|  |
| --- |
| GENUS INNOVATION LIMITED |
| Backup Procedure |
| PRCD\_BACKUP |
|  |
| **Genus** |

|  |
| --- |
| This procedure defines the Backup and Restoration process to protect the organization’s Intellectual Property. |

Contents

[Overview 2](#_Toc424373769)

[Objective 2](#_Toc424373770)

[Scope 2](#_Toc424373771)

[Inputs 2](#_Toc424373772)

[Entry Criteria/Triggers 2](#_Toc424373773)

[Tasks 2](#_Toc424373774)

[Verification 4](#_Toc424373775)

[Guidelines 4](#_Toc424373776)

[Definitions 4](#_Toc424373777)

[Data Backup 4](#_Toc424373778)

[Data Archival 4](#_Toc424373779)

[Data Restoration 4](#_Toc424373780)

[Timing 4](#_Toc424373781)

[Storage 4](#_Toc424373782)

[Tape Drive Cleaning 4](#_Toc424373783)

[Age of tapes 5](#_Toc424373784)

[Subversion Backups and Live Replication 5](#_Toc424373785)

[Responsibility 5](#_Toc424373786)

[Data Backed Up 5](#_Toc424373787)

[Tape Storage Locations 5](#_Toc424373788)

[Magnetic Tape 5](#_Toc424373789)

[Exit Criteria/Outputs 6](#_Toc424373790)

# Overview

This procedure defines the Backup and Restoration process to protect the organization’s Intellectual Property.

# Objective

The purpose of this procedure is to define backups and restoration activities in Genus so that they are capable of effective data security. This also protects the data in the event of an equipment failure, sabotage, or disaster.

# Scope

This process is applicable to all activities under the purview of the R & D Division in Genus.

# Inputs

* All Work products

# Entry Criteria/Triggers

* Periodicity
* The practitioners have undergone QMS trainings with focus on performing their processes.

# Tasks

| Sr. No | Task | Owner/Role |
| --- | --- | --- |
|  | **Prepare Backup Plan** |  |
|  | Prepare the backup plan using “Backup and Restoration Plan” template ( TMPL\_BKPPLN) which includes:   * The backup server where backups will be stored * The programs or tools to be used for backups * Groups of users whose backups are to be taken * Periodicity of the backups * Periodicity of testing restoration of backups and archived content * The offsite location where the backups will be archived * The programs or tools to be used for Data Recovery/Restoration | Configuration Administrator |
|  | **Review and Approval of Backup Plan** |  |
|  | Get the Backup Plan reviewed and approved by the Design Head. | Configuration Administrator |
|  | **Data Backup and Restoration** |  |
|  | Configure the workstations of identified users for automatic data backup. | Configuration Administrator |
|  | Ensure that backups are being taken as per defined schedule. | Configuration Administrator |
|  | Ensure that backups can be restored successfully. | Configuration Administrator |
|  | **Data Archival** |  |
|  | Prepare for data archival. | Configuration Administrator |
|  | Archive the backup at the offsite location defined in backup plan | Configuration Administrator |
|  | **Testing Restoration of archived data** |  |
|  | Restore a sample of data from the archived media. | Configuration Administrator |
|  | Verify that the content can be restored successfully. | Configuration Administrator |
|  | Update the Backup plan with the findings. | Configuration Administrator |
|  | **Data restoration** |  |
|  | Users that need files restored must submit a request to the designated personnel. Include information about 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. This information needs to be sent by Email. | Users |
|  | The latest backups are used to restore the file/files. The data is verified with respect to the file properties and contents specified by the user | Configuration Administrator |

\* Improvements/Suggestions are solicited on “Process Improvement Proposals Database”.   
\*For details on the Roles and Responsibilities of the practitioners, Refer "Roles and Responsibility" document in the QMS.

# Verification

* Verification of data backup plan by Design Head
* Verification of the restored data
* The backup activities are subject to audit in line with “IT Infrastructure Audit checklist” (CHKL\_ITAUDT).

# Guidelines

Refer "Configuration Management and Release Procedure" (PRCD\_CONFIG) for Access Rights, location of work products, naming convention and types of controls.

## Definitions

### Data Backup

Data Backup is the saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data.

### Data Archival

Data Archival is the saving permanent storage media such as magnetic tapes, Hard disk, DVD.

### Data Restoration

Data Restoration is the retrieval of Backed up data for active use.

## Timing

Full backups are performed regularly. The periodicity of the Backups is fortnightly.

Storage  
There shall be a separate set of Backup media for each year full data.   
At least one month backup data must be preserved and other media can be rotated and used for taking further backup.

Tape Drive Cleaning  
Tape drives shall be cleaned quarterly.

## Age of tapes

The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than two years shall be discarded and replaced with new tapes.

### Subversion Backups and Live Replication

* Create a repository at the backup location.
* Create a “pre revision property change” hook file in the repository, which may return success only. i.e. the contents of the batch file may only be “exit 0”
* Initialize svnsync with the destination(created in step 1 above) and the source repository(the repository which needs to be backed up) paths using “svnsync init <dest> <source>
* Create a backup script with the command line “svnsync sync <dest>” and schedule the same to run with desired periodicity. The destination repository will be an exact image of the source repository at this point.

Refer “Repository Replication” section in “Repository Administration” chapter of the official “[Subversion Book](http://svnbook.red-bean.com/)” for more details.

## Responsibility

The Design Head shall delegate a member to perform regular backups. The delegated person shall test backups and the ability to restore data from backups on a quarterly basis.

Data Backed Up  
Data to be backed up include the following:

* User’s important data
* Source Codes
* PCB Design
* Mechanical Design
* IDEs
* Databases
* Project Data
* SharePoint

Tape Storage Locations  
Fortnightly tapes shall be stored in a fireproof and secured safe.

### Magnetic Tape

* Number of tapes required for taking Firmware, Software, PCB Design data fortnightly
* Number of tapes required for taking Mechanical Data fortnightly

At least 3 sets are required for one year.

# Exit Criteria/Outputs

* Verified Backups