	Version 1.00	Effective Date: Oct 01, 2018	Information Technology Policies & Procedures
	Section: Organizing and monitoring IT		Page 1 of 3

# Physical Access Management

## Policy Statement

Jubilee Life Insurance Company should establish processes to physically protect the IT assets from unauthorized access. No one, other than the authorized and approved individuals should be able to access the sensitive areas. Access of vendors, auditors and any other person should be approved and an authorized person should escort their visit.

## Objective

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


## Prerequisite

This procedure should be read in conjunction with:

- Information Security Policies
- Access Control Policy

## Responsibility

- Group Head Digital, Technology and Strategic Planning
- Data Centre Owner
- IT Technical Staff/NOC Staff

	Version 1.00	Effective Date: Oct 01, 2018	Information Technology Policies & Procedures
	Section: Organizing and monitoring IT		Page 2 of 3

## Procedure


A designated in charge of Data Centre shall be nominated from IT Team. The Data Centre Owner shall be responsible for managing Physical Access requirements to Data Centre.

### Third party / Vendor Access to Server Room / Data Centre

Step	Description	Responsibility
1.	In case vendor visit is required, access request to be forwarded to Data Center In charge for Approval	Data Centre Owner
2.	Vendor to fill 3 <sup>rd</sup> party Vendor visit log book. Details to be recorded.	NOC Staff
3.	Vendor to be supervised throughout his stay at Data Centre.	NOC Staff
4.	3 <sup>rd</sup> party log book to be reviewed	Data Centre Owner

### IT Personnel Access other than designated Personnel to Server Room / Data Centre

Step	Description	Responsibility
1.	Request for authorization of permanent access to server room, along with an explanation to be sent to Group Head Digital, Technology and Strategic Planning.	Group Head Digital, Technology and Strategic Planning
2.	Temporary access shall be granted by Data Center Owner after the evaluation of the request. This may include IT employees (part time and/or full time) who do not have direct responsibility for the maintenance and repair of equipment housed in the Data Center	Data Centre Owner

	Version 1.00	Effective Date: Oct 01, 2018	Information Technology Policies & Procedures
	Section: Organizing and monitoring IT		Page 3 of 3

3.	Request shall be approved or rejected for permanent or temporary access. Outcome to be documented by Data Center Owner	Data Center Owner
4.	After approval, an access card (RFID) will be assigned to the IT staff seeking permanent access to the Datacenter.	Data Center Owner
5.	In case request is approved, Access to be granted to requestor. List of approved users with access to Data Centre to be updated	Data Center Owner
6.	In case of temporary access of an IT personnel Log sheet should be updated for the visit.	Data Center Owner

## Physical Access Revocation

Step	Description	Responsibility
1.	In case of termination/resignation of IT Staff, or change in responsibilities, access to server room / data Centre shall be revoked.	Data Center Owner
2.	The outgoing IT Staff's access card (RFID) to be formally collected and signoffs to be acquired for the return of card on employee clearance.	Data Center Owner
3.	Approved list of users to be updated and reviewed periodically	Data Center Owner