GOVERNMENT OF WEST BENGAL
DEPARTMENT OF INFORMATION TECHNOLOGY
AND ELECTRONICS
Moni Bhandar, Webel Bhavan Campus, Block-EP&GP
Sector-V, Salt Lake, Kolkata-700 091

No - 225 (76)-ITE-18011/2/2026 Date - 05/03/2026

From: Secretary to the
Government of West Bengal.

To: 1) Additional Chief Secretary/ Principal Secretary/ Secretary to the Government of West Bengal_____ (all) Department.

2) District Magistrate_____(all) District, West Bengal.

Sub: Standard Operating Procedure (SOP) of West Bengal State Data Centre (WB-SDC).

Madam / Sir,

I would like to draw your kind attention to the fact that a Standard Operating Procedure (SOP) of West Bengal State Data Centre (WB-SDC) has been prepared for providing seamless services in a structured and rational manner and within a reasonable timeline for the user organizations. A copy of the said SOP is attached with this letter for your kind perusal and information.

In this regard, I would like to request you to circulate the said SOP down the line within your jurisdiction for a wider reach of the same.

Yours faithfully,

Encl: As stated.

Secretary

No. 225(76)/1(7)-ITE-18011/2/2026 Date: 05/03/2026

Copy forwarded to:-

1) CEO, WBETS.
2) Director, WB-CSIRT
3) Managing Director, WBEIDC Ltd.
4) CEO, WTL.
5) Member Secretary, CsCOE.
6) Project Manager, WB-SDC, Plot- 5, Block- BP, Sector-V, Salt Lake City, Kolkata-700091.
7) SPA to the Special Secretary, IT&E Department, GoWB.

Special Secretary
to the *Government of West Bengal*

STANDARD OPERATING PROCEDURE (SOP) FOR

WEST BENGAL STATE DATA CENTRE

The West Bengal State Data Centre (WBSDC) is a key initiative under the Department of Information & Technology, GoWB. It aims to consolidate services, applications, and infrastructure to ensure efficient electronic delivery of government services to citizens, businesses, and other government entities.

Hosting Service offered by WBSDC

The following services are provided by WBSDC

Sl No	Services Description
1	**Department onboarding within the WBSDC Hosting Portal**
2	**Domain Registration**
3	**SSL Certificate Provision**
4	**Provisions of Virtual Machines (VMs) and reclaim of VM**
5	**Provision of Virtual Private Network (VPN)**
6	**Port Opening/IP Whitelisting**
7	**Provisioning of Internet Service**
8	**Server Load Balancing & Network Security Services**
9	**Application Load Testing Services**
10	**Application Go-Live : Hosting Application via Public Internet**
11	**Server Backup facility**
12	**Disaster Recovery service for Database only**
13	**Call Logging and Interactive Ticketing Service**
14	**Physical Access Provisioning at WBSDC**

1. Department onboarding within the WBSDC Hosting Portal

a. Head of the Department of every department shall designate an individual(s) who will be responsible for all hosting activities for that department. Department shall select personnel(s)who will be accessible round the clock during emergent situation(s) and who can coordinate technical requirements through hosting portal (**https://hosting.wb.gov.in**).

b. Department needs to access the WBSDC Hosting Portal at **https://hosting.wb.gov.in**as and when required for technical support or to register their requirement(s) related to WBSDC.It is accessible from the public internet for all government organisations.

c. For immediate access to all hosting services, department needs to create departmental account in the hosting portal (**https://hosting.wb.gov.in**), department needs to REGISTER first in the hosting portal.

d. The registered Users of the Department in the hosting portal in case of a transfer should provide the Charge Handover request in the hosting portal for access to the old hosting requests provided by the new designated user.

e. The Department is requested to periodically review the User registered in the hosting portal. The Charge hand over request needs to be provided in the portal for transferred or retired User to obtain the access of the old user hosting requests in the profile of new User. The Head Of the Department should provide the request judicially for seamless access to the hosting portal.

*** **All requests for Department onboarding in the WBSDC Hosting portal will be processed, subject to approval by the Department of IT&E, GoWB**. ***

2. Domain Registration

a. Before the application can be accessed from the internet, the Department must have a URL/Domain name bound to a Public IP provided by WBSDC. The Department must apply for a 4th- or 5th-level domain name under wb.gov.in via the WBSDC Hosting Portal.

b. After receiving theapplication for domain creation through the Hosting Portal, WBSDC will initiate the process of domain creation. The DOMAIN NAME SYSTEM (DNS) registration for all domains under **wb.gov.in** is managed by **registry.gov.in** (Govt. of India). The estimated time to complete the process is **THREE WORKING DAYS**, excluding Saturdays, Sundays, and Government holidays.

c. WBSDC shall assign pubic IP from the WBSDC IP pool for 4th and 5th level domains registration for **wb.gov.in** only.

d. In case of requisitioning Department provides a URL/Domain name from a third-party provider (*.gov.in/*.org/*.in) **a request for a Public IP must be placed for hosting**. Application can only be hosted publicly after mapping of public IP with the third-party domain.

e. Requests for Domain registration for applications hosted outside WBSDC will not include an SSL certificate; the user department must arrange it. WBSDC will only facilitate to registering the

Domain and requesting Department must share the Public IP against which the domain needs to be registered.

f. The Department(s)having their own existing domains (e.g; *.gov.in, *.in, *.org etc.) and intended to shift their existing application at WBSDC must apply for a **wb.gov.indomain** for their existing application. The valid SSL certificate for the same will be provided by WBSDC in due course.

*** **All requests for domain registration within the WBSDC Hosting portal is subject to the approval of the Department of IT&E, GoWB**. ***

3. SSL Certificate Provision

a. All applications going live from WBSDC must have a valid SSL certificate.
b. WBSDC provides SSL certificates only for 4th-level domains/URLs under the wb.gov.in domain.
c. If the domain/URL is a 5th-level domain under wb.gov.in, the requesting Department shall be responsible for procuring and providing a valid SSL certificate.
d. If the domain/URL is registered through a third-party provider, therequesting Department must arrange a valid certificate for the application.
e. Department / Directorate must ensure that a valid SSL certificate is obtained and submitted. (except 4th level domain i.e. wb.gov.in)
f. Application shall not be live without a valid SSL certificate.
g. In cases where the Department / Directorate provides the SSL certificate, it is their responsibility to ensure that WBSDC receives a new SSL certificate before the existing one expires. Failure to do so will result in the discontinuation of the public access of the application.

4. Provisions of Virtual Machines (VM)& Reclaim of VM

a. All request for VM provisioning/De-provisioning/Resizing must be provided through the hosting portal only.
b. WBSDC retains the right and authority to optimize / re-allocate VM resources after validating the application documents/architecture before final provisioning of VM.
c. WBSDC only provideslicensed operating systems and databases (Microsoft Windows Server/RedHat Linux/Microsoft SQL Server) while provisioning of VMs.
d. Minimum (by Default) OS partition (C: or root File system) providesby WBSDC is 100 GB.
e. No **data file**(Application or Database Files) shall be allowed to be stored in the OS System Partition.
f. As per security policy of the WBSDC, antivirus software in all VMs shall be installed by WBSDC, and WBNGSOC shall install the security log analyser software without any exception.
g. As per WBSDC security measures, after the first login in the allocated VM(s), the default password must be changed immediately by the user's Department before proceeding further.

h. Depending upon the number of VMs requested, VM Provisioning /De-Provisioning/Resizing required time duration may differ from the Turnaround Time table provided in **Table – A** (last page of this document)

i. WBSDC only provide VMs for Application, Database, File Server for **domain-based hosting** only and**notfor Mail Servers, Graphical applications, or Local network applications.**

j. WBSDC does not provide VMs or storage for storing video surveillance data (CCTV feed).

k. VMs may require a restart on a case-by-case basisresource resizing and, in cases of extension of the storage partitions.

l. The VMs need to be shut down by the user Department during resource resizing and extension of the storage partitions. After completion, the WBSDC will intimate the relevant Department to START the VM.

m. VMs UPGRADATION / RESIZEshall bedone only after reviewing the actual utilisation ofthe allocated resources like **vCPU, Memory & Storage.**

n. No VMs UPGRADATION / RESIZE will be entertained **if the utilisation of the already allocated resources over the last 30 days is below 70% of the total allocated (vCPU, Memory & Storage Space).**

o. The user Department must complete testing and implementation before going live / public within the mentioned timeline (90 days) against the VMs provisioned for. VMs that are not used for production / go-live / public after 90 days will automatically be deactivated.

p. The respective user Department will get prior notification for VM deactivationfor not being moved to **production/go-live** within the stipulated time (90 days) as per WBSDC protocol. The deactivation notification will be sent via the Hosting Portal and the registered email addresses.

q. The User Department may request the VM performance log (vCPU, memory and storage) as and when required through the hosting portal. WBSDC in no circumstances will share its internal security device log such as (firewall, WAF etc).

r. User Department must contact directly to WBNGSOC (**support_wbngsoc@wb.gov.in**) for the logs of the VMs allocated to them by the WBSDC, specifying period of log required subject to availability of the same, provided security analyser tool is installed in the respective VMs.

s. Vulnerability Assessment (VA) test report will be provided by the WBNGSOC (**support_wbngsoc@wb.gov.in**) onrequest by the user Department only for their allocated VMs.

t. WBSDC shall not provide Virtual Machine, Storage space, or other services for development, staging, and testing purposes.

*** **All requests for VM provisioning in the WBSDC Hosting portal will be completed, subject to approval by the Department of IT&E, GoWB**. ***

WBSDC Resources Reclaim

- WBSDC continuously monitor the Hosting resources (such as vCPU, Memory, and Storage) provided to the User Department, and will be authorised to reclaim the resources after prior notice to the concerned department, if found that the resources so allocated are under utilised by the User Departments and kept idle for a maximum period of 90 days.

  The resource reclaim percentage is shown in the table below.

Resource Type	Utilization Minimum Threshold	Reclaimed Resource
vCPU	<30%	50%
Memory	<30%	50%
Storage	<30%	50%

***** As an example, if a VM is initially provisioned with 32 vCPU/32 GB memory and have 29% of vCPU and memory utilization for three months (90 Days), the resource reclaimed by WBSDC will be 16vCPU/16 GB memory (50% of 32 vCPU/32 GB Memory) *****

***** VMs provisioned to the Departments,and configured by the User Department for Data backup/database replica purpose will be deprovisioned after providing a prior notice. WBSDC has own default backup solution for Primary Database VMs and will not allow provisioning of separate VMs for any other backup purpose *****

5. Provision of Virtual Private Network (VPN)

a. WBSDC will provide VPN client facility to every application owner for accessing remotely and securely for their allocated VMs.

b. Maximum 5 numbers of VPN users can be provided for every application and associated domain. Additional claimon VPN users are purely need based and subject to approval of the appropriate authority, Department of IT&E, GoWB.

c. The VPN application request shallbe made through the hosting portal only.

d. Two-factor authentication is standard (Password and Mobile OTP) for VPN access.

e. VPN credentials will remain active for 90 days from the date of provisioning and shall auto-expire. Departments must submit renewal requests through the hosting portal for re-activation of the same.

f. Department/Directorate and any owner of the used VPN user must provide a VPN deactivation request through the SDC hosting portal (**https://hosting.wb.gov.in**) if the VPN connection is no longer required.

g. The VPN should be usedonly for Application hosting requirements. **WBSDC does not provide a VPN for development**; it should be used judiciously.

h. VPN requests received by the WBSDC shall be processed after working hours (5.30 P.M. onwards).*** **All requests for provisioning of VPN within the WBSDC Hosting portal will be considered, subject to the approval of the Department of IT&E, GoWB**. ***

6. Port Opening/IP Whitelisting

a. WBSDC provides a facility to communicate the hosting infrastructure within and outside.
b. Department /Directorate (application owner) can provide a Port opening request through the hosting portal only.
c. WBSDC provide the port opening facility either permanently or for a specific period as per the requirements of the application owner.
d. WBSDC may prevent / reject any port opening request(s) on security ground, if port(s) are found to be vulnerable and harmfulto WBSDC infrastructure.
e. The port opening request require white listing of WBSDC IP bythe external entities (e.g; Bank, Aadhaar, etc.) to function properly. Requesting department will confirm it through hosting portal.
f. Port opening requests are processed at WBSDC after working hours (5.30 P.M. onwards).

*** **All requests for Port opening / IP Whitelisting within the WBSDC Hosting portal will be processed, subject to approval by the Department of IT&E, GoWB**. ***

7. Provisioning of Internet Service

a. WBSDC provides internet facility in the allocated VMs as per requirement of the concernedDepartment for a certain period (48 hours).
b. The Department /Directorate or application owner should submit a request for internet facilityto the VM through the Hosting portal.
c. WBSDC provide a maximum of 48 hours of internet facility in the allocated VMs, for each request that automatically gets deactivated after 48 hours. For further requirement (if any), a new request must be submitted through the hosting portal.
d. WBSDC keeps the right to approve or reject any such application regarding internet facility.
e. WBSDC do not provide open internet for security concerns and has implemented Geo-fencing for cyber security, which may prevent access to some specific internet sites or services from being available.

8. Server Load Balancing & Network Security Services

a. Server Load Balancer (SLB) facility is available at WBSDC only for the web/application equipped for provisioning of minimum of two web/application server VMs.
b. Department /Directorates with multiple servers may request SLB service. WBSDC provides services to the SLB-equipped application to enhance high availability and performance on request only.

c. WBSDC is equipped with Advanced firewall services combined with Intrusion Prevention Systems (IPS) and**Web Application Firewall (WAF)** to protect web applications by monitoring, filtering, and blocking malicious HTTP/S traffic and thereby protecting infrastructure from unauthorized access attempts.

d. WAF does profiling of normal application behavior to detect and block abnormal activities. Application ownerneed to modify their application accordingly for protection from a wide range of cyber threats.

e. WBSDC usesCountry-wise IP restriction system to control access based on geographic location to enhance security.

f. As per security protocol, WBSDC does not share details about installed FIREWALL.

9. Application Load Testing Service

a. WBSDC provides**Application Load Testing**up to 5000 concurrent sessions. The Respective Department shall test its application at the WBSDC load-testing facility before going live for public.

b. Department shall apply through the WBSDC hosting portal for application load testing. After receiving application, WBSDC will share the testing date and time. The application development team shall report to WBSDC along with the application flow and other necessary details required for load testing.

c. Without load testing, the application shall not be made live from the WBSDC cloud.

10. Application Go-Live: Hosting Application via Public Internet

a. This request shall be submitted by the Department / Directorate through the WBSDC Hosting Portal using the **Deploy-to-Production** option.

b. Application Go-Live: Hosting the application via the public Internet will be processed by submitting a valid **Safe to Host certificate** (Application security audit by a CERT-In empaneledorganisations) or by submitting a **temporaryRisk Acceptance declaration** under **signature and seal** of the HoD of the concerned department valid for90 days only. In that case after the expiry of90 days hosting of such application will be halted till the submission of **Safe to Host certificate.**

c. User Department / Directorate must conduct the Vulnerability Assessment (VA) test for their allocated VMs, WBNGSOC (**support_wbngsoc@wb.gov.in**) will provide the same.

Application Go-Live with Security Audit certificate

d. A CERT-IN empaneled auditor must audit the application and certify **Safe to Host**before hosting. It is the department's responsibility to upload a valid Safe-to-Host certificate.

e. Expiry of the above-mentioned application security audit certificate (Safe to host certificate) must be renewed by any CERT-In empaneled organisations prior to expiry and the same should be updated through the WBSDC Hosting Portal also.

f. If the user Department requires the Vulnerability Assessment (VA) test for their allocated VMs, they need to contact WBNGSOC (**support_wbngsoc@wb.gov.in**) for the same.

Application Go-Live with **Risk acceptance declaration**

g. In case of urgency to make the application live before completing the security audit by a CERT-IN empaneled organisations, the Department /Directorate**intended to host** their application must go through **scanning of the application** from the Next Generation Security Operation Centre (WBNGSOC). The respective application owner shall contact WBNGSOC for application scanning (support_wbngsoc@wb.gov.in).

h. After completion of the scanning of the application by the WBNGSOC, the respective application owner will share the **application scanning report** with WBSDC through the hosting portal along withthe**Risk acceptance declaration** in the format available in the WBSDC hosting portal.

i. The risk-acceptance declaration needs to be uploaded after being duly signed and stamped by the Head of the Department for the interim period. However, it remains the Department's responsibility to provide the Safe-to-Host certificate to WBSDC within 90 days mandatorily.

j. If the Department / Directorate fails to provide the required safe-to-host certificate within the promised timeframe (90days), WBSDC reserves the right to revoke public access to the application with prior intimation communicated to the registered email address of the concerned department.

k. Any security breach affecting WBSDC infrastructure due to vulnerabilities in the application will be the sole responsibility of the respective Department forapplication(s) goes live with a risk-acceptance declaration.

l. All applications going live from WBSDC must have a valid SSL certificate. WBSDC provides SSL certificates only for 4th-level domains/URLs under wb.gov.in. For the 5th-level domain /URL under wb.gov.in, the concerned Department will be responsible for procuring and providing a valid SSL certificate.

m. If the domain/URL is registered through a third-party provider, the concerned Department /Directorate must ensure a valid SSL certificate obtained and submitted to WBSDC.

n. Application should not go live without a domain/URL and a valid SSL certificate.

o. Instances, where the Department / Directorate provides the SSL certificate, it shall be their responsibility to ensure that WBSDC receives a new SSL certificate before the expiry of the existing one. Non-availability will result in the termination of public access to the application.

11. Server Backup facility

a. WBSDC keeps back up for all the primary production database VMs only as per the default backup protocol of WBSDC and by default, the Backup retention will be for 7 Days.

b. Only Primary Database VMs are going to be backed up as per WBSDC Backup protocol.

c. WBSDC backup infrastructure facility is not available for Co-located infrastructure deployed and maintained by the user Department. The SDC backup facility exclusively available for the SDC cloud infrastructure.

d. All Co-located infrastructure installed at WBSDC by the user Department must deploy the backup infrastructure for their co-located setup physically installed at WBSDC and maintain by the Department only.

e. Any other backup solution for co-located infrastructure located outside SDC infrastructure will not be provisioned by SDC.

12. Disaster Recovery service for Database only

a. WBSDC keeps clone of every production databaseof VMs at its disaster recovery (DR) site.

b. As per standard DR replication protocol, WBSDC only replicates the Production DB VMs in every 6 Hours.

c. The Department/Directorate or application owner may also engage an internal or external System Integrator to configure OS- or database-level replication if needed. The default cloud replication will be suspended during that time. Replication will be executedon the basis of OS & database replication features.

13. Call Logging and Interactive Ticketing Service

a. For all types of communications related to WBSDC, an interactive call-logging and ticketing system available through the WBSDC Hosting Portal.

b. Registered users must raise a ticket for any issues related to WBSDC infrastructure & Services through the WBSDC hosting portal. All tickets are acknowledged and responded by the WBSDC Technical Team within two (2) hours from receipt of the same.

c. Once a ticket is raised, WBSDC will provide updates and may seek additional inputs through the same ticket. Registered users are required to monitor the ticket response and provide the required reply to facilitate the timely disposal and closure of the issue.

d. All the Service Requests raised by User Departments like VM Provision, VM-Resize, VPN Request, etc., that require approval from the IT&E Department will only be worked upon on working days between 10:00 A.M. and 5:30 P.M., except Saturday, Sunday and Government Holidays.

14. Physical Access Provisioning at WBSDC

a. WBSDC is an extremely secured place and beyond the purview of general access. However, for Physical Access,request in SDC hosting portal from the concerned department are mandatory.Whoever require physical access to WBSDC for any sorts of technical reasonneeds to apply through hosting portal for entry in the WBSDC premises. It is recommended that a senior official from the organization accompany their technical personnel if they belong to a third-party

institution.As per security protocol WBSDC shall not provide internet facility to any third-party assets (Laptop / tablet etc.) within the WBSDC.

b. Organizations may also raise a physical access request for large-scale data transfers. In that case data backup must be made via an external disk drive, after being thoroughly scanned for viruses, malware, and other security threats before being plugged in to the WBSDC infrastructure. WBSDC will then provide a jump server to facilitate high-speed data transfer, ensuring a significantly faster, safer connection than a VPN.

c. As per security protocol of the WBSDC, using through SDC internet connectivity, **ONLINE (through VPN/API/Point to Point Whitelisting)** bulk data transfer from WBSDC to external entity or vice-versa is prohibited.

d. Requesting department must ensure all details provided in the physical access request is accurate. In case of discrepancies, the Department/Directorate will be responsible for such lapses and required to submit a new request to proceed with access approval.

Standard Time Duration for Various Services provided by WBSDC

Table - A

Sl. No.	WBSDC Services	Turnaround Time in Business Hours/working days
1	VM Creation/ Deletion (Per VM)	24 Hrs. (One working day)
2	VPN Request	24 Hrs. (One working day)
3	Port Opening Request	24 Hrs. (One working day)
4	Internet request	24 Hrs. (One working day)
5	VM resizing	24 Hrs. (One working day)
6	Domain request	72 Hrs. (Three working day)
7	NAT request or Public Hosting	24 Hrs. (One working day)
8	Backup request	24 Hrs. (One working day)
9	Call Ticket Response	2 Hrs.

CONTACT DETAILS OF WBSDC

1. WBSDC HOSTING PORTAL - https://hosting.wb.gov.in
2. WBSDC Email - helpdesk.wbsdc@wb.gov.in
3. WBSDC Helpdesk Contact - 033-4087 4310

Secretary to the Government of West Bengal
Department of IT&E