



বিষয় : Backup and Restore Guidelines

সার্ভার/কম্পিউটারের হার্ড ড্রাইভে সংরক্ষিত ব্যাংকের বিভিন্ন রকম ব্যবসায়িক ও দাপ্তরিক তথ্য ও উপাত্তসমূহ যেকোন মুহূর্তে নষ্ট বা অকার্যকর হয়ে যেতে পারে বিধায় তা বিধি মোতাবেক যথাযথভাবে নির্দিষ্ট সময়ব্যাপী সংরক্ষণ করা অত্যন্ত জরুরী। এছাড়াও বৈদ্যুতিক গোলযোগ বা Bad Sector সৃষ্টির কারণেও সার্ভার/কম্পিউটারের হার্ড ড্রাইভ নষ্ট হয়ে যাওয়ার সম্ভাবনা থাকে।

পাশাপাশি প্রতিনিয়ত বিভিন্ন ম্যালওয়্যার/ভাইরাস দ্বারা কম্পিউটার/সার্ভার আক্রান্ত হয়ে সকল ডাটা বিনষ্ট বা Encrypted হয়ে যায় যা অধিকাংশ ক্ষেত্রেই পুনরুদ্ধার করা যায় না। তাই ব্যাংকের প্রয়োজনীয় ব্যবসায়িক ও দাপ্তরিক ডাটাগুলো কম্পিউটার হার্ড ড্রাইভ এ সংরক্ষণ এর পাশাপাশি যথাযথ মিডিয়ায় Backup গ্রহণ পূর্বক সংরক্ষণ করতে হবে এবং সময়ে সময়ে পরীক্ষণ পূর্বক তথ্য ও উপাত্তসমূহের Confidentiality, Integrity, and Availability (CIA) নিশ্চিত করতে হবে।

০২। বর্ণিত বিষয়টি বিবেচনা করে ব্যাংকের বিভিন্ন রকম ব্যবসায়িক ও দাপ্তরিক তথ্য ও উপাত্তসমূহের Backup & Restore Guidelines প্রণয়ন করা হয়েছে। Backup & Restore এর গাইডলাইন নিম্নে উল্লেখ করা হলোঃ

Backup and Restore Guidelines

1.0 Purpose

The purpose of this policy is to maintain the integrity and availability of information, processing and communication services. This Policy is to ensure that necessary controls are in place to protect data in the event of a hardware failure, accidental deletion or unauthorized changes or block level corruption. It also to ensure that backup copies are created at defined intervals and regularly tested.

2.0 Reference documents

Guideline on ICT Security For Banks and Non-Bank Financial Institutions (May, 2015 Version 3.0) which is issued by Bangladesh Bank.

3.0 Goals

The main goals of this guideline are:

- To define and apply a clear backup and restore standard for all corporate information systems.
- To define backup and recovery standards per data prioritization.
- 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 secure backup and restoration processes and the media employed in the process.
- To set the retention periods of information contained within system level backups designed for recoverability and provide a point-in-time snapshot of information as it existed during the time-period defined by system backup policies.

৩

৪

4.0 Principle

The following principles direct this policy:

- Performing proper backup, storage, and handling of data is necessary for all departments to achieve their objectives.
- Staff must accurately follow the policy and protect the availability, confidentiality, and integrity of data.

5.0 Backup Media

Backups must be stored in SAN (Storage Area Network), NAS (Network Attached-Storage), Tape Drives, HDD, Removable Disks, CD, DVD and any other media approved media. Tape drives are automated and require a third party backup application or backup capabilities in the operating system which is valid for DC & DRS.

6.0 Backup environments

A critical component of any data backup and recovery initiatives is to properly identify all environments and the associated data that required backup procedures. This would include, but not limited to, the following platforms and supporting systems:

- Network device backups, such as configuration file, rule sets, and other critical data.
- Servers, (both virtual and physical stand-alone) such as all operating systems, and associated applications (i.e., databases, web server applications, etc.) for all Microsoft Windows, UNIX, Linux, and any other type of other operating systems.
- Database servers, Application servers, Process servers, ATM Interface servers, SMS servers, Internet Banking servers, DNS servers, email servers, FTP servers, AD servers and all other systems associated servers.
- External system resources are those owned, operated, maintained, and controlled by any entity other than BKB, but for which these very resources may impact the confidentiality, integrity, and availability (CIA) of BKB system resources and supporting assets.

Data custodians are responsible for providing adequate backups and restores to ensure the recovery of data and systems in the event of failure. Backup provisions allow business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of bank data backups and restores need to be maintained.

7.0 Backup Methods

Backup process is run on a regular scheduled time, complete with reporting metrics and other critical information.

9

R

8.0 Types of Backups and Default Backup Scheduling

Backup activities for full, differential, and incremental are to take place on an as-needed basis, such as in the following manner:

- Full: At a minimum, once a week.
- Differential: At a minimum, daily.
- Incremental: As necessary.

8.1. Backup frequency

The department should maintain the following backup frequency schedule:

- Core Production
 - ◆ Real time data replication from Data Center (DC) to Disaster Recovery Site (DRS).
 - ◆ Scheduled DB transaction log backup
 - ◆ Day end backup
 - ◆ Weekly Full backup
 - ◆ Monthly Full backup
 - ◆ Half year Full backup
 - ◆ Year end Full back up
- Application Software/ Utility Software
 - ◆ Latest Version with patches
 - ◆ Full backup
- System Software
 - ◆ Latest Version with patches
 - ◆ Full backup
- Configuration Files
 - ◆ Full backup
 - ◆ Relevant backup initiated by configuration changes.
- Internal services and data
 - ◆ Weekly Full backup
 - ◆ Daily Incremental backup
- Document File
 - ◆ Daily backup
 - ◆ Monthly backup

8.2 Backup Retention Periods

Sl	Particulars	Retention Periods
01.	Day end backup	Daily backups will be retained for a week before being overwritten.
02.	Weekly Full backup	Weekly full backups will be retained for a week before being overwritten.
03.	Monthly Full backup	Monthly full backups are kept for 12 months on disk storage before being overwritten.
04.	Half year end full back up	Half year end full backups are kept for 24 months on disk storage before being overwritten.

SI	Particulars	Retention Periods
05.	Year end Full back up	Yearend backups must be preserved as per storage media life.
06.	Application Software/ System Software/ Utility Software	Backups will be overwritten when latest version has been implemented and patch updated.
07.	Network/ Security Device Configuration	Latest configuration file backups must be stored properly as per change frequency.
08.	Document File	Daily backup will be kept in PC/Server and Monthly backup will be retained for a week before being overwritten.

9.0 Backup Exceptions (As required)

Any exceptions to the types of backups and the default backup scheduling are to be approved by authorized personnel, with a valid and justified reason. Additionally, such exceptions – which are ultimately changes to the backup process are to be submitted with a formal change request, reviewed and approved by authorized personnel. Furthermore, changes to any of the tools and utilities used for the backup process also require the use of a documented change request, initiated by select personnel only. The backup platform is a critical component of the organization’s information technology infrastructure, thus great care and due diligence must be enacted when involving changes to its process.

10.0 Backup Reporting Metrics

Backup reporting activities, for all types of backups (i.e., Full, Differential, Incremental, etc.) are to be monitored on a regular basis for ensuring the success of the backup process itself. Specifically, all backups conducted are to generate reporting metrics for which authorized personnel are to review in a timely manner. Such reporting metrics include, but are not limited to, the following:

- E-mails confirming the current status and final result – such as success or failure of the backup.
- Reports generated confirming the current status and final result – such as success or failure of the backup.
- Portals for which authorized employees can log into for reviewing and confirming the current status and final result such as success or failure of the backup.
-

Backups that are successful are to be recorded as such, yet backup failures exceptions are to be handled immediately, with all appropriate steps undertaken for ensuring the timely backup of such data.

Failures and exceptions are delivered via email reports or metrics from the backup utilities notifying authorized employees of such issues. Depending on the nature, severity, and urgency of the backup itself and the resolution for correcting the issue, a thorough and analysis is to be undertaken for correcting the issue in a timely manner and for helping mitigate the issue in the future.

R

9

Backup Reporting Metrics Format

SL No	Content	Date	Backup Type	Backup taken by			Backup review by			Remarks
				Name	Designation	Signature	Name	Designation	Signature	
1	2	3	4	5	6	7	8	9	10	11

11.0 Backup Storage and Security

Appropriate security measures are to be implemented for backups, which includes all necessary physical security controls, such as those related to the safety and security of the actual backup media – specifically – disks, tapes, and any other medium containing backup data. This requires the use of a computer room or other designated area (facility) that is secured and monitored at all times and whereby only authorized personnel have physical access to the backups. Thus, "secured" and "monitored" implies that the facility has in place the following physical security and environmental security controls:

- Constructed in a manner allowing for adequate protection of backups.
- The use of cages, cabinets, or other designated, secured areas for securing backups.
- Access control mechanisms consisting of traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e. iris, palm, fingerprint scanners/readers). Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are retained as per Bangladesh Bank Guidelines.
- Adequate closed-circuit monitoring, video surveillance as needed, both internally and externally, with all video kept as per Bangladesh Bank Guidelines days for purposes of meeting security best practices and various regulatory requirements.
- Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.
- Appropriate power protection devices for ensuring a continued, balanced load of power to the facility for where the backups reside.

11.1 Backup Storage Designated Area

Backup storage designated area are given below:

Backup Particulars	Type	Storage Area/Location
DC/DRS	Onsite	One copy of all types of backup will be preserved in DC/DRS.
	Offsite	One copy of all types of backup will be preserved in offsite location.
Head Office Department /Controlling Office/ Online Branch	Onsite	One copy of all types of backup will be preserved in respective office.
	Offsite	One copy of software backup will be preserved in offsite location (Other Department/ Divisional Office/Regional Office/ Nearest Branch.
Offline Branch	Onsite	One copy of all types of backup will be preserved in respective Branch.
	Offsite	One copy of all types of backup will be preserved in offsite location (Divisional Office/Regional Office/ Nearest Branch.

12.0 Media Management and Quality Control

All backup media is to be clearly labeled, logged accordingly, and rotated as necessary for ensuring all retention periods are adhered to, while also utilizing existing mediums (i.e., tapes, disks, etc.) for writing over and copying as necessary for future backups. Additionally, media management practices for backups also required that strict policies be in place for transporting media to and from the off-site approved facility being used by BKB. As such, an authorized list is to be kept that includes only select personnel allowed to transport and recall media, with no exceptions.

Either in manual form or electronic format, the following information is to be recorded regarding backups:

- Name and unique identifying number of backup medium.
- Contents of the backup
- Data classification of backup
- Location of where it is being stored
- Origination of backup – where the medium initially came from.

If backups are being transported, the following is to be recorded:

- Purpose
- Name of individual requesting backup
- Intended destination
- Date of release
- Date of return
- Any other information deemed relevant

As for quality control initiatives, backups are to be used until they reach a point far before in which the quality of the data may come into question, ultimately to avoid media failures. At any time, if the quality of media becomes an issue, the data is to be immediately removed to another medium, with the compromised medium being disposed in accordance with company policy.

13.0 Transporting of Media

Transporting backup media is vital for ensuring its safety and security at all times during movement. The following best practices are to be adhered to at all times, when applicable:

- Backup media is to be properly packed and stored for ensuring its safety during movement, which means using approved cases and other protective devices.
- Backup media is to be kept away from extreme temperatures, both heat and cold, during movement.
- Backup media is never to be left alone or unsupervised during transportation.
- Only approved transport methods and vehicles are to be utilized.
- Transport is to be in a direct manner as possible, with no unnecessary stops or deviations from the intended route.
- When necessary, transport of media is to also include additional security precautions as required.

14.0 Backup Requests and Retrieval

Backups are to be available in a timely manner for any such requests for restoration. Such requests require written approval by authorized personnel detailing the request, along with all applicable information as necessary. A change request is to be opened for such requests, and approved by authorized personnel. As for the restore process, it is to be conducted by authorized personnel who will test for ensuring a complete restoration was achieved, along with conducting any user-acceptance and system testing. Lastly, the restore media is to be promptly returned to the physically secured area for safe storage.

15.0 Backup Recovery Abilities

On a regular basis, such as quarterly, and no less than twice a year, authorized personnel are to examine the back media health checkup, and report on the ability to effectively restore and recover data in the event of such a request. This required examining the facility for which data is being stored for ensuring its overall safety and security. Furthermore, all backup mediums, such as tapes, disks, and other supporting hardware and software utilities, are to be examined for ensuring proper function. Such information and all relevant findings are to be reported upstream to management, with recommendations for improving upon or correcting any issues or concerns.

16.0 Business Continuity and Disaster Recovery Planning (BCDR)

Documented Business Continuity and Disaster Recovery Planning (BCDRP) are vital to protecting all BKB assets along with ensuring rapid resumption of critical services in a timely manner. Because disasters and business interruptions are extremely difficult to predict, it is the responsibility of authorized BKB personnel to have in place a fully functioning BCDRP process, and one that also includes specific policies, procedures, and supporting initiatives relating to the safety and security of backups, and supporting systems for which to restore backup data on.

17.0 Continuous Monitoring of Backup Environment

It's also vitally important to undertake continuous monitoring practices over the entire backup environment for ensuring its confidentiality, integrity, and availability (CIA). As such, authorized personnel are to ensure the following:

- All applicable environments requiring backups have been readily identified.
- The backup types (full, differential, and incremental) along with the default backups scheduling, is commensurate with the needs of BKB.
- Backup results are being sent to, reviewed, and assessed by authorized personnel.
- All backup infrastructure both hardware and software related are performing and function as expected, with no exceptions or deviations regarding performance, accuracy, and other critical measures deemed relevant. Infrastructure, includes, but is not limited to, the following:
 - Backup software
 - Backup hardware
 - Tapes
 - Tape and library drives
 - Other storage and connectivity apparatus

18.0 Backup Retention Periods and Disposal Procedures

All backup tapes are recycled back into use except year end backups. If the backup media does not work properly, backup media must be destroyed. Please note that prior to physically destroying any of the actual devices used for storing data, all data must be electronically removed (i.e., wiped, formatted, etc.) as the primary layer of security before being destroyed.

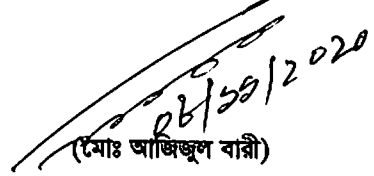
০৩। এছাড়াও Backup & Restore এর ক্ষেত্রে বাংলাদেশ ব্যাংক কর্তৃক জারিকৃত “ Guidelines on ICT Security for Banks and Non Financial Institutions, 2015 ” বিষয়ক পলিসি, বাংলাদেশ কৃষি ব্যাংক কর্তৃক জারিকৃত “ICT Security Policy” ও সময়ে সময়ে জারিকৃত আইসিটি পরিপত্রসহ অন্যান্য নির্দেশনাসমূহ অনুসরণ করতে হবে।

০৪। ব্যাংকের অভ্যন্তর মূল্যবান বিভিন্ন রকম ফিন্যান্সিয়াল ও দাপ্তরিক ডাটাগুলো আপদকালীন সময়ে প্রাপ্তির নিশ্চয়তা এবং তথ্যের Confidentiality, Integrity, and Availability (CIA) নিশ্চিত করার জন্য বিধি মেতাবেক Backup গ্রহণ ও সংরক্ষণ নিশ্চিত করার জন্য বর্ণিত Backup & Restore Guidelines পরিপালন করার জন্য নির্দেশনা প্রদান করা হলো।

০৫। এ আদেশ অবিলম্বে কার্যকর হবে।

অনুমোদনক্রমে-

আপনার বিশ্বস্ত

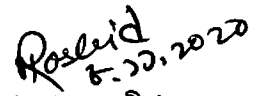

(মোঃ আজিজুল বারী)
মহাব্যবস্থাপক (প্রশাসন)
আইসিটি মহাবিভাগের দায়িত্বে

প্রকা/ আইসিটি (সিস্টেমস)/গাইডলাইনস-১৩(১)/২০২০-২০২১/১৩৭৯

তারিখঃ ০৮/১১/২০২০

সদয় অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য অনুলিপি :

- ০১। চীফ স্টাফ অফিসার, ব্যবস্থাপনা পরিচালক মহোদয়ের সচিবালয়, বিকেবি, প্রকা, ঢাকা।
- ০২। স্টাফ অফিসার, উপব্যবস্থাপনা পরিচালক-১, ২ ও ৩ মহোদয়ের সচিবালয়, বিকেবি, প্রকা, ঢাকা।
- ০৩। স্টাফ অফিসার, সকল মহাব্যবস্থাপক মহোদয়ের দপ্তর, বাংলাদেশ কৃষি ব্যাংক, প্রধান কার্যালয়, ঢাকা।
- ০৪। স্টাফ অফিসার, মহাব্যবস্থাপক মহোদয়ের দপ্তর, সকল বিভাগীয় কার্যালয় ও স্থানীয় মুখ্য কার্যালয়, বাংলাদেশ কৃষি ব্যাংক।
- ০৫। অধ্যক্ষ, স্টাফ কলেজ, বাংলাদেশ কৃষি ব্যাংক।
- ০৬। উপ-মহাব্যবস্থাপক, সকল বিভাগ, বিকেবি, প্রকা, ঢাকা।
- ০৭। বিভাগীয় নিরীক্ষা কর্মকর্তা, সকল বিভাগীয় নিরীক্ষা কার্যালয়, বাংলাদেশ কৃষি ব্যাংক।
- ০৮। মুখ্য আঞ্চলিক/আঞ্চলিক ব্যবস্থাপক, সকল মুখ্য আঞ্চলিক/আঞ্চলিক কার্যালয়, বাংলাদেশ কৃষি ব্যাংক।
- ০৯। সকল আঞ্চলিক নিরীক্ষা কর্মকর্তা, বাংলাদেশ কৃষি ব্যাংক।
- ১০। ব্যবস্থাপক, সকল শাখা, বাংলাদেশ কৃষি ব্যাংক।
- ১১। নথি/মহানথি।


(মোঃ মাসুম রশীদ)
উপ-মহাব্যবস্থাপক