BASELINING PROCEDURE DOCUMENT

Keynote Financials Services Ltd.

KEYNOTE

Author:	MD(Designation)
Owner:	MD(Name)
Organization:	_________ (Company name)
Version No:	1.0
Date:	(Date)

Document Control

Document Title **Baselining Procedure 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)	Base-lining Procedure Document	(Date)	1.0

Distribution

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

BASELINE PROCEDURE DOCUMENT

PURPOSE OF POLICY

Company assets should be hardened and configured securely. Systems should be configured with reference to CIS or NIST benchmarks. This document will cover assets like Windows, Linux and other devices.

SCOPE OF POLICY

This policy applies to:

- All the company assets like Servers, Desktop, Network Devices in the organization.

BASE LINING PROCESS – WIDOWS SYSTEMS

- Software Installation
  - KFSL maintains list of approved software.
  - New software installation should follow appropriate change management process along with all necessary business approvals.
  - System Administrator should review installed software on all desktop, laptops and servers at frequency of 6 months.
  - All unnecessary software should be removed from desktops, laptops and servers.
- Disable or Remove Unnecessary User-names
  - Default user accounts should be disabled.
  - If default user account is required to be used, user-name should be renamed.
  - Only necessary user should be part of Administrator group
- Strong Password Policy
  - Strong password policy should be followed for all user accounts:
    - Enforce Password History – 5 Passwords
    - Maximum Password Age – 60 Days
    - Minimum Password Age – 2 Days
    - Minimum Password Length – 8 Characters
    - Password must require complexity – Enabled
    - Account Lockout Threshold – 5 Invalid Attempts

- Disable or Remove Unnecessary Services
    - System Administrator should review all the services running on desktops, laptops and servers at frequency of 6 months.
    - All unnecessary services should be removed from desktops, laptops and servers
    - Run all services with low privilege user
- Install Security Patches
    - Install latest service pack for the server
    - Install all security patches regularly
        - Critical Risk Patch – within week
        - High Risk Patch – within month
        - Medium Risk Patch – within quarter
        - Low Risk Patch – within half year
- Install Anti-Virus and Anti-Malware
    - Install approved anti-virus on the desktop, laptops and servers.
    - Install all latest plugins and signatures released by anti-virus company.
- Auditing & Logging
    - Configure server with correct time zone settings.
    - Ensure that server is synchronized with centralized NTP server.
    - Ensure auditing is enabled and audit logs are pushed to centralized log server.
    - Configure strong permissions on log files
    - Configure Audit Logs as mentioned below:
        - Audit Account Logins Event – Success & Failure
        - Audit Logan Event – Success & Failure
        - Audit Policy Change – Success & Failure
        - Audit Privilege Use – Success & Failure
        - Audit Account Management – Failure
        - Audit Object Access – Failure
        - Audit Process Tracking – Failure
        - Audit System Event – Failure

- User Management
  - Shudo privilege should be given to limited users only
- System Access Management
  - Insecure services like telnet, ftp, rlogin, rsh, etc. should be disabled
  - Use secure remote administration protocols like SSH for server console access
  - Disable remote login for root user
- Strong password policy should be enforced
  - Pass Min Length – 8 Characters
  - Pass Max Days – 45 Days
  - Pass Min Days – 7 Days
  - Pass Warn – 14 Days
- Auditing & Logging
  - Enable auditing for all critical activities like user authentication, package installation, user addition, etc.
  - Configure strong permissions on log files
  - Server time should be synchronized with Centralized NTP server
  - Backup should be scheduled for all critical data with centralized log server
- Secure Permissions
  - Configure secure permissions on critical system files like password, shadow and group
  - Configure strong permissions on Cron and AT services to schedule jobs
  - U mask should be configured to 022
- Install Security Patches
  - Install all security patches regularly
    - Critical Risk Patch – within week
    - High Risk Patch – within month
    - Medium Risk Patch – within quarter
    - Low Risk Patch – within half year

BASE LINING POLICY STATEMENTS

- Only software that has been approved for use by the IT department may be installed on the organization's computing devices.
- Non-essential software applications and services will be uninstalled or disabled.
- Servers, desktops and laptops will be configured to prevent the execution of unauthorized software.
- Vulnerability scanning and inventory scanning software will be configured to automatically uninstall unauthorized software.
    - BIOS passwords will be implemented on all desktops and laptops to protect against unauthorized changes.
- The boot order of desktops and laptops will be configured to prevent unauthorized booting from alternative media.
- All desktops and laptops will be built from a standard image. Any change to the standard image must be supported by a business case.
- Access to the local administrator account will be restricted to members of IT Department to prevent the installation of unauthorized software and the modification of security software and controls.
- Default passwords will be changed following installation and before use in a production environment.
- All desktops and servers will be protected by anti-virus and anti-spy-ware software. The anti-virus and anti-spy-ware software will be configured to automatically download the latest threat databases.
- The use of removable media will be controlled. Removable media will be controlled by endpoint protection software.
- The headers on web servers and email servers will be changed.
- All server & new application must pass a vulnerability assessment prior to use. All network and operating system vulnerabilities will be rectified prior to use.