GOVERNMENT OF WEST BENGAL
DEPARTMENT OF INFORMATION TECHNOLOGY AND ELECTRONICS
MONIBHANDAR (5TH& 6TH FLOOR), WEBEL COMPLEX, BLOCK- EP & GP
SECTOR- V, SALT LAKE, KOLKATA- 700091
Phone:2357-2533, Fax: 2357-2534, E-mail: secit@wb.gov.in

No. 588-Estt/ITE-20012/2/2020 Date: 28/12/2020

Subject: **West Bengal State Electronic Data Centre Storage Sharing and Electronic Data Retention Guidelines, 2020.**

Ref: This Office Notification vide No 584-Estt/ITE-20012/2/2020 dated 28.12.2020.

The State Government in the Department of Information Technology & Electronics has issued Notification under reference to formulate 'West Bengal State Broadband Policy 2020' wherein the instant ORDER features as Annexure D.

ORDER

The Governor is pleased hereby to make the following guidelinesin order to bring clarity, simplification and standardization in the process of electronic data storage, data sharing and data retention after the primary objective of electronic data processing has been achieved. West Bengal is poised to promote transparency in electronic Data Protection measures by bringing in a set of guidelines that ensures that electronic data storage, data sharing and data retention is undertaken in a legal, transparent and secure manner.

The Government of West Bengal is poised to promote transparency in allocation, augmentation & reclamation of storage space and implementation of proper Information Security Management System (ISMS) through a set of guidelines that ensures all data would be protected and applications to be hosted under safe & securer environment in State Data Centre.

Through these guidelines, the Government of West Bengal (GoWB) in the Department of Information Technology & Electronics, would be able to ensure that Government departments and organisations along with their parastatals, subsidiaries, corporations, statutory authorities including associated agencies –public and private organizations abide by laid down guidelines as enumerated below.

1. Short title, extent and commencement

a) The guidelines may be called the **"West Bengal StateElectronic Data Centre Storage Sharing and Electronic DataRetention Guidelines, 2020"**
b) It shall extend to the whole of the State of West Bengal
c) It shall come into force with effect from the date of issue.

2. Definition

Data is the new oil to drive the economic growth. The state governments who are cognizant of the rise of data economy, will feature in the list of the successful states in terms of stability, investment, employment generation, smart public service delivery, overall growth and prosperity. Data is a set of values of subjects with respect to qualitative or quantitative variables. Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized. When data is processed, organized, structured or presented in a given context so as to make it useful, it is called information. Information, necessary for research activities are achieved in different forms. The main forms of the information available are[1]:

- **Primary data**: Primary data is an original and unique data, which is directly collected by the researcher from a source according to his requirements.
- **Secondary data**: Secondary data refers to the data which has already been collected for a certain purpose and documented somewhere else.
- **Cross-sectional data**: Cross-sectional data is a type of data collected by observing many subjects (such as individuals, firms, countries, or regions) at the same point of time, or without regard to differences in time.

[1] https://microbenotes.com/data-and-its-types/

Dept. of Information Technology & Electronics * Govt. of W. B. *

- **Categorical data**: Categorical variables represent types of data which may be divided into groups. Examples of categorical variables are race, sex, age group, and educational level. It is qualitative in nature.
- **Time series data**: Time series data is a collection of quantities that are assembled over even intervals in time and ordered chronologically. Example: temperature, weight or population data.
- **Spatial data**: It is also known as geospatial data or geographic information it is the data or information that identifies the geographic location of features and boundaries on Earth, such as natural or constructed features, oceans, and more. Spatial data is usually stored as coordinates and topology and is data that can be mapped. Spatial data is used in geographical information systems (GIS) and other geolocation or positioning services.
- **Ordered data**: Data according to ordered categories is called as ordered data. Ordered data is similar to a categorical variable except that there is a clear ordering of the variables. For example, for category economic status ordered data may be, low, medium and high.

West Bengal State Data Centre (WBSDC) - WBSDC was established under National e-Governance Plan (NeGP) (presently known as Digital India) and to ensure shared, reliable and secure infrastructure services centre for hosting and managing the e-Governance Applications of State and its constituent departments. Several critical applications including citizen centric applications were hosted in the State Data Centre. With the increase in demand for hosting environment it is imperative to develop certain guidelines for effective utilization of storage space and implementation of Information Security Management System (ISMS) under WBSDC environment.

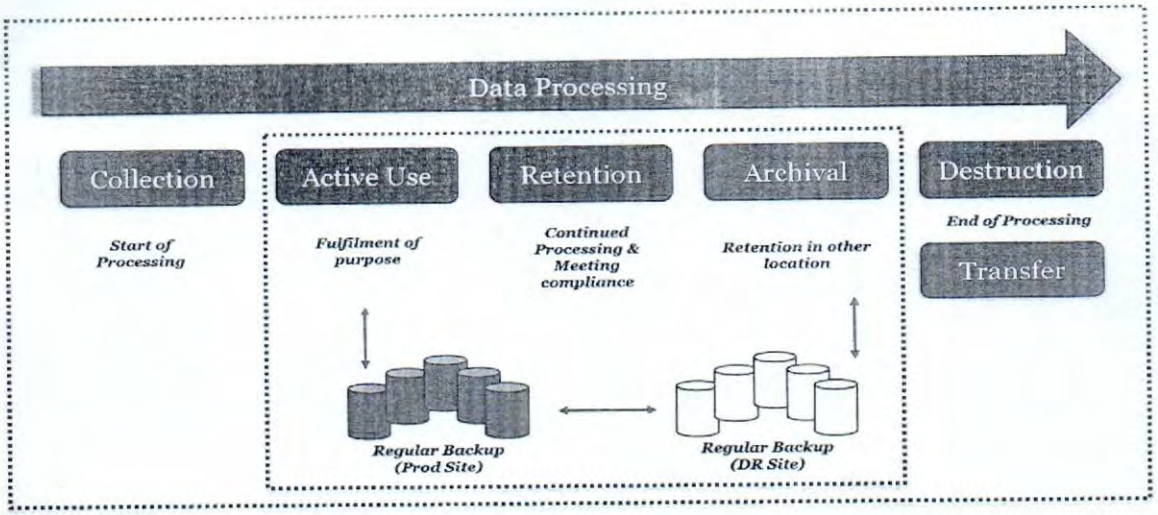
For Government application and processes, most of the data is being processed at various levels viz. National Informatics Centre, State Data Centre (SDC), Local Data centres (Department specific) for achieving better public service delivery and participative governance. In accordance to the MeitY guidelines, focussing on the State Data Centre (SDC) and its importance of data retention plan, the Government of West Bengal has decided to lay down through a set of state electronic data guidelines which are majorly categorised into six (7) verticals:

A. Electronic Data Storage
B. Electronic Data Classification
C. Electronic Data Sharing in *anonymous* format
D. Electronic Data Retention
E. Electronic Data Security
F. Electronic Data Disposal or archival
G. Electronic Data Allocation & reclamation of storage space at State Data Centre (SDC)

In terms of government services catering to public needs, huge amount of electronic data is being consumed and processed everyday by both Government organizations and private entities. In most of the instances, a substantial volume of data is being retained in form of electronic records even after the primary objective of data processing is fulfilled. While data retention is necessary for future business/ Departmental needs or statutory/ regulatory requirements, it is also important that the electronic form of data storage, data sharing and data retention are done in an authentic and secure way. A proper standard is required to be in place to avoid data breach and reduce unnecessary storage consumption.

Note: Electronic Data – *Documents in electronic form comprising various types viz. *.doc, *.odt, *.txt, *.pdf et al; Emails, Multimedia and the likes are considered as Electronic Data. Individuals and the organization that create / process/ share/ store the electronic data are responsible to ensure that the data is stored in appropriate location, and in classified format.*

Dte. of Information Technology & Electronics * Govt. of W. B. *



3. Goals & Objectives

All state electronic data needs be securely stored, backed-up, archived and disposed in a consistent manner in regard to its criticality, sensitivity, present & future requirements in line with the industry best practices. Data classification is a key component for making consistent and appropriate decisions related to secure data storage and retention. Primary objectives revolve around electronic data storage, anonymous data sharing and data retention guidelines are listed below-

- To optimise electronic data storage space and cost at State Data Centre (WBSDC)
- To bring in transparency and make the Departments aware of their roles, responsibilities in management of SDC
- To host citizen centric data under safe & secure environment
- Effective management of risk with an understanding of possible threats and the risk of security exposure within DataCenter
- To set out limit for electronic data retention period
- To identify critical electronic data and finalize type and volume of data to be retained and for what purpose
- To maintain transparency in electronic data processing in Government processes
- To meet regulatory compliances
- To ensure that electronic data is deleted / scrapped after the agreed retention period is over
- To monitor and enhance the performance of scheduled backups

4. Applicability of the Guidelines

The guidelinesare applicable to all the Government departments and organisations along with their parastatals, subsidiaries, corporations, statutory authorities including associated agencies – public and private organizations having server and storage location in West Bengal storing public data. All employees working in the above-mentioned organizations, will directly fall under the ambit of the electronic Data Retention Guidelines and hence abide by them. All electronic records that are created, handled, stored, processed, anonymously shared by any of the above organizations in form for business and operations shall also come under the ambit of West Bengal Electronic Data Sharing and Retention Guidelines, 2020.

The guidelines enlisted herein will also be applicable for those organisations who desire to avail the services from WBSDC.Any user may deploy their existing or new application except Top Secret & Secret applications (data or information that can cause serious threat/ damage to the security of the state/ country or compromising the National interest). All applications before hosting need to obtain Safe to Host certificate from CERT-In empanelled security auditor. The scope of these guidelines includes but not limited to the ease of allocation, management and effective usage of resources as well as protection of assets and services delivered by WBSDC.

5. Implementation framework

Following Public Information Infrastructure will collaborate to achieve the end goals and objectives of these guidelines:

A. Electronic DataStorage: The electronic data is being stored at various level:

a. **National Informatics Centre (NIC):** Under Ministry of Electronics and Information Technology (MeitY) in the Indian government, supports the national level initiatives and provides infrastructure to help support the delivery of government IT services and the delivery of some of the initiatives of Digital India. As per the drafted Personal Data Protection Act, the data principal (data owner), data fiduciary and data processor strictly confined to the Central government. The electronic data is consumed, processed, stored and maintained by the central government.

b. **State Data Centre:** Under the state government, provides infrastructure support and electronic data management including electronic data generated in any form, stored, processed and maintained by the state government authorities. All employees both permanent and contractual are strictly not allowed to use the official system for their personal needs.

c. **Local Data Centres***(storing government/ public data)*: These includes the data centres which are facilitating respective state/s with a third-party engagement programs in delivering public benefits. The electronic data stored, processed and maintained by state or local authorised bodies. All employees both permanent and contractual are strictly not allowed to use the official system for their personal needs (*storing of personal data*).

d. **Government Departments**: They are inclusive of Directorates, Municipalities, District, Sub-division and Block level Government units, Gram Panchayats and other local self-government bodies in any form that are connected to activities of electronic data consumption, processing and maintenance for public benefits. All employees both permanent and contractual are strictly not allowed to use the official system for their personal needs.

e. **End point systems existing in government** (*in any form*): The system owner or data owner may be responsible for all the electronic data stored, processed and maintained in system or application. The administrator will be responsible for proper data management, network management and providing access control rights to restrict misuse of data. The onus also lies on the departmental heads for overall electronic data management. All employees both permanent and contractual are strictly not allowed to use of the official systems for their personal needs (*storing of personal data).* The storing of unofficial or personal content (*in any form*) in public systems is strictly prohibited. The department or the system issuing authority will not be liable for any type of personal data loss in case of personal data is kept in the system (*issued by the governing body*) but the authorised system owner will be liable for ensuring data privacy (*of the official data*) even if it is stored by the official in one's personal system with or without prior approval of the Head of the Office. Government shall not be liable for safe-keeping of data kept in personal system of any official.

B. Electronic Data Classification: Data can be classified in two ways – (a) mode or format of data &(b) criticality of data

a. Based on the mode or format of data, data, which comes under the ambit of the retention guidelines, they can further be classified as follows -

i. **Electronic Data** – Documents, Emails, Multimedia are considered as Electronic Data. Individuals and the organization that create / process/ share the electronic data are responsible to ensure that the data is stored in appropriate location, format, classified format.

ii. **Electronic Data for Business Applications** – Other type of electronic data includes the business application records which are generally required for business analysis purpose and can be required to be temporarily stored. These type of data needs special attention and must be erased after primary objective is fulfilled and data retention period is over.

iii. **Physical Records converted into Digital format** – The Government of West Bengal is the front runner in adopting and promoting digitization through various single window systems. The government is encouraging all the state departments and their respective subsidiaries to migrate from the paper-based work culture to digital impressions. There are the still few physical / printed copies of documents that are created out of day to day operations and business obligations. These documents are very critical to the security of respective departments and its subsidiaries or entities

and must be handled with utmost care. The Department is taken measure to convert the physical files into digital ones.

Note: *The West Bengal State Data Centre Storage Sharing and Electronic Data Retention Guidelines, 2020 is strictly targeted towards the electronicmedium of data (for Government use) which is stored, processed, retained or archived within the geographical boundaries of the state.*

b. Based on the criticality of data, *ElectronicData* can be classified in the following manner. Data retention period primarily depends upon the critical nature of the data.
   i. **Confidential Data:** This classification applies to allinformation generated and shared within and/ or across various state departments, its subsidiaries orentities. Its unauthorized disclosure could adversely impact its business, its stakeholders, its business partners, its employees and/or its customers.
   ii. **Internal Data:** This classification applies to information that is specifically meant for employees of a department, its subsidiaries or entities. While its unauthorized or unintended disclosure is against the prescribed guidelines, it is not expected to seriously or adversely impact the governmental processes, business, employees, customers, stakeholders and/ or business partners.
   iii. **Public Data:** This classification applies to information, which has been explicitly approved by the government/ Department/ management for release to the public.
   iv. Restricted Data: Highly confidential, there should be a separate provision of restricted data:
      - ➔ Data classified as Restricted and Protected or Confidential will be stored only in approved locations; viz. State Data Centre and/or on approved equipment or storage facilities notified by the Government as and when applicable.
      - ➔ Nodal officers, to be duly notified by the Government, shall have the authorisation to make duplicate copies or shadow files of the such classified data.
      - ➔ Standards for storing electronic data containing sensitive data shall be formulated, notified and periodically reviewed.
      - ➔ Standards for copying/ printing of hardcopy containing sensitive data shall be formulated, notified and periodically reviewed.
      - ➔ Periodic reviews shall be performed by Third Parry Security Assurance Agency to ensure compliance with datamanagement policies, standards and procedures.

C. Electronic Data Sharing in anonymous format

Data collaboratives is an emerging form of partnership in which participants exchange data for the public good, have huge potential to benefit society and improve decision making. But they must be designed responsibly and take data-privacy concerns into account. The state departments generate tons of cross sectoral data which may reap direct benefits for the State-level Start-ups, MSMEs, public service delivery organisation, state departments, its subsidiaries or entities, data collaboratives et al. These data-sets when utilised properly, can drive decision making, improve situational and causal analysis. The unique collections of data will help government decision makers to better understand issues such as traffic problems, healthcare, transportation or financial inequality and design more agile and focused evidence-based policies to address them. AI will be at the centre of twenty-first-century governance, its output is only as good as the underlying models. And the sophistication and accuracy of the models generally depend on the quality, depth, complexity, and diversity of data underpinning them. Data collaboratives can thus play a vital role in building better AI models by breaking down silos and aggregating data from new and alternative sources. Moreover, such data exchanges enhance decision-makers' predictive capacity. The anonymised data sharing will deliver benefit to Public service delivery providers by:

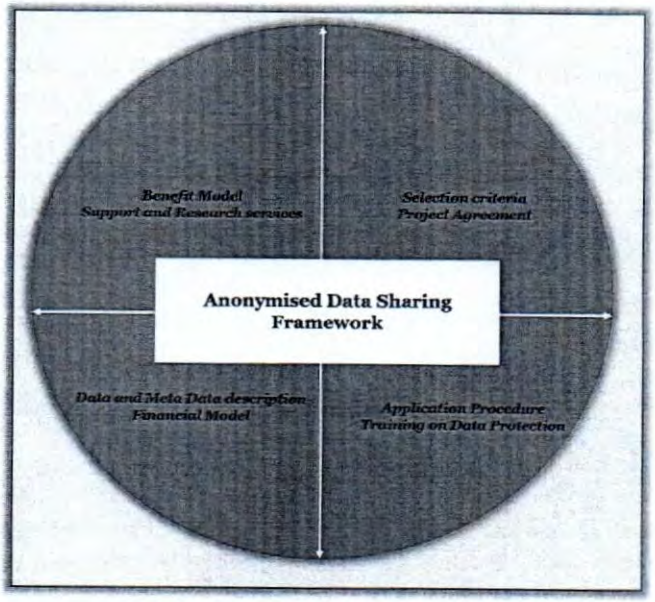
a. Reduce duplication and wastage
b. Better target front service delivery
c. Monitoring demand and delivery pattern
d. Improving level of customer satisfaction
e. Facilitating evidence-based policy and decision making
f. Identifying root cause of the problems/ challenges
g. Predicting user service needs

h. Increasing public trust in government and Public functions
i. Enabling research

To seek the above listed benefits, the shared data (*anonymised format- to add data protection and prevent data breaches*) should reach the right recipients viz. Start-up or Developer community, MSMEs, state decision makers, public service delivery organisation and NGOs; State Government in the Dept of IT&E has laid down West Bengal Transactional Data Sharing Guidelines, 2020.

The data sharing system is designed based on the below parameters; the details will be communicated as an when required:

1. Selection Criteria
2. Project Agreement
3. Application procedure
4. Training on data Protection
5. Data and Meta Data description
6. Financial and Benefit Model
7. Support and Research services



Anonymised Public Transactional Data Sharing Framework

Special emphasis has to be made so that all security pre-requisites are adhered to by those Start-Ups before they are offered, counselled and allowed to host their applications on this C-IaaS.

D. Electronic Data Retention: RTI Act does not require the public authority to retain records for indefinite period; Information needs to be retained as per the record retention schedule. Various types of data viz. business/ personal/ public data are processed for different purposes and are of different critical level – hence, retention periods also vary on case to case basis. Retention of electronic data has to be reviewed periodically to check the status of objective of retaining the data. While finalizing a retention period, the following factors are to be kept in mind –

a. Type of electronic data in consideration
b. Purpose of electronic data retention
c. Legality of the department/ organizations for collecting, processing and retaining the data under consideration

In certain instances, criteria shall be established by which the retention period of the data can be determined, thereby ensuring that the data storage and retention can be regularly reviewed against those criteria. Data must be deleted/ destroyed after pre-defined retention period is over.

In limited exceptional circumstances, Data (business/ personal) can be retained for a longer period where such retention is for archiving purposes and are in the public interest, for scientific or historical

research purposes, or for statistical purposes. All such retention will be subject to the proper data security measures at technical and organisational level and the Secretary of the concerned administrative department shall expressly notify such extension stating clearly the need for exceptional retention.

Beyond the identified time period for normal retention, the owner of the data shall have to take a copy of the said data from the 'in-system – the application/location that includes Data Centre & Disaster Recovery (DR) site' into a physical tape or otherwise, as to be decided by the owner under notification, and preserve it for archival period of retention.

Note: *Before any transactional data is archived into the physical tapes or drives, data must be made anonymised and shared with the state public data sharing system for facilitating the state government, start-ups, MSMEs for helping state to grow based on analysis in form of measuring trends, training data for their application or systems, research and development.*

Based on international standard practices, Data Retention period for different types of data will be as follows:

CATEGORY	RETENTION PERIOD (in system – the application/ location where primary use of the data was held i.e. Data Centre & DR site)	TOTAL RETENTION PERIOD (including archival)
Medical Records	3 years	25 years (inclusive of the 3 years) or based on applicable regulations
HR Records	3 years	25 years (inclusive of the 3 years) or based on applicable regulations
Medical & Security Assistance Case Record	2 years	3 years (inclusive of the 2 years)
Call Recordings	1 year	2 year
Audit logs	3 months	2 year
Corporate Secretariat Record	Life of the entity	Life of the entity + 50 years
Accounting & Financial Records	2 years	7 years or based on applicable regulations
Procurement & Contract Record	Contract Duration	Contract Duration + 7 years or based on applicable regulations
Travel Tracker Records	2 years or based on contractual commitments	3 years or based on contractual commitments
Other Records	2 years or based on applicable regulations	2 years or based on applicable regulations

Explanation: In order to check whether a candidate has attempted before in an entrance examination, the data of that candidate after his first attempt, is required to be kept only until his age crosses the upper limit or the maximum number of attempts that one is allowed. Later, the electronic data is securely encrypted and transferred to a physical tape to optimise data centre storage cost.

E. **Electronic Data Security**: After the primary objective is fulfilled, data can be retained for a longer period for business/ regulatory purpose as per pre-approved retention period. In many instances, during this period, data is archived to save storage cost. Be in in system retaining or data archival, this is important to secure the data under consideration.
   a. All data during retention/ archival must be encrypted/ locked by using proper encryption methods
   b. All electronic data records shall be archived in secure labelled storage onsite or secure offsite location
   c. All the electronic data must be reviewed (*after a defined interval*) to check the status of the purpose of data retention

d. In case electronic data archival is outsourced, the selected vendor shall also come under state Data Retention guidelines and must comply with the existing data protection guidelines and state prescribed Information security standards.
e. Data stored in the physical tape/s (*both is SDC- Production site and DR site*) by the data owner must be checked/ validated by structured walkthrough or sample testing at a defined time frame based on the historic and economic importance.

F. Electronic Data Disposal or archival

The first step is to review of all electronic data requirements in regard to the electronic data retention need, usage frequency (*last time used*) and to decide whether to destroy or delete or archive any data once the purpose of those data is fulfilled or no longer required. Overall responsibility and ownership for the destruction or deletion or archival of the electronic data falls to the Nodal Officer of the owner organisation, notified duly for the said purpose.

Once the decision is made to dispose of the data according to the state electronic data retention guidelines 2020, the data should be deleted, shredded, archived or otherwise destroyed completely. The method of disposal varies and is dependent upon the nature of the document. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the duly notified Nodal Officer either delegates or subcontracts for this purpose. The data disposal process must be controlled in order to avoid loss of important data. The disposal process must be documented and approved by the duly notified Nodal Officer.

Prior to (a) transferring data into physical tape for archival beyond the primary retention period prescribed and (b) destroying the data permanently after completion of the total retention period including archival, the Nodal Officer with explicit written permission from the Head of the Department shall upload the said data on Public Transactional Data Sharing System after due anonymisation so that the said public data can be used by MSMEs and Start-ups in the greater interest of public service.

Disposal method shall vary depending upon the critical nature and type of the Data. This is briefed below-

- **Level I**: The electronic data in form of strategic, economic, security and/or financial importance, which are on the higher side on CIA (confidentiality, Integrity and availability) level requires highest security and confidentiality for a department/ organization, shall be disposed securely using prescribed standards. Disposal of such data should include proof of destruction.
- **Level II**: Proprietary data containing confidential information such as name, signature, address which may be used by third party for fraudulent activities, but don't contain personal data, shall be made anonymised and then disposed securely.
- **Level III**: Data that doesn't contain any confidential or personal information and are published as public information, can be stripped electronically or disposed through a recycling company or deleted electronically whichever is applicable.

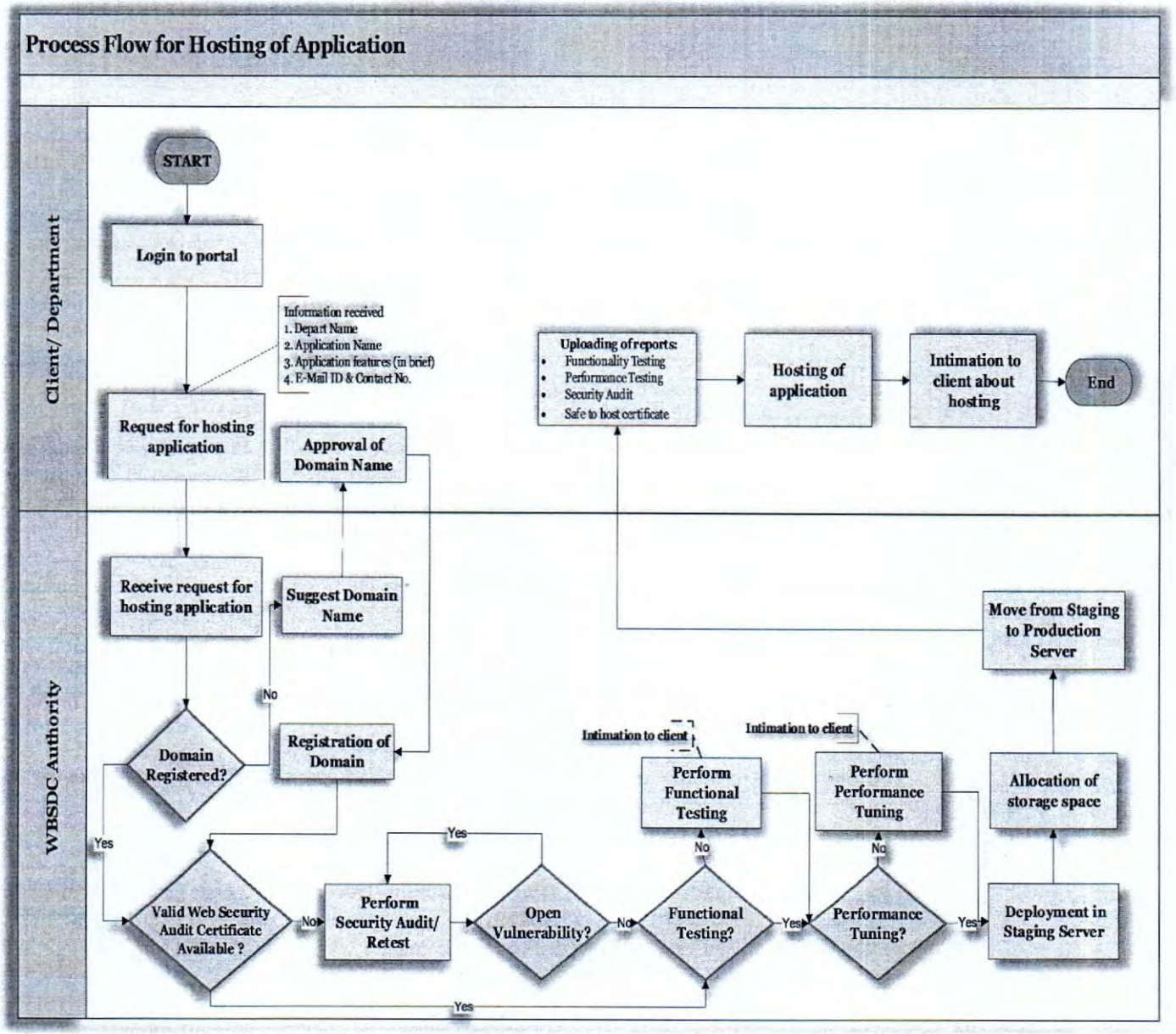
G. Sharing of Public Transactional Data with West Bengal Public Transactional Data Sharing System:

In compliance with the provisions of the West Bengal Public Transactional Data Sharing Guidelines, 2020; any public transactional data, if not already shared on the above-mentioned system after duly anonymising the same, should be first anonymised and shared on this system for ensuring their full utilisation by Start-ups, MSMEs, Govt organisations, NGOs of the State for promoting research and development, analysis and decision making including promotion of industry based upon such anonymised public transactional data.

H. State Data CenterStorage Space Requisition guidelines

The State Government departments, associated Government organisations, parastatals etc. who desire to host any type of the application and/ or avail any form of the services from WBSDC should apply online for seeking storage space for hosting their required application/s. A Self-Supporting Portal (SSP) of WBSDC should be in place for requisition of storage space, augmentation & reclamation of storage space, monitoring and other remote service management under WBSDC operations. In case of rejection of requisition, applicant should receive an email notification from WBSDC authority containing the reason of rejection. Some criteria need to be followed before hosting of an application, which are as follows:

a) Before hosting, each website must contain proper domain name and must be security audited by the CERT-In empanelled Security Auditor. In case of non-availability of the same, WBSDC authority will aid the applicant in meeting pre-requisites and ensuring compliance
b) Safe-to-Host certificate must be issued by the concerned CERT-In empanelled Security Auditor on latest version of their respective website/ web portal and furnished at the time of hosting at WBSDC.
c) The resources required for hosting of web application (application space & database space) would be provided by WBSDC authority
d) To host any application in WBSDC Cloud, the applicant initially needs to furnish the specification details in brief viz. number of VMs, storage space etc.
e) The allocation of storage space for the application will depend on the application Size (KLOC– Thousands (Kilo) of Lines of Codes)), Transactions/ Day and number of Concurrent Users.
f) For large application the initial storage size will be maximum up to 2 TB and small application the initial storage size will be maximum up to 500 GB. The average size of storage space required for a single transaction will be considered as 10 MB (including data & supporting like image, pdf etc.)
An indicative process flow for hosting of an application at WBSDC environment are mentioned below:



Dept. of Information Technology & Electronics
Govt. of W.B.

Once the initial space will be exhausted then the owner of the hosted application has to re-apply through online portal for space augmentation along with the certain mandatory documents/ reports viz. Load/Stress testing report, Profiler statistics, System and Application Logs etc. for validation purposes. The size of allocable space will be decided based on the sizing of the hosted application and the usability

The WBSDC authority has the mandate to withdraw unutilized allotted space, if the initial allocated space is underutilized. In that case the free space will be reclaimed in the free storage pool. These guidelines will be applicable for space reclamation of existing application in WBSDC if after 6 months from the date of space allocation, less than 75% of the storage space was utilized.

Once in every three year, for any hosted application, when more than 80% of the presently allocated storage space is exhausted then the owner of the application need to ensure that the existing data needs to be archived year on year basis in a dedicated archive storage space as designated/ provided by the SDC authorities and accordingly the existing storage is cleaned up to bring down the occupancy of storage space to at least 10%.

The data to be cleaned will be primarily transactional in nature. The master data related to any hosted application do not require any clean up or archival activities

J. Application Architecture guidelines

The web application to be hosted at WBSDC must comply with predefined standards in their design for better performance and easy maintainability so that it can deliver better user experience, ease of monitoring and improves service quality. The guidelines to be followed are:

- The application to be hosted in WBSDC must be designed following n-tier architecture. Exceptions can only be made in case of any application containing static content.
- All dynamic web applications must comply to the Model-View-Controller (MVC) architecture.
- Multiple clusters (Master/Slave) may be maintained to ensure service quality wherever the load is high.
- The application design is to be structured and includes defined parameterized data field to avoid Cross Site Scripting, SQL Injection or cyber-attacks of similar nature.
- All the up-loadable content (e.g. PDF, images etc.) are to be stored in a separate node, either in any Content Management System (CMS) or any structured hierarchical mapped folder in SAN or storage system of similar nature
- Any sensitive data like password, payment information, personal data etc. must be encrypted to avoid unauthorized usage and need to comply with respective industry standards
- Retrieval (export) or modification of any data stored in the database must not be allowed without formal approval from the application/ data owner of the application and SDC authorities.

K. User Access Management guidelines

These guidelines will ensure that access to the information assets is allowed based on the requirements of the business applications, information asset classification legal and contractual requirements.

- The application/ data owner/s should define security requirements of their respective web application/s
- Proper Access control should be deployed as per the defined role/s and comply with Contract terms.
- Minimum or baseline level of access control should be defined and implemented on all information types and data levels
- Every WBSDC information system user must have a unique user ID and password for system access.
- WBSDC documents, software's and any form of information should never be sold or transferred to any third party (Non WBSDC user) for any purpose. In case of any exception, an exception request needs to be raised and seek formal approval and authorization from the appropriate WBSDC authorities
- In case of any data leak or data loss of sensitive information or any form of data disclosure to unauthorized parties, the data/ application owner and department heads should be notified immediately.
- WBSDC information systems users are prohibited from gaining unauthorized access to any other information systems to prevent any form of damage, alteration, disruption to the operation or services.
- In case of separation from WBSDC, all user access privileges, and login access must be revoked immediately as on date of separation.

- A third-party user management audit procedure needs to be defined and followed quarterly.

L. Information Security Management guidelines

To ensure Confidentiality, Integrity, Availability and Privacy (CIAP) of information stored in the WBSDC environment, the certain security guidelines need to be followed by every user of WBSDC. All important Information Security Controls need to be followed by the WBSDC management and operation team namingly ISO 27001:2013- controls for data centre physical security & environmental controls, supply chain security, personnel security and network security. ISO 27017 controls for use of cloud services. ISO 27018 controls for protecting Personally Identifiable Information (PII) in public clouds which will also be in line with the ISO/IEC 29100:2011 controls that provide privacy framework where privacy controls are required for the processing of PII. Certain mandatory guidelines under Information Security Management Systems that are mandated are mentioned below:

i. Password Guidelines:

- Stringent criteria above the baseline for creation and usage of passwords should be followed for specific business requirement.
- All WBSDC systems will automatically lockdown after three unsuccessful password attempts on it by any user.
- Users are not allowed to reuse the last ten (10) old passwords in his account towards enhancement of the security to maintain the effectiveness of password history by enabling the minimum password age security policy settings.

ii. Backup as a Service Guidelines:

- Up-to-date backups of all critical items should be maintained to ensure the continued provision of the minimum essential level of service. These items include Data files, utilities programmes, databases, operating system software, Application system software, encryption keys, Pre-printed forms and business documentation plans.
- The Systems backups should consist of regular full and incremental backups.
- Media retention periods should be established and approved by WBSDC management in accordance with legal/regulatory and user requirements.
- Incremental Backups should be taken daily and Full backups should be taken weekly. Both should be retained at least for a period of 2 weeks. Monthly Backups should be retained for a period for at least One year. Yearly Backups should retain for at least two years.

iii. Cryptography Guidelines

- Data transferred through wide area network connections between WBSDC and its Customer(s) through internet as the medium should be adequately protected with suitable encryption technologies.
- Based on business requirements, business and/or customer sensitive and very confidential data stored on IT systems and applications (including on portable digital media, backup media, and in logs) should be encrypted.
- WBSDC authorized trusted authority should have the ability to issue or revoke electronic signatures as per business requirements, on behalf of an identified Licensed Certifying Authority (CA).

iv. Patch Management Guidelines

- WBSDC would carry out an assessment to understand the impact of vulnerabilities to WBSDC's IT environment.
- Patches should be tested in the test environment before actual implementation in the production environment by the system owners. Exceptions to this requirement should be recorded and maintained in case, testing is not feasible.
- However, any system should be rolled back once a patch implementation is found to be inappropriate or erroneous.
- Patches should be implemented by the system/ application owners at the earliest to all the vulnerable systems after assessment for applicability in WBSDC's IT environment. Critical patches should be installed within 10 days of release by the software vendor. Patch implementation information should be announced to the intended audience before the implementation in the production environment by the system owners.

v. Remote Access Security Guidelines

- Remote access to WBSDCs IT resources from public network will be allowed only after successful identification and authentication of users.
- Access to critical applications in the intranet will be granted only with two factor authentication.
- In case of user separation from WBSDC's services, user credentials will be deactivated on the last day of the user promptly by the respective account administration personnel.
- Virtual Private Network (VPN) access to WBSDC's resources will be authenticated using Active Directory (LDAP). User Authentication and authorised VPN session must be encrypted.

vi. Information access guidelines

- User access to IT infrastructure and applications should be granted based on an individual's job, required role & responsibilities on a "need-to-access" and "need-to-know" basis and the authorization should be obtained as defined in the access control matrix.
- Access control matrix should be maintained for IT infrastructure and applications.
- Third party access to IT infrastructure and applications should be permitted after due authorization from Information Owner.
- Users should not connect any new resources onto Network without getting prior approval from WBSDC authority.
- All logs/record evidences will be stored for a minimum period of a 45 days on primary storage (file server) and then 3 months on secondary storage. In case if necessary, for legal, contractual or for security related incidents the specific logs can be stored for a longer duration.

vii. Security incident management guidelines

- Any event impacting information security should be logged through self-supporting portal as per the Security Incident reporting procedure.
- Security incident can be classified as -
  - Cat A: Leakage of Sensitive/ Confidential information
  - Cat B: Violation to WBSDC policies
  - Cat C: Unauthorized access to information
  - Cat D: Identity thefts
  - Cat E: Loss/ Misuse of WBSDC's/client's asset
  - Cat F: Misuse of WBSDC's information & Computing resources
  - Cat G: Incidents related to Physical security
  - Cat H: Incidents leading to threat against national security.
- Procedures should be followed for reporting, recording, investigation and closure of incidents.
- All incidents should be categorized based on the severity, type and suitable corrective actions initiated based on this severity.
- Security incidents should be analysed and preventive & corrective actions taken to minimize recurrence of an incident.
- Forensic investigation should be carried out based on the severity and type of security incidents.

M. Removable Media Usage Guidelines

- Removable Media ports/interfaces (USB) usage within the WBSDC environment in general, should be controlled by disabling the Removable Media Interfaces in the Desktops and Servers.
- All removable media devices have to be declared at the security register by all users entering/ exiting the premises.
- Usage of personal removable media is not encouraged; however removable media may be used with laptops for legitimate business needs, only after ensuring that media is malware free and laptop is adequately protected against accidental infection from the media.
- All removable media devices need to be scanned for malicious threats and remove all unnecessary data prior to use further.

- User must not copy WBSDC sensitive information including but not limited to WBSDC personal contacts, Intellectual Property documentation, Non-public personal information such as credit card numbers, social security numbers etc. into the removable media from WBSDC assets.
- Information stored in removable media devices to address genuine business requirements, should be in an encrypted format.
- Employees should keep their official removable devices securely to avoid any theft or unauthorized data access.
- Access for enabling/usage of removable media within the Data Centre for official purposes should be permitted only after due authorization from WBSDC.
- Users found in non-compliance with this "Acceptable usage policy for Removable Media" will be deemed in violation of this policy, this requires an investigation and appropriate disciplinary action to be taken, up to and including termination from services.

N. Software Usage Guidelines

- Software with expired licenses and pirated or personal software must not be used in the IT environment of WBSDC.
- Users in WBSDC must exercise extreme caution prior to installation of software in WBSDC's IT infrastructure especially when the software is obtained through Vendors, Downloaded from Internet, Removable storage media and unauthorized software shared by another user. Software should be tested by WBSDC and authorized for use before installation.
- Users must not resort to any type of online transactions (E.g.: usage of personal credit cards for purchasing software) to purchase and download official software (for formal usage) from the Product Vendor websites, bypassing WBSDC's procurement process.
- WBSDC resources (such as WBSDC supplied software or software accessed in WBSDC IT assets) must only be used for business purposes in the course of normal business operations.
- Outright download and informal installation of Freeware software in WBSDC's machines is prohibited considering potential security vulnerabilities to WBSDC's IT resources.
- Regular audits to be carried out by WBSDC authority using automated tools to understand the usage pattern of software & associated licenses and also the type of freeware downloads.

O. Start-Up Support Guidelines:

The West Bengal State Government has accepted in principle and allocated a portion of the cloud infrastructure of the WBSDC for the state start-up community to utilise the best available sectoral data for their robust system development, live data testing and better tracking of the user lifecycle in terms of public service delivery.

In order to maximise reach and ensuring more Start-Ups receiving support, the Dept of IT&E being the Nodal Dept will decide the standard configuration to be offered to each of the Start-ups.

Considering the above and/or prevailing comparative rates of various cloud-service providers, the State Government in the Department of IT&E will finalise the pricing model for providing web space to Start-Ups and state MSMEs.

The rate for such service, to be collected by the State Implementation Agency (SIA) as to be decided and under the aegis of the Dept of IT&E, shall duly be notified with concurrence from the State Finance Dept.
The proposed cost for such facility includes all licenses, tools and OS in various stages of deployment, to be charged monthly by the State Implementation Agency (SIA) notified by the Nodal Department i.e., Department of Information Technology & Electronics. Facility for availing rebate (of 15% or such amount as to be duly notified) will be extended to such Start-ups and MSMEs who will pay the charges on a yearly basis, in advance. This minimal revenue will augment Government funds in maintaining and providing a benchmarked service delivery to these Start-ups and MSMEs, which is first of its kind in the country.

A Selection Committee to be notified by the State Government in the Dept of IT&E, being the Nodal Department shall call for application through Departmental Portal with adequate publicity in digital as well as print media and select fifty (50) deserving Start-Ups to be offered the above Cloud Infrastructure as a Service (C-IaaS) at the WBSDC.

P. Grievance Redressal Guidelines

Any grievances related to the operations & maintenance of WBSDC should be raised online through Self-Supporting Portal (SSP) of WBSDC. There will be specific timeframe in solving the problems and feedback to be captured online for further improvement.

By order of the Governor,

Sd/-
Principal Secretary to the
Government of West Bengal.

No. 588-Estt/ITE-20012/2/2020 Date: 28/12/2020

Copy forwarded for kind information and necessary action to :-

- The Secretary to the Government of India, Department of Telecommunications, Sanchar Bhawan, New Delhi 110001.
- The Secretary to the Government of India, Ministry of Electronics & Information Technology, 6, CGO Complex, New Delhi-110003.
- The Additional Chief Secretary / Principal Secretary/ Secretary, Department(all).
- The Managing Director, WBEIDC Ltd, Block – EP & GP, Sector-V, Salt Lake, Kolkata-700 091.
- The Dy Director General, Telecom Enforcement Resources & Monitoring (TERM) Cell, West Bengal, 82, Ballygunj Place, 2nd Floor, Kolkata-700 019.
- The Dy. Director General, Telecom Enforcement Resource & Monitoring Cell, Kolkata Licensed Service Area, QA Bhawan, ,Block –EP&GP, Sector-V, Salt Lake, Kolkata-700 091.
- The Chief General Manager, BSNL, West Bengal Telecom, 1, Council House Street, Kolkata-700 001.
- The Chief General Manager, BSNL, Calcutta Telephones,34, BBD Bag (South), Kolkata -700001.
- The District Magistrate, District(all),West Bengal.
- The OSD to the Chief Secretary, Govt. of West Bengal.
- The PS to the Hon'ble MIC(IT&E Department),GoWB.
- The Sr. PS to the Principal Secretary to the Govt. of West Bengal, IT&E department.
- The Advisor, Telecom Regulatory Authority of India, Kolkata Regional Office, Bharat Bhawan, 1st Floor, 3, C.R. Avenue, Kolkata 700072.
- The Director General, COAI, Sector 2, 14, Bhai Vir Singh Marg, Sector 4, Gole Market, New Delhi, Delhi 110001.
- The Chief Executive Officer, Webel Technology Limited, BP-5,Sector-V, Salt Lake, Kolkata-700091.
- The Head(Operation), Tata Tele Services Ltd, PS-Srijan Tech Park, DN-52,12th Floor, Sector-V, Salt Lake, Kolkata-700 091.
- The Chief Operating Officer, Vodafone Idea Limited, 8, Major Arterial Road, Tower-C, DLF IT Park, 15th & 16th Floor, New Town, Kolkata-700 156.
- The Nodal Officer, Bharti Airtel Ltd, Infinity Building, 7th Floor, Sector-V, Salt Lake Electronics Complex, Kolkata-700 091.
- The Assistant Manager-Legal, Tower Vision India Pvt Limited, Signet Tower, DN-2,Unit No 1101, 11th Floor, Sector-V, Salt Lake, Kolkata-91.
- The Manager-Regulatory, Reliance JIO Infocomm Ltd, Ecospace, Business Park, 3B,4th Floor, Rajarhat, Kolkata-700 156.

- The Advisor, Indus Towers Ltd, Godrej Waterside, 8th Floor, Tower-I, Unit-801,Plot No-5, Block-DP,Sector-V, Salt Lake, Kolkata-91.
- The Head, American Tower Corporation India, 145, Rash Behari Avenue, 4th Floor, Kolkata-700 029.
- The Director General, TAIPA, 2nd & 3rd Floor, 7, Bhai Veer Singh Marg, Gole Market, New Delhi-110 001.
- The Circle Head, Aircel, 3rd Floor, Globsyn Crystal Building, Plot-11 & 12, Block- EP&GP, Sector-V, Salt Lake, Kolkata-700 091.

Joint Secretary to the
Government of West Bengal
Information Technology & Electronics