Backup, Restoration and Retention Policy

Objective

To meet the enterprise business objectives and ensure continuity of its operations, JLI shall adopt and follow well-defined and time-tested plans and procedures, to ensure timely and reliable backup of its IT assets. The Backup Policy reiterates the commitment of JLI towards delivering the fastest transition and highest quality of services through the backup arrangement ensuring that its customers, business activities and services do not suffer in any way.

The data backup covers all systems managed by the Technology department. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with IT.

All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data must be stored on the network/departmental drives provided.

Prerequisite

This Policy should be read in conjunction with:

Information Security Policies, including:

- Communications Security
- Operation Security
- Physical and Environmental Security

Responsibility

- Group Head Technology and Project Management
- System Administrator
- Database Administrator
- Network Administrator
- Application Administrators
- Fileserver Administrator
- Designated IT staff

Backups

- JLI will take the backups through different mechanisms for daily, weekly, and monthly backups.
- Daily, weekly, and monthly backups of the Core Applications schedule will be stopped, and manual backup would be processed to cater month-end closings.
- Daily backups are retained for 7 days i.e., day 1 of week X backup expires at 11:59 PM of same day next week.
- Full backups are performed weekly. Full backups are retained for 4/5 weeks depending upon the number of weeks in current month i.e., week X of Month 1 backup expires on Week X of Month 2 (retention: ~1 Month) before being overwritten.
- Monthly backups of the machines are spread over full month and are retained for ~1 Year, i.e., Backup of Month 1 will be expired on last day of 12th Month.
- Backups should be executed after office hours and are completed before 8:00 AM on official working days.
- Upon completion of backups, media copies should be moved from backup locations to designated onsite and offsite according to scheduled interval define in IT SOP.
- Backups are stored in secure locations. A limited number of authorized personnel have access to the backup application and media copies.
- Backup of the data held within Database Systems have data backup routines which ensure database integrity is retained.

The following outlines Backup Software support – including policy configuration, restores, backups:

- It is the responsibility of the JLI Infrastructure team to make sure backups are running as scheduled.
- The team will verify that backup jobs have been completed successfully and will inform the business/Application owner if problems occur.
- When a new server is added to the production environment, the owner of server / application will connect with Infrastructure team to have the server added to the backup system for daily, weekly, or monthly scheduled or on demand backups.
- It is the responsibility of Infrastructure team to install updates/upgrades of the backup software in the servers.

Restoration

- Restoration is done on the request of service owners mentioned in IT SOP.
- Physical or logical data restoration is done by loading the desired media into the library and initiating the restore process from master backup server.
- User data retention is weekly and restored on user's request with appropriate approval.
- Acceptance of data request is subject to availability of data according to its retention period.
- Restoration of File & Folder backup is always performed on separate location, it is the requester's responsibility to analyze restored data and overwrite the existing if needed.
- Restoration of VMWare level backup always performed after deletion of existing virtual machine.
- As part of Backup SOP, the Infrastructure team will test the restoration of core business system backups on a quarterly basis and preserve the available logs.
- Infrastructure team will not entertain such restoration request where data files moved/delete by data owner without any intimation to infrastructure team, in that case backup copy does not contain the requested data.
- In order to restore the files, the user must submit a request to the IT department, which, in case of critical restoration, shall be authorized by head of the relevant department. Request should contain the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

Backup Retention

The time lapse between when a backup is created and when it is formatted to be destroyed or potentially reused. This can be considered the 'shelf-life' for the backup and is how long the backup will be kept before the images are expired. Backups will be saved onto magnetic tapes, or disks or cloud (Currently under JLI Services).

The backup retention policy covers the infrastructure and procedures that are provided for organizational data backup and recovery. It is the responsibility of the application owners to determine the backup schedule, recovery point objective, and retention per application. Although they may seek guidance from the Jubilee Life Infrastructure team, it is the responsibility of the Application Owners to manage the data retention for their application(s). This policy does not cover data retention for compliance or legal purposes.

Following are the backup retention frequency:

1. Daily Backups:
    a. File and folders backup will be kept on backup tape/disks for 7 days.
    b. Incremental and full backups will be moved to designated places daily after backup completion.
    c. Occurs at scheduled 4 to 6 iterations per week.
    d. Daily tagged tapes will be reused as the daily backup expires after 7 days if they are viable.
2. Weekly Backups:
    a. Full and incremental weekly backups will be moved to designated places after backup completion.

    b. Occur as scheduled; 4 / 5 iterations per month (depends upon the weekend days per month)
    c. Tapes may be reused as they expire if they are still viable.
    d. Retained for 4/5 weeks (depending on the number of weeks in a month)
3. Monthly Backup
    a. Full VMs and file & folder backup will be kept on designated backup tapes for 1 year.
    b. Occurs as scheduled; 12 iterations per year.
    c. Tapes may be reused as they expire if they are viable.
    d. Duplicate copy of core business application's monthly backup will be stored securely off-site as defined in the IT SOP.
    e. Retained for ~1 Year and backup expires on 1st day of 12th month.
4. Special Backup Requests (i.e., litigation, system upgrades, retirements etc.)
    a. Special backup requirements should be initiated by business/application owners with all the relevant approvals.
    b. Special backup requests must contain the time and reason for retention.
    c. New tape/disk procurement may be required to fulfil the request.
    d. Full backups may be sent off-site upon request.
    e. Copies may be set up for up to 6 months, 1 year or for lifetime retention as per the request from business/application owner.