in any business operations. Computer networks of ADF shall be segregated from external networks and all connections to external networks including the internet, outsourced vendors and partners shall be authorized and provided in a secure manner. All remote access to the ADF's network must be authenticated and provided based on business requirements. Networks shall be designed and maintained for high availability and to meet the requirements of the users.

Purpose:

To establish adequate controls, for protecting information transmitted to and from ADF environment, and proper security controls to safeguard IT equipment.

Scope:

This policy shall be applicable to all the IT equipment at ADF. Network components like Routers, firewalls, switches, servers, desktops and laptops shall be configured to meet the security requirements.

Responsibilities:

All users

Policy Statement:

Adequate network security controls shall be implemented to:

"Protect **ADF's** information transmitted, stored and processed on the network from unauthorized disclosure, modification or destruction".

"Protect the supporting network infrastructure of **ADF**"

Network Management

- This section aims at measures used to build up a secure network architecture
- Although most of the network controls are implemented and managed by vendors, this document lays down the requirements from ADF.

Network Design

Following guidelines shall be followed for network services:

- The servers shall be implemented for single primary function, wherever possible. This shall simplify configuration, thereby reducing the risk of errors in configuration. In some cases, it may be appropriate to offer more than one service on a single host computer (e.g. database, DNS, ftp and http services). All servers are on premises and protected from infiltration and malicious damages including its data from natural perils.

- Any unused or unwanted network devices and services shall be removed or disabled. Non-working devices shall be removed from the network once replaced with working ones.

- If the business requires any services or ports to be enabled, they shall be enabled only after proper authorization and testing to avoid misuse.

Network Component Security

- All network components shall be identified and access shall be restricted to authorized personnel.
- Inventory of all network components shall be maintained.
- All premises hosting communication equipment such as Servers, Switches, Firewalls, ISP Routers, CCTV, Etc, shall be secured from unauthorized physical access. The access control may be in the form of:
    - Manned by Security Guards
    - Access control systems like Card readers and Keypad locks

Wireless Access

- Access to Wireless LAN across **ADF** shall be over encrypted channel using stronger encryption methods.
- It shall be ensured that wireless access points are secured properly.
- SSID (Service Set Identifier) of the wireless network shall be unique.

Network Segregation

- Proper segregation of network access shall be defined.
- Firewall shall be configured for IPS and IDS policies to monitor the traffic flowing in from external networks.

Change control

- Any change to the network architecture connectivity shall be authorized by Manager/Head IT.
- Modifications to access control lists on the network devices shall be authorized by Manager/Head IT.

Documentation

- Network documents are considered as sensitive information and shall only be made available to the authorized individuals only on a need-to-know basis.
- A detailed network architecture diagram shall be maintained.

Enforced Path

- Specific ports of business applications and systems shall be allocated/whitelisted
- Access restrictions shall be placed on perimeter devices like routers, firewall, etc.
- Based on need for network segregation, logical domains/Virtual LANs (VLAN) shall be created
- The segregation shall be as per business requirements
- Command line access to systems shall be limited to the authorized people only

Redundancy

- Adequate redundancy shall be built-in to the network links
- Redundant links shall have the same level of security as the primary links

Clock Synchronization

- Time synchronization, by means of NTP (Network Time Protocol) on Domain server, shall be implemented for all computing systems across ADF, thereby enabling audit trails with accurate date-time stamp.

Network Devices

This section aims at measures to build up a secure network by adopting best practices in managing network devices.

General

- All default passwords to network devices and various IT components for administrative purpose shall be changed as per password policy.
- All network components shall be configured with strong authentication/password.
- All network devices that transmit information over the network shall be configured properly so as to protect information from getting leaked, hacked or intercepted.
- All systems and software shall have latest OEM supplied patched / updates installed.
- It shall be ensured that Antivirus software is active on all the systems.

Enforcement:

All those employees found to have violated this Policy shall be subjected to disciplinary action, up to and including termination of employment/contract and/or financial penalties.

****