System Management and Administration

Policy Statement

The system administrators of Jubilee Life Insurance are responsible for the installation of OS in servers and user-end systems across the organization. The configuration of the OS should be such that they are enabled to generate logs of activities. System clocks should be synchronized throughout the organization to investigate and backtrack a particular activity. Moreover, only the company-approved software products should be installed into the systems.

Objective

The Policy is to outline the responsibilities and guidelines for all individuals who function as system administrators.

Prerequisite

This Policy should be read in conjunction with:

- Information Security Policies, including
- Communications Security

Responsibility

- Group Head Digital, Technology and Strategic Planning
- System Administrators

Procedure

Step	Description	Responsibility
Clock Synchronization		
1.	On a quarterly basis system clock of the central server shall be checked to ensure it is accurate.	System Administrator
2.	System clocks of all the machines shall be synchronized with the clock of central server automatically when the client machines log on to the central server. User shall not have rights to modify system time.	System Administrator
Installation of Server end OS		
1.	System administrator shall provide OS software that shall be approved before installation. The System administrator is responsible for all server aspects of installation of the systems, nobody shall install or modify software on a server without the approval of the authorized person. Specialized software like CRM, Cognos will be installed by specific vendors with approval of system administrators.	System Administrator
2.	All the default passwords of the system supplied accounts present in the Operating system shall be changed, and all unnecessary default accounts shall be disabled. Administrator account should be locked and renamed as "Mahtab" for secure admin login.	System Administrator
3.	A separate ID with privileges shall be created for use. System supplied or "Administrator" & "root" equivalent access accounts shall not be used for day to day operations.	System Administrator
4.	The server shall be joined with the JLI's domain, where applicable.	System Administrator
Installation of User end OS		
1.	The Helpdesk Support Staff is responsible for all aspects of installation of the OS and software on end user's PC. All end users shall be barred from administrative controls. Admin roles can be provided for some specialized task for limited time after approval from Group Head Digital Technology and Strategic Planning	Helpdesk Staff
2.	All the default passwords of the system supplied accounts present in the Operating system shall be changed, and all unnecessary default accounts shall be disabled.	Helpdesk Staff
3.	The prepared system shall be joined with the JLI's domain before providing to end users	Helpdesk Staff/System Administrator
Configuration of Servers		
1.	Auditing shall be enabled for all sensitive and security related events. Moreover, key events like Failed Login and Successful Logins and sensitive file/folder access related events will be logged at a minimum on all servers and reviewed periodically	System Administrator

2.	Un-necessary OS services shall be stopped. Template for JLI security baseline should be used for windows/Linux server.	System Administrator
3.	Configuration shall be created having all OS template baselines settings. This template shall be updated upon configuration changes in baseline setting	System Administrator
Operation		
1.	A list shall be maintained of access rights of the authorized OS Local users. This list shall be updated whenever required.	System Administrator
2.	List of approved software should be maintained for Server's and end users PC. Approved software list is part of IT Approved SOP.	System Administrator / Helpdesk
Monitoring		
1.	OS related logs (Event Logs) shall be reviewed for any suspicious activity. Any anomaly noted shall be reported to Group Head Digital, Technology and Strategic Planning. Logs review mechanism should be established, and logs will be reviewed as per the established mechanism periodically.	System Administrator
2.	Logs of privileged user IDs (System Administrator/ root/ Administrator) shall be reviewed as stated in user access management policy.	Team Lead System Administration