Backup and Recovery Policy for Third Parties

As at
Nov 2023

Backup Policy for Third Parties

Introduction and Purpose

The purpose of this policy is to define the need for performing periodic computer system backups to ensure that mission-critical, data, applications, users' data, and archives are adequately preserved and protected against data loss and destruction. All third parties responsible for providing and operating mission-critical applications must document and perform system specific data backup or at least minimal data backup periodically.

Policy Application

This is a Group-wide policy of BNK Banking Corporation Limited ("BNK Group" or "the Group") applicable to:

- All 3rd parties holding BNK data.
- Material 3rd parties only

Policy Requirements

- Backups of all BNK data and software must be retained such that computer operating systems, applications and data are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.

- The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.

- At least three versions must be maintained.

- At a minimum, one fully recoverable version must be stored in a secure, off-site location. An off-site location may be in a secure space in a separate building, or with an off-site storage.

- Derived data should be backed up only if restoration is more efficient than creation in the event of failure.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.

- Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data centre disaster scenario, if applicable.
- Backup and recovery documentation must be updated whenever there is a change to technology, business change, or migration of applications to alternative platforms.

- Recovery procedures must be tested on an annual basis.

Types of Backups

BNK Group categorises backup approaches and frequency of backups depending on the criticality of the service and data. Backups can be created daily, weekly, or monthly basis. The table below defines the different types of backups to be followed across the group and by all 3rd parties.

Critical & Important Suppliers/ Systems (where applicable)

Types of Backups	Description	Appropriate Use
Full Backup	A full backup creates a copy of every file on a storage device	Annual (verified) backup. Monthly backup Weekly Backup Daily Backup
Incremental Backup	An incremental backup is a backup type that only copies data that has been changed or created since the previous backup activity was conducted. An incremental backup approach is used when the amount of data that must be protected is too voluminous to do a full backup of that data every day.	Weekly Backup Daily Backup
Data Replication	This is the process of sharing information to ensure consistency between redundant resources such as software or hardware components to improve reliability,	Real- Time

	fault tolerance or accessibility.	
Transaction Log Backup	A transaction log backup creates copies of only those records (in some cases before and after images of records) on a storage device that are changed since the last backup. It requires a version of the application program to run all of the transactions since the last full backup.	Daily Backup

Minimal Backup Policy

The following minimum backup policies apply to critical and important systems.

Type of Data	Minimal Backup Policy	Backup Recovery Test Frequency
System Software	Latest Version plus patches, at least weekly	Annual (verified) backup.
Application Software	Latest version plus patches at least weekly	Annual (verified) backup
System Data	Daily	Annual (verified) backup
Application Data (e.g., Core banking data)	Daily with real-time transaction files	Annual (verified) backup

Monitoring, Escalation and Reporting

Monitoring*:* All 3rd parties are expected to monitor all backups and ensure that a successful backup has been completed after each procedure.

Escalation: In the event of a backup failure 3rd parties must report the failure and remediation results to BNK within 24 hours via the BNK IT Manager, Head of IT Governance, or the CIO.

Reporting: All 3rd parties must provide backup, recovery, or remediation reports (where applicable) monthly as part of operational service level performance reporting.

Right to Audit

All 3rd parties should, given reasonable notice provide BNK, its nominee or any regulator access to monitor or audit Backup and Recovery records and their compliance to this policy. It is expected that 3rd parties must give assistance, reasonably requested by BNK to facilitate the monitoring or audit of the backup and recovery processes.

Roles, Responsibilities & Accountabilities

Third Party/Suppliers

- Perform backup and recoveries as stipulated in this policy.
- Provide backup reports monthly and recovery test reports on an annual basis to BNK Group.
- Report incidents/failures to BNK associated with backup and restore testing of the systems/data they are responsible for and manage.

Policy Compliance

This policy shall take effect upon publication. Compliance is expected with all material 3rd parties who provide services to BNK.

Exceptions

- If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support services provided to BNK Group, 3rd parties shall request an exception through BNK Chief Information Officer (CIO).
- All exceptions must be recorded in the BNK risk register.

Breach of Policy

Consequences: Any Critical 3rd party found to have violated this policy may be subject to damages, specific performance, or contract cancellation and restitution within the framework of the relevant vendor contracts.

Backup Policy for Third Parties

Definitions

Backup Policy:	A backup policy clarifies specific procedures, policies, and responsibilities, including a well-defined schedule for performing backups, ensuring a more stable process.
Recovery:	A return to a normal state of health.
Replication:	The action or process of reproducing or duplicating.
System Data:	Data that is always kept in the system files.

Material Revisions

Version No.	Approval Date	Effective Date	Nature/Purpose of Review/Details of Amendment	Reviewer(s)
2.0	24/11/2023	22/11/2023	NFRC Review update	NFRC
1.0	Nov 23	Nov 2023	New Document	CIO IT Manager Head of IT Gov & Security