North Shore Technologies

Back Up Policy

Revision History

Ver.	Date	Description of Change	Authored / Revised By	Reviewed By	Approved By
0.1	25th Feb, 2009	Draft	Abhishek Rautela	Ausaf	Sudhir Saxena
1.0	30th Feb, 2009	Initial Version	Abhishek Rautela	Ausaf	Sudhir Saxena
2.0	12th Oct 2009	Updated the tasks section. Mentioned that the backup would be taken on the tape drives.	Abhishek Rautela	Ausaf	Sudhir Saxena
2.1	19th May, 2010	Reviewed	Abhishek Rautela	Ausaf	Sudhir Saxena
2.2	5th Jan, 2011	Reviewed and Formatting	Abhishek Rautela	Ausaf	Sudhir Saxena
3.0	22nd Aug, 2011	Update section 2 & 5	Abhishek Rautela	Ausaf	Dhananjay
3.1	21st May 2012	Storage Device	Ajeet Singh	Saket Madan	Dhananjay
3.2	10th March 2014	Update section 3 & 4	Saket Madan	Dhananjay Kumar	Ajay Kumar Zalpuri
3.4	12th July 2017	Update section 2 for back up policy and retention period	Ajeet Singh Jitendra Singh	Saket Madan	Dhananjay
3.5	12th Sep 2019	Update section 4.1 & 4.3 for Backup and restore.	Ajeet Singh/ Jitendra Singh	Saket Madan	Ajay Kumar Zalpuri
3.6	15th Nov 2019	Update section 4.5for General Rules for Retention Periods.	Ajeet Singh	Saket Madan	Ajay Kumar Zalpuri

Table of Content

1. Purpose

NST recognizes that the importance of the timely backup and restore. The regular backups and restore is not only important from project point of view but is also useful for organizational growth and productivity. Therefore, this backup and restore policy highlights the areas that are in scope of the backup and restore. The purpose of this policy is as follow:

- To safeguard the information assets of NST
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

2. Scope of Backup Policy

In Scope:

- Domain Controller- Weekly on external drive located in server room.
- Azure Machines -Daily Image Backup retention up to 3 days. GRS (Geo Redundant storage) Policy applied.
- TFS Server- Daily full backup of MS SQL Database on external drive located in server room retention up to 7 days.
- Account (Tally, FAMS and Paypac) Daily back up on external drive located in server room started from 2015 and will continue.
- Account (User Backup) – Weekly Back up of Desktop data (Key User) on external drive located in server room retention up to 30 days.
- Camera- DVR Internal storage backup up to last 30 days.
- Data of department heads- User using One drive mechanism.
- DB backup of SAP machine- Daily full backup of MS SQL Database on one drive retention up to 7 days.
- Attendance system - Weekly full backup of MS SQL Database on external drive located in server room retention up to 7 days. COSEC retain its own transaction backup up to 30 days.
- Firewall- Daily configuration backup on external drive as well as one drive located in server room retention up to 30 days.

3. Responsibility

Infrastructure team: The infrastructure team is responsible for carrying out regular backups and restore

Stakeholders: The relevant project/support team will verify the restore data at first time and as and when restoring is required.

4. Backup & Restoration

NST would be liable for the backup mentioned in the Scope of the policy. The frequency of the backup is on daily incremental and weekly full basis.

4.1 Backup:

- Azure - backup of machines snapshots retention is 3 days
- Azure - MS SQL database backup retention is 7 days
- In case of finance backup, one copy is available on external mass storage and second copy is available on one drive
- Backup Media (External Mass storage) shall be stored safely to protect them against theft and unauthorized access. Weekly critical backup stored on One drive.

4.2 Data Recovery:

- In the event of a catastrophic system failure, off-site backed up data will be made available to users as and when required.
- In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

4.3 Restore:

Backups will be verified periodically

- The backup media is regularly tested to ensure the reliability of backup information. SVAM IT team configured Backup alert policy for every 2 hours in Azure via email for MS SQL.
- Azure daily full back up in every 24 hours and send alert in case of any failure.
- The demo restore is performed half yearly to verify that backups have been successful.
- In the event of accidental deletion or corruption of information, requests for restoration of information will be made to SVAM IT Team.
- On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:
    - To check for and correct errors.
    - To monitor the duration of the backup job.
    - To optimize backup performance where possible.

- IT will identify problems and take corrective action to reduce any risks associated with failed backups.
- IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

4.4 Access Level of Backups:

- Only IT head and 2 members of IT team have access to backup and restore

4.5 General Rules for Retention Periods:

Differential or Incremental backups will be performed daily. Daily backups will be retained for a weeks. Daily backup media will be reused once this period ends.

Item	Retention Period
E-mails created or received during official business and which are kept as evidence of the NST functions, activities, and transactions.	Records may not be disposed of unless written authorization have been obtained from the Management
Primary evidentiary records, including copies of forms issued for value, vouchers to support payments made, pay sheets, vouchers or cheques, invoices and similar records associated with the receipt or payment of money.	5 Years
Records relating to assets no longer held or liabilities that have been discharged.	5 Years
A record of any third party to whom the information was disclosed must be kept for as long as the information is used.	As long as the information is used and at least 3 year thereafter.
All personal data which has become obsolete.	Destroy
Employees Records	Records may not be disposed of unless written authorization have been obtained from the Management