9. Logical Access Management

Policy Statement

The logical access within the infrastructure of Jubilee Life Insurance Company should be controlled and it should emphasize the job related need of the individual. The access to the information assets should be approved and should be granted to facilitate the business.

Objective

The objective of this document is to establish security requirements for access to the information resources of JLI. Effective implementation of this Policy will streamline the process of access management and minimize unauthorized access to JLI's proprietary information systems.

Scope

- Operating Systems
- Databases
- Applications
- Network Systems

Prerequisite

This procedure should be read in conjunction with:

- Information Security Policies
- Access Control Policy

Responsibility

- Group Head Digital, Technology and Strategic Planning
- Team Lead/Unit Head / Head of Department (Business Head)
- System, Application, Database and Network Administrators
- HR
- Users

Policy

Logical Access Grant for New Employee

Ste	Description	Responsibility
1.	After Employee Number creation of User from HR, relevant manager of User shall file a request user at the SFR / RMS Portal for granting access to various systems. The request shall at a minimum, include the following: • Access Rights Required for each application(s) • Necessary comments to justify the requested rights.	Unit Head/Team Lead/User
2.	All Logical Access Requests shall be approved by respective Unit Head / Head of Department via RMS/SFR or any other documented means.	Unit Head/ Business Head
3.	Only approved request to be forwarded to IT Department via RMS/SFR portal	System enforced via Helpdesk
4.	All Access requests shall be assigned to System / Application / Database / Network Administrators and should be documented.	System enforced via Helpdesk System / Application / Database / Network Administrator
5.	The User-ID along with requested rights shall be created on the requested application(s) The User Shall be notified with required login-credentials as per the procedure defined in IT SOPs	System / Application / Database / Network Administrator / User
6.	After obtaining the formal endorsement from the User, the request shall be closed in the RMS/SFR Portal with appropriate comments.	System / Application / Database / Network Administrator / User

Logical Access modification

Ste	Description	Responsibility
1.	User shall file a request at RMS/SFR portal. The modification for access rights request shall at a minimum but not limited to, include the following: • Access Rights Required/To be Modified (Add or Remove) for each application(s) • Necessary comments to justify the requested rights.	User
2.	All Logical Access Requests for Access Rights Modifications shall be approved by respective Unit Head / Head of Department.	Unit Head/ Head of Department// Business Head
3.	Only approved request to be forwarded to IT Department.	System enforced via Helpdesk
4.	All Access rights modification requests shall be assigned to System / Application / Database / Network Administrator in the RMS/SFR request.	Application / System / Database / Network Administrator
5.	User-ID along with requested rights shall be updated/modified.	System / Application / Database / Network Administrator / User
6.	After obtaining the formal endorsement from the User the request shall be closed in the RMS /SFR	System / Application / Database / Network Administrator / User

Logical Access Revocation

Ste	Description	Responsibilit
Exit of Employees		
1.	IT Department shall be informed of terminated employee. IT should be intimated as soon as the Last Date of Employment is recorded in HR Management System by HR.	HR/Helpdesk
2.	After the Last Date of Employment, relevant Administrators shall revoke access from all JLI applications and systems as per user exit process and update the same in the system.	Application Administrator/ Network Administrator/ Database Administrator
3.	Exit employee's user deletion should be maintained in the centralized system.	Application Administrator/ Network Administrator/ Database Administrator
4.	HR Department will be intimated in case of non-recovery of any IT assets assigned to terminate employee.	Technical Assistance
5.	If an account stays in active for 90 consecutive days, it should be disabled.	Application Administrator/ Network Administrator/ Database Administrator
Transferred Employees		
1.	IT Department shall be informed of transferred employee. As soon the employee's transfer Date of Employment is recorded in HR Management System.	HR
2.	Employee transferred status shall be updated in the system, respective administrators to revoke access from all JLI business applications except AD and Email.	Application Administrator/ Network Administrator/ Database Administrator

3.	Logical access modification process (as defined above) will be initiated for new access rights of the transferred employee	IT Department

Account Unlocking

Step	Description	Responsibility
1.	In case user account is locked out, User need to contact respective administrator and the account can be unlocked as per access control policy protocols.	User/Application /DB/ System/ Administrator
2.	Respective administrator will change the password whenever required.	Application Administrator/ Network Administrator/Database Administrator
3.	Password shall be changed at first logon.	User

Access Rights and Logs Review

Ste	Description	Responsibility
Privileged Ids		
1.	Logs of privileged ID's e.g. root, sys, system and generic ID with admin roles etc shall be generated and reviewed as per IS Policy.	Database Administrator/ Application Administrator/ Network Administrator
2.	Logs to be reviewed for any suspicious activities and review results to be retained for Audit purpose. Investigation to be carried out in case suspicious activities detected.	Respective Team Leads

Privileged Users		
1.	Logs of privileged users e.g. DBA, Application Administrator , system administrators etc., shall be generated and reviewed as per IS policy.	Database Administrator/ Application Administrator/ Network Administrator
2.	Logs to be reviewed for any suspicious activities and review results to be retained. Investigation to be carried out in case suspicious activities detected.	Respective Team Leads