

# Information Booklet



**WEST BENGAL STATE DATA CENTRE**  
**Department of Information Technology**  
**Government of West Bengal**

## Version History

Version / Release	Release Date	Change No.	Section Changed	Modification done by
1.0	12/07/2011	0	Information Booklet for Stake Holders	WBSDC-CT
1.1	22/07/2011	1	Policy Matters	WBSDC-CT
1.2	27/07/2011	2	WBSDC-LD Agreement	WBSDC-CT
1.3	10/08/2011	3	Management, Services at a Glance	WBSDC-CT
1.4	16/08/2011	4	How to join WBSDC? Agreement, Policies, WBSDC Infrastructure	WBSDC-CT
1.5	26/08/2011	5	Incorporating original WBSDC images and cosmetic changes	As suggested by DIT, GoWB and SeMT
1.6	06/09/2011	6	Appearance modification	As suggested by DIT, GoWB
1.7	28/11/2011	7	SLA separated as an individual document	WBSDC-CT
1.8	30/01/2012	8	Why SDC introduced, Minor Changes in the presentation.	As suggested by SIA
2.0	27/06/2013	9	Hosting Model, Policies ,SLA Modified	WBSDC-CT

## Table of Contents

<b>ELITE SYNOPSIS .....</b>	<b>3</b>
<b>1. SERVICES AT A GLANCE:-.....</b>	<b>5</b>
<b>2. BACKGROUND AND MISSION.....</b>	<b>6</b>
<b>3. PURPOSE &amp; SCOPE.....</b>	<b>7</b>
<b>4. WHY SDC .....</b>	<b>8</b>
<b>5. SDC'S OPERATIONAL VISION.....</b>	<b>10</b>
<b>6. WBSDC CONNECTIVITY .....</b>	<b>12</b>
<b>7. HOW TO JOIN WBSDC.....</b>	<b>14</b>
<b>8. WBSDC INFRASTRUCTURE .....</b>	<b>16</b>
<b>9. POLICIES .....</b>	<b>26</b>
9.1 PHYSICAL ACCESS CONTROL POLICY .....	27
9.2 NETWORK SECURITY AUDIT POLICY.....	34
9.3 BACKUP POLICY .....	35
9.4 SERVER SECURITY POLICY.....	42
9.5 FIREWALL POLICY.....	48
9.6 AUDIT LOG POLICY .....	50
9.7 PORTABLE MEDIA USAGE POLICY.....	56
9.8 REMOTE ACCESS POLICY.....	58
9.9 PASSWORD POLICY .....	60
<b>ANNEXURE-I.....</b>	<b>61</b>
A. SERVICE AND RESOURCE OPTIONS: .....	61
B. OPERATION COST OF DCO .....	64
C. LIST OF SUMMARY REPORTS.....	67
<b>ANNEXURE-II(FORMS).....</b>	<b>70</b>
FORM- 1: QUESTIONNAIRE FOR THE LINE DEPARTMENTS.....	71
FORM 3: WBSDC ACCESS REQUEST DECLARATION.....	82
FORM 4: WBSDC ACCESS REQUEST FORM.....	83
FORM 5: ONLINE SDC ACCESS REQUEST .....	84
FORM 6: CHANGE REQUEST.....	85
FORM 7: DECLARATION FOR TEMPORARY USAGE OF WBSDC RESOURCES.....	87
FORM8: UNDERTAKING FOR VPN ACCESS.....	88
FORM9: VPN ACCESS REQUEST FORM .....	89
FORM 10: SAFE TO HOST CERTIFICATE FOR SECURITY AUDIT .....	90
FORM 11: UNDERTAKING .....	91
<b>ANNEXURE-III(POSITIONING OF LINE DEPARTMENT) .....</b>	<b>92</b>
<b>ANNEXURE-IV(GLOSSARY /ABBREVIATIONS) .....</b>	<b>97</b>
10. MANAGEMENT .....	98
11. CONCLUSION .....	99
12. REFERENCES.....	100

## Elite Synopsis



Over the years, several initiatives have been undertaken by the State and Central Governments to usher in an era of e-Government to improve the service delivery to the people of India. Establishing core infrastructure such as Wide Area Network, Data Centre in each state is one of the major e-Government initiatives under the National e-Governance Plan (NeGP) with the intent to provide centralized computing facility and support efficient Governance in the country for on-line service delivery to the citizen, business and Government. The State Wide Area Network (SWAN) in West Bengal is in operation for a couple of years while West Bengal State Data Centre (WBSDC) is made operational a few months ago. Both of these are situated in the Webel complex of Saltlake, Kolkata.

The WBSDC is built upon a floor area of about **400 sq m** with a provision for extension of about **120 sq m**. The SWAN and WBSDC are based on the latest state-of-art technology with a vigorous architecture having multilevel redundancies, security and scalability with an additional emphasis in three-tier power supply system. The WBSDC complied with a world class **Tier II data centre** (having redundant capacity components and distribution path serving business continuity) as per **TIA 942 standards** with a **guaranteed service level of 99.749%** has a safe, secure, monitored, highly available power and cooling arrangements that is capable of accommodating several racks for network components and servers under centralized and simplified management. WBSDC is on the process of achieving **ISO 27001/20000 Standard**.

The WBSDC is powered through a separate substation with two different sources of grid power supplies supported with multiple generator sets. A sturdy building management system with fire fighting arrangements, water leak detection system, biometrics for access control, alarms & surveillance, rodent repellent, public address system etc ensures safe and secured operation of WBSDC complying with ISMS standards. The WBSDC is fabricated with a full-bodied network infrastructure complied with both present generation Internet Protocol (IP v4) as well next generation Internet Protocol (IP v6) using Dual-Stack deployment and equipped with multilevel security system including intrusion prevention, demilitarisation and two-level firewalling. WBSDC has robust Intranet Backbone coupled with 2 different Upstream Internet Service Providers.

'**Banglar Mukh**' the State G2C Portal for Govt. of West Bengal, a single window representative portal for the Government of West Bengal, 'E-District' Application for e-enabling of District Administration Services having backend computerisation, a pilot project for district level services (initially with two districts), **WBSASPFUW (West Bengal State Assisted Scheme of provident Fund for Unorganised Workers)**, an application for serving the people categorized as unorganised sector and the '**Kolkata Urban Services for the Poor (KUSP)**', a project to serve the deprived people of urban areas has been hosted in the WBSDC.

Besides, the Data Centre possesses several servers to cater to shared services over multiple OS platforms with virtualisation, viz. Windows, Linux and database management systems such as Oracle, MSSQL etc. The shared services also include power, storage space, local area network, tape library and abundant rack space to accommodate additional servers in the server farm. **Facility Management Services (FMS)** including routine backup, continuous monitoring of security, servers, network devices, application and database services, immediate resolution of defects and incidents are part and parcel of the 24 x 7 operational infrastructures.

The FMS also includes furnished accommodation for the support personnel to be deployed by the Line Departments for regular support of their infrastructure. Measures are also being taken to create Disaster Recovery Service Centre (DRS) in a different seismic zone and integrate the WBSDC with it in order to maintain absolute business continuity with prevention of any data loss.

Line Departments interested in hosting applications in WBSDC may choose any one of the following hosting models depending on the complexity, criticality and volume of their application: Dedicated, Partially shared, and fully shared hosting models. They need to sign a **Service Level Agreement (SLA)** with DIT prior to hosting.

The subsequent sections of this document factor the background, architecture, brief infrastructure, and essential policies for server, security; the common and optional services detailed in the generic agreement, standards and procedures for effective and efficient usage and better management of the resources.

## 1. Services at a glance:-



**Application Hosting Services** available for **24x 7** with a guaranteed service level uptime of **99.749%**. Services available in SDC may be classified as the following (explained below in brief):-

<i>Infrastructure Services</i>	<i>Managed Services</i>
<b>1. Rack Space: Cooled rack space with abundant space for additional racks</b>	1. Managed Security Services
<b>2. Power Supply: Multi-tier, Uninterrupted Redundant Power Supply services</b>	2. Backup Services (Routine backup as per the requirement of the stake holders.
<b>3. Collocation Service for Line Department's hardware, storage, network and server.</b>	3. Vendor Management
<b>4. Connectivity to SWAN &amp; Internet (Internet facility with options for enhancement (on demand)).</b>	4. Basic Hardware and OS level support
<b>5. Fully redundant Network Services with firewall and IPS.</b>	5. Storage configuration and Management
<b>6. Staging Service (virtualized).</b>	6. <b>Held Desk Services</b> (24 x 7).
<b>7. Shared Service for Hardware, Network &amp; Storage and other Compute Infrastructure</b>	7. <b>Antivirus and Host based Intrusion Prevention Service.</b>
<b>8. Application Hosting Service(for Line Departments)</b>	8. <b>VPN facility</b> (on demand) for remote management.
<b>9. Facility Management Services:</b> <ol style="list-style-type: none"> <li>i. Database Monitoring</li> <li>ii. Application Monitoring</li> <li>iii. Server health &amp; performance Monitoring</li> <li>iv. Access Control</li> <li>v. Network Monitoring</li> <li>vi. Incident Reporting</li> <li>vii. Asset Management</li> <li>viii. Support.</li> </ol>	



## 2. Background and Mission

**West Bengal State Data Centre** is a key-supporting element of e-Government Initiative provided by the Govt. of West Bengal for facilitating and strengthening the centralised Information Technology enabled Services related opportunities and establishments with



greater security, reliability, availability and serviceability to consolidate services, applications and infrastructure to provide efficient and quality service delivery environments for the Line Departments and also to the other users related to G2G, G2C and G2B services more efficiently and effectively.

- 3.1** It acts as a mediator and convergence point between open unsecured public domain and sensitive government environment. It enables various departments to host their services / applications on a common infrastructure leading to ease of integration and efficient management, ensuring that computing resources and the support connectivity infrastructure (WBSWAN) is adequately and optimally used.
- 3.2** WBSDC is equipped with a centralized and integrated monitoring system both for IT and NON-IT infrastructure with appropriate fire fighting and alarms and supported by DG. It supports many functionalities e.g. Central Repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc.
- 3.3** It Facilitates users intending to set up their own exclusive environment within the ambit of WBSDC. In case Departments are using repository of Servers at the District level, the WBSDC in such case may act as a central repository for consolidation of the disaggregated resources.

### 3. Purpose & Scope

This Information Booklet is articulated to keep Line Department (LD) s and other stakeholders well-versed with comprehensive information of the presence, composition and the services of the WBSDC vis-à-vis e-Gov infrastructure including its Policies, Standards, Norms, and generalized Agreement for the Line Departments. This working document is prepared to keep track of the addition and alterations in infrastructure, services and processes required to fulfil the expectations of Stakeholders. The abbreviations used in this document are listed in [Annexure-IV](#). The ultimate objective is to maintain transparency of the Government endeavour among the stakeholders by presenting clear & concise document.

The scope of this document takes account of all the Line Departments of the Government of West Bengal and all other Stake holders who have direct or indirect business needs to WBSDC and will be using the resources of e-Gov infrastructure. This document consists of an overview of e-Gov Infrastructure, services, simplified architecture, SDC connectivity, policies, procedures and standards along with provisions of different service options, hosting models for Government Departments. It also elucidates the benefits of application hosting in SDC & simplifies the procedure of joining SDC for the LDs. The scope also describes WBSDC's presence, capability and connectivity to SWAN and Internet.



## 4. Why SDC

West Bengal State data centre is envisioned to facilitate the Line Departments / Public Sector Units to host and manage their software applications for Citizen, Business and Government services online through use of a common centralized system of latest state-of-art Information and Communication Technology.

Having such common facility for all, on the other hand, if any Department intends to host their application in their own setup, the same would be expensive proposition in many ways as follows:

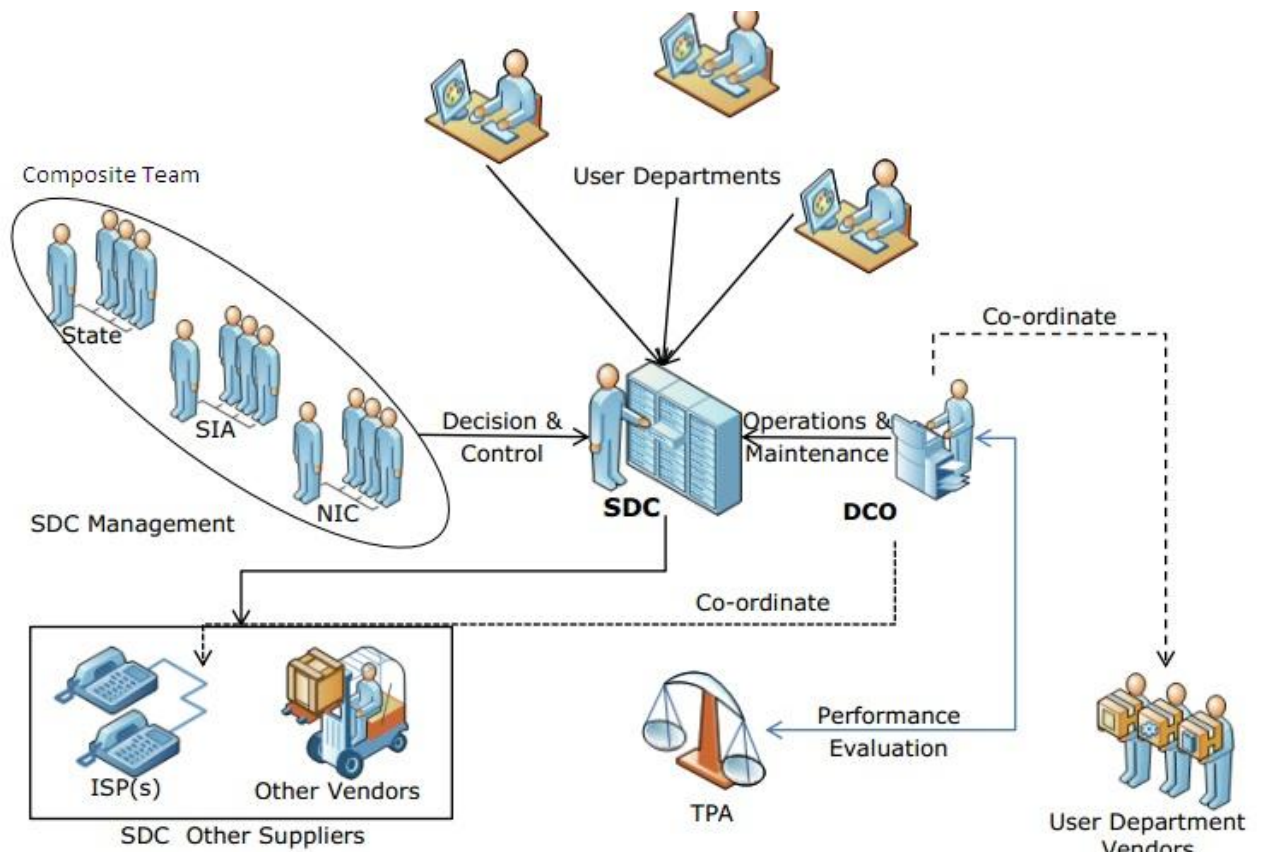
- I. High initial investment for preparation of setup including space, power supply, cooling facilities and other equipments
- II. High day-to-day management costs
- III. Hiring and retaining personnel to maintain the data centre
- IV. High cost of upgrading technology and acquiring newer services
- V. High cost in training/hiring professionals to maintain computing resources

In this scenario, **Government of West Bengal having 52 departments each having in-house data centres will replicate the above cost which in turn will become a major financial burden for the department as well as the Government to manage all the 52 data centres individually. So,** it is far more economical to share such a common high-end infrastructure to accommodate all the Government applications thereby minimizing the cost of maintaining & managing server, storage, network & other computing resources. Hence, Departments can easily outsource these services to host their application in the above mentioned collocated environment. Collocation offers several business advantages with regard to time and money as follows:-

- a) **24\*7 Power backup:** WBSDC is powered through a separate substation with two different sources of grid power supplies supported with multiple generator sets
- b) **Better utilization of space:** Collocation in SDC will help the Departments efficiently utilize the office as they don't need to bother about owning separate server farm area.
- c) **Precision controlled environment** having optimum temperature & humidity.
- d) **Physically secured infrastructure** by biometric access control system & security personnel employed.
- e) Having the benefit of **SDC's inbuilt sturdy building management system** including fire detection & suppression system, rodent repellent system, smoke detection system, water leak detection system.
- f) **Freedom from Maintenance & Management issues:** To focus on your core competencies of application development instead of worrying about managing & maintenance issues of IT infrastructure.
- g) **Robust Network infrastructure** with redundant firewalls, IPS, HIPS, Antivirus.
- h) **Greater network redundancy** means maximum up time: ensuring applications will always be up and accessible. This is because data centre have bandwidth support from multiple ISPs.
- i) **Centralised operation** provides ample support and security for the IT concerns of a Department.
- j) **Technical Support Advantages** avoid problems of deploying human resources and can expect the highest levels of dedicated service.
- k) **Cost reduction regarding training/hiring qualified technical personnel** – with certifications like CCNA and MCSE – who monitor your networks and server 24x7 and prevent an impending problem from blowing up into a crippling crisis.
- l) **Guaranteed level of services** – better than what you would have in-house through a Service Level Agreement (SLA).
- m) **Help desk facility:** You also get a 24x7 help desk to contact in case of any trouble.

By utilizing collocation services in a data centre facility, Departments will realize an immediate benefit in terms of costs saving, improved redundancy & 24\*7 Service assurance.

## 5. SDC's Operational Vision



WBSDC Stake Holders include:

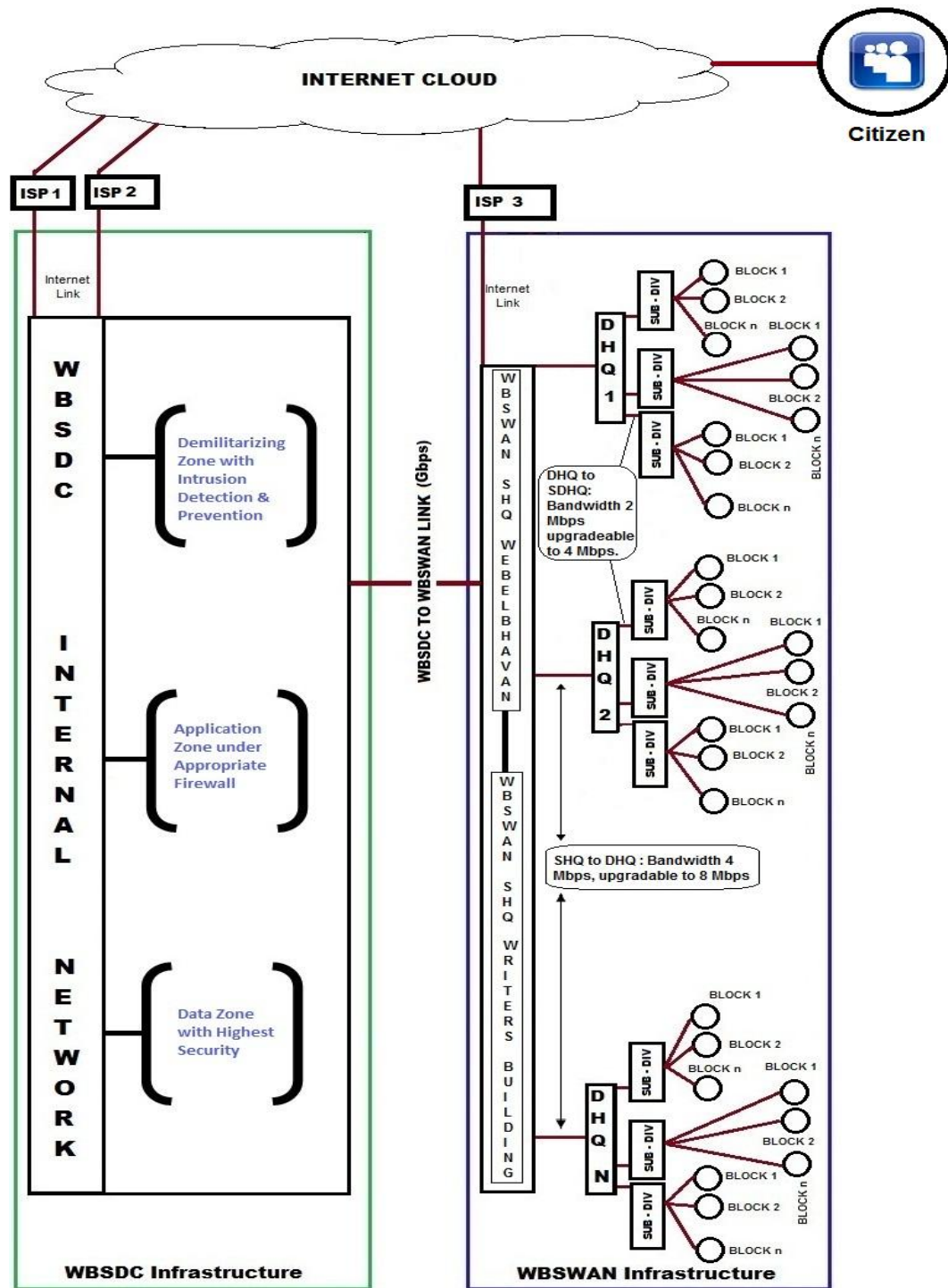
- A. **Department of IT (DIT), Govt. of India** -Scheme execution Agency for SDC, Technical & Financial support to States, Program Management & Monitoring at Central level.
- B. **State Implementing Agency-** Implementation & Management for SDC
- C. **SDC Consultant-** Supports SIA for SDC planning (DPR and RFP preparation, bid management) SDC Project Management & Monitoring for the Implementation duration
- D. **Data Centre Operator-**Implementation, Operations & Maintenance of SDC for project duration

- E. **Third Party Auditor-** For SLA and Inventory Audits for O&M period of SDC scheme for QGR payments to DCO
- F. **STQC-** Audits & Certification, and Monitoring of TPA
- G. **NIC-** Composite Team Project Manager and team members of Composite Team, and DR provisioning

**Composite Team:**

- A. Dedicated deployment for NeGP
- B. Interface between State & User Department
- C. CT facilitated under SDC fund
- D. Visibility in all stages of projects
- E. Policy Management across State Services
- F. Roles & responsibilities growing with time
- G. Equipped with Industry Best Practices

## 6. WBSDC Connectivity



**West Bengal State Wide Area Network** is the backbone network for data, voice and video communication throughout the state of West Bengal and this Government Intranet, through which e-Governance activities of the Government of West Bengal are being undertaken, is based on IP (Internet Protocol) technology.

#### **Salient features of WBSWAN:**

- ➔ WBSWAN network provides connectivity of Data, Voice & Video Communication facilities from State Switching Centre at Kolkata up to all District Headquarters as well as some important cities on 2 Mbps (E-1 link) leased line of BSNL.
- ➔ WBSWAN Network infrastructure is having its Two separate State Head Quarters (one is in the premise of the WEBEL Bhavan, WBEIDC, Block EP & GP, Sector – V, Salt Lake and the second one is in the Writer's Building, B.B.D Bag, Kolkata.). These two State Head Quarters are also interconnected to ensure redundancy, uptime and better services to be provided to all the stake holders.
- ➔ State Head Quarter to District Head Quarter: Bandwidth 4 Mbps upgradable to 8 Mbps. District Head Quarter to Sub Divisional HQ: Bandwidth 2 Mbps upgradeable to 4 Mbps.
- ➔ State Capital as well as each District Headquarter has Video Conferencing, Multi-conferencing facility through Multipoint Conferencing Unit (MCU) at Kolkata.
- ➔ Provision for horizontal expansion for connectivity at all levels.

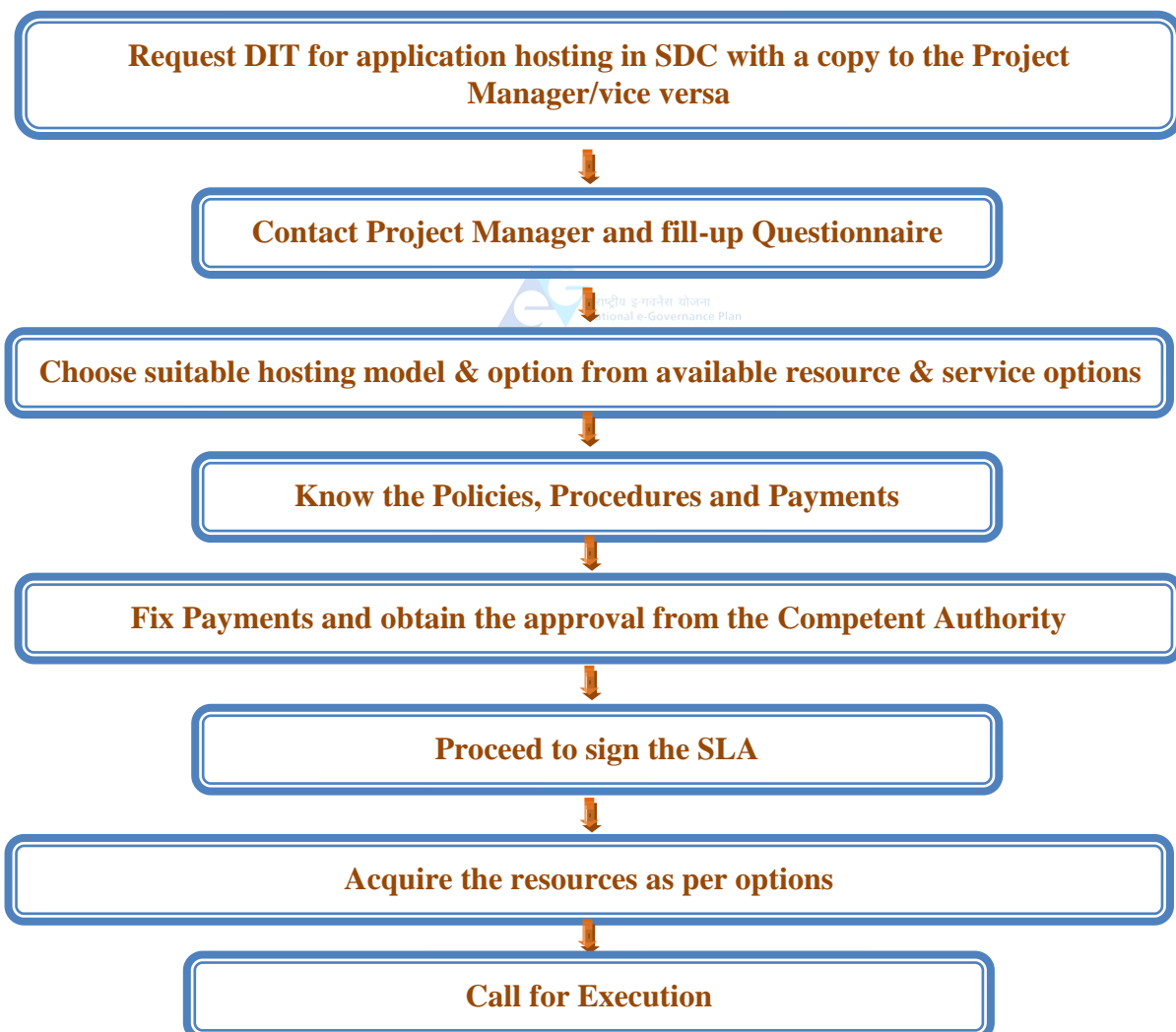
#### **WBSWAN services & applications:**

- ➔ This Intranet is aimed at providing seamless connectivity among Government departments / directorates as well as among the various offices of each department / directorate all over West Bengal.
- ➔ Government Application Service Provider (ASP) project will be based on this network.
- ➔ Improve the Government-Citizen and Government-Industry interface as well as efficient Intra-Government information flow resulting in effective, efficient and transparent administration.



## 7. How to join WBSDC..

Line Departments (LD) may contact the Project Manager, Composite Team, NeGP for necessary details towards participating in WBSDC. The LD will be provided with the hosting models along with different service options. LD may choose an appropriate hosting model and service options, while receiving required clarifications. As per the service option opted LD needs to make arrangement to supply associate hardware and software required for the model as chosen. Once the details of resources and services to be dedicated and / or shared from the LD's end are finalized, they are required to sign an agreement with DIT to proceed further. For easy understanding of the joining process refer the diagram given below:-





## 8. WBSDC Infrastructure

**WBSDC**, a tier-II level Data Centre with 99.749% uptime is well equipped with redundant power, sufficient cooling accommodation for collocating servers, multiple Internet links, common servers, storage with high availability. It is ready to host applications and co-locate systems of Government departments ensuring effective utilization of centralized computing resources in a secure environment. A simplified architecture is enclosed as [Annexure III](#).

### DIT Approved Components

Racks (Server, Network)

Servers (Application, Database, Web)

SAN Storage (in TB)

Tape Library (Cartridges)

Software and Licenses (Antivirus, HIPS, EMS, Backup)

### SDC Features

Tier-II DC Compliant : 99.749% Availability

Infrastructure Redundancy (Network, Power, Security)

ISO 27001 / 20000, TIA 942 Standards Compliant

Security- (Physical, Biometric, Video Surveillance)

BMS, EMS, online back up, VTL

## 8.1 Physical Infrastructure NON-IT:

WBSDC Physical Infrastructure is designed with sufficient redundancy to prevent catastrophic failures. Following are the brief details of its components.

- b) Power Supply:** It is powered through a separate substation with 3-Phase 415 V Grid Power with two different sources of power supplies, three redundant (3) uninterrupted power supply systems of 160 KVA each in unified load balancing mode supported by three (3) diesel generators of 380 KVA each connected in auto sensing and synchronized mode.



- c) Air Conditioning:** Data Centre requires round the clock 365 days precision cooling to maintain temperature of  $22 \pm 2$  Deg. C and relative humidity of 50 % RH. WBSDC is equipped with cooling capacity of 66 TR (3 x 22TR) with 1 PAC standby to maintain a balanced and appropriate environment for optimal systems operations of Computer hardware.



- d) Building Management system (BMS):** WBSDC's Building Management System monitor the entire critical infrastructure(24\*7) and protect the data centre from Fire, unauthorized entry and surveillance in all areas. This BMS panel is integrated with various other critical components of the data centre such as: Fire Alarm System, Main LT Panel Energy Meter etc.

- e) **Fire prevention:** WBSDC is equipped with fire detection and suppression system which has been designed and installed as per **NFPA 72 and IS: 2189**. An automatic fire detection system is designed to detect a fire in its incipient stage and to automatically initiate pre-programmed control functions.
- f) **Biometric Access control system:** It provides computerized control over entry to any area that demands highest security possible to ensure data and information protection from external threats. Biometric Device ensures that only a person with a registered authentic identification is permitted to enter high security areas. The device / system scrutinises a primary, unique and physically inseparable biometric characteristic (fingerprint, voice, etc.) of an entrant for the purpose of authentication. All high risk areas in WBSDC are equipped with biometric access control system having three layers of security checking in terms of swiping contact less smart card reader, fingerprint scanning and passwords authentication.
- g) **CCTV surveillance:** WBSDC's Closed Circuit Television (CCTV) System ensures effective surveillance of each nook and corner of the entire floor space and creates a record for post event analysis. The system is also capable of continuous on-line monitoring of events.

The video output from individual camera locations is available on the high resolution monitors via Digital Video Recorder (DVR), which is capable of handling multiple camera, continuous motion detection, alarm, pre alarm handling and schedule recording modes, ***Recording up to 25 images per second per channel***, high speed searching well-equipped with back-up management and external storage device.

**h) Public Address System:** It serves the dual purpose of making general announcements as well as to alert the users present in the floor at that point in time by making a special tone under critical conditions that demands attention. Speakers are capable of broadcasting superior quality, integrated emergency critical alarm signals and voice communications with high efficiency yielding maximum output at minimum power across 200 – 12000 Hz frequency range.



**8.2 Network and Security Infrastructure:** WBSDC's Network Infrastructure having compatibility with both the internet protocol versions, IPv4 and IPv6, consists of Internet Gateway Router, Firewall (External and Internal), IPS/IDS, HIPS, Server Load Balancer, Switch (Core, Application, and DMZ).



**a) Internet router:** WBSDC Network Infrastructure is equipped with high-end branded integrated redundant services routers which is capable of integrating security, application layer functions. The routers provide intelligent network services, converged communications and support the bandwidth requirements for multiple Fast Ethernet interfaces per slot. It integrates a comprehensive set of security features such as **firewall, IPSec and Secure Sockets Layer (SSL) VPN, intrusion detection and prevention system** along with other key features like increased default and maximum memory for future services growth, advanced service interfaces (network analysis, IDS, content engine), integrated hardware for encryption services processing that supports **IPSec DES, AES etc. encryption modes** without the need for separate modules.



- b) Network based IPS:** Intrusion Prevention appliance is placed transparently in the network to provide vulnerability-based protection through proactive signature updates with protocol anomaly and rate limit for prevention of already known attacks.

It can monitor up to **9 network segments** and can transparently scan the network traffic ensuring that there are no routing changes in the network. It **scales up to 4 Gbps with maximum concurrent sessions up to 40,00,000.**



- c) Firewall:** Redundant External Firewalls are positioned to protect the internal system infrastructure from the Public Internet and act as a first line of defense for the applications hosted in the data centre.

Their unique combination of ASIC-accelerated performance, integrated multi-layered security solutions, and constantly-updated, in-depth threat intelligence delivers the highest level of network, content, and application security with **Maximum Firewall Throughput of 7 Gbps / 37 Gbps and Maximum IPSec VPN Throughput of 1 Gbps / 19 Gbps.**

Further redundant internal firewalls are placed to provide more secured, robust and threat free infrastructure. Attacks which are not detected by external firewall and IPS can be stopped by internal firewall before hitting Database server with firewall throughput ranging from 5 Gbps (real-world HTTP) to 10 Gbps (max), maximum firewall connections of 90,000/sec, maximum 3DES/AES VPN Throughput of 1 Gbps.

d) **Core Switch:** It offers a high-performance platform on which services from the network to the applications level can be enabled for every port. It supports **720 Gbps of throughput with up to 400 mbps of forwarding capacity** with capability to add a variety of security, WAN, voice and L4-7 services. The switch is populated with 4nos of 48 port 10/100/1000BaseT line cards and a single 24 port fibre module.

e) **Application Switch:** WBSDC is equipped with Redundant Application switches for maximum productivity, integrated security, optimised delivery, and manageability and investment protection while enabling the deployment of new applications such as IP telephony, wireless access, video surveillance, building management systems, and remote video kiosks.



f) **DMZ:** Demilitarised Zone or DMZ refers a physical or logical sub network that contains and exposes WBSDC's external services to a larger untrusted network i.e. Internet. It adds an additional layer of security to local area network (LAN); so that an external attacker only has access to equipment in the DMZ, rather than any other part of the network. It is connected between gateway firewall and Core switch to monitor the traffics that allowed by firewall.

- g) Server Load Balancer:** The load balancer is introduced for distributing work loads to a set of networked computer servers in such a manner that the computing resources are used in an optimal manner. It supports segmentation/virtualisation to distribute load for multiple services, servers, thereby increasing the availability of the server as well as improves performance.



- h) HIPS:** Host based Intrusion Prevention System is an agent, which will be installed on all critical servers and managed by central management server to push the policy, updates and display the real time logs based on the Operating Systems (OS) and applications running on the server. It monitors and blocks the traffic that are targeting on OS and application.
- i) Antivirus:** Antivirus provides multiple layers of protection, messaging security, web, data loss prevention, and data and system recovery vendor. Automatic controls helps to achieve, prove, and enforce adherence to IT policy and regulatory objectives with ease. Simplified implementation & operations by quickly deploying with minimal disruption to your environment through easy management and optimized utilization of system resources. Centrally manages backup and recovery tasks for multiple desktops/laptops/servers across entire organization.

It instantly protects threat with support from the largest Global Intelligence Network in the world along with comprehensive virus protection against malicious threats that target Windows, Linux and Macintosh systems.

- 8.3 Server Farm Infrastructure:** WBSDC's 1489 Sq. ft. Server Farm Area can accommodate up to 42 Racks among which few racks are already in place having Staging Server, Web / App / Database Server, Management Server, DNS / Directory / Antivirus / Backup Server with high end specifications viz. high Performance Xeon® technology, 6 Core Processor (2.67 GHZ , 16MB Level 3 cache), DDR3 RAM expandable up to 256GB , support for multiple disks hot plugability, and multiple embedded NC373i Multifunction Gigabit Network Adapters with TCP/IP Offload Engine.



- 8.4 Backup and Storage:** Regarding Storage the current infrastructure is capable of using both State-of-Art SATA and FC technology and can be scalable up to 960 disks. Storage could also be connected with the Servers with redundant channels to minimize the risk of Server-Storage Connectivity Failure at its most.

The Backup Architecture is flexible to meet recovery-time and recovery-point objectives faster, more-reliable backup and recovery.

- 8.5 Software:** WBSDC is equipped with multiple Operating System platforms like Windows 2008, Linux Enterprise Edition 5 to extend its support for applications of both Linux & Windows Platform. Staging Environment, supported by multiple OS, is created using powerful virtualisation technology for patch upgradation & testing purpose. Database software like Oracle 11g, MS SQL Server, MySQL etc are available. EMC NetWorker is used as backup software.

**8.6 Health Monitoring:** Overall Performance Monitoring of WBSDC Infrastructure, Network Fault Management, Database and Application Management, Real Time Report Generation, Server Health Monitoring, Help Desk, Incident Reporting etc. covered over a period of 5 years with 99.749% uptime. It includes:



- a) Better management of historical records and reports of network devices and servers.
- b) Real time reports/alerts of server and network devices.
- c) Access related detailed record of servers.
- d) Asset management record of servers.
- e) Application and Database performance management.
- f) Incident Reporting regarding abnormality of server or network devices.
- g) Help Desk Service to coordinate with users.







## 9. Policies

A Policy can be considered as a Statement of Intent or a Commitment. It is typically described as a principle decision to achieve rational outcome(s). Policies are generally adopted by the governance body whereas procedures or protocols would be developed and adopted by senior executive officers. In this context, the term applies to Government, public sectors, private sector organizations and groups, and individuals. We have considered the following policies for effective utilization and better management of the WBSDC resources:-

### List of Policies:-

- 9.1 Physical Access Control Policy
- 9.2 Network Security Audit Policy
- 9.3 Backup Policy
- 9.4 Server Security Policy
- 9.5 Firewall Policy
- 9.6 Audit Log Policy
- 9.7 Portable Media Usage Policy
- 9.8 Remote Access Policy
- 9.9 Password Policy



## 9.1 Physical Access Control Policy

### 9.1.1 Purpose

The purpose of this policy is to provide direction and guidance to assist WBSDC users in maintenance and management of access control system. The Access Control Policy is a living document that will be modified and updated as needed.

### 9.1.2 Scope

Security for the State Data Centre is the responsibility of all WBSDC users who are sharing the data Centre space. “**Physical Access Security**” defines a system that restricts access to a facility based on a set of access control parameters. Access control systems include card reading devices of varying technologies and evidentiary cameras. The following are the general policies, and practices that govern access to this sensitive area. This document provides mainly access control guidelines for different WBSDC users. Failure to maintain these can be considered grounds for personnel action as per the provisions of Information Technology Act. Failure of a vendor, consultant, or contractor to follow the guidelines set forth in this document will have ground for termination of agreements and potential legal action.

### 9.1.3 Types of Policy

#### 9.1.3.1 Access Authorization Request Policy:

Access privileges will only be granted to individuals who are either WBSDC staffs or have a legitimate business need to be in the data Centre. A central point of contact should be assigned for each data Centre. These contacts should be delegated by the responsible Project Manager, e-Governance Infrastructure claiming responsibility for the physical area, and maintenance thereof.

#### 9.1.3.1.1 Requesting Access

An individual requiring physical access to a restricted area should obtain the necessary forms referred in [Annexure-II \(B and C\)](#) for limited purpose (supervisory access) access to the WBSDC depending on the requirements. Access request can be submitted in the either of the following ways:

- A. The access request application forms should be duly filled up, signed and submitted to the project manager-e-Gov.
- B. Online access request can be made by submitting the scanned application form (duly filled up & signed) by email to [projectmanager.egov@wb.gov.in](mailto:projectmanager.egov@wb.gov.in).
- C. Directly access request email can be sent to [projectmanager.egov@wb.gov.in](mailto:projectmanager.egov@wb.gov.in).  
(Please refer [Online SDC Access Request](#) section for details.

Access to WBSDC area will only be granted after verification and authorization by the project manager, e-Gov.

#### 9.1.3.1.2 Reservation of Access Rights

Each responsible entity for a data Centre should agree to the disclaimer that access to the secured area may be revoked temporarily or permanently for any reason, at any time at the discretion of the Project Manager. Each applicant or WBSDC user should go through the general guidelines for access rights while requesting for any type of access to the secured area.

#### 9.1.3.1.3 Emergency Access

Emergency access to the WBSDC without having appropriate identification and access right is not permitted. Each resource does have primary *authorized* personnel and secondary *authorized* personnel ready “on call” to respond to a situation at all times. Proper contact information is developed to avoid emergency access completely.

The only exception allowed to the Data Centre Security Policies and Practices is temporary suspension of these rules if it becomes necessary to provide emergency access to medical, fire and police officials.

### 9.1.3.2 General Guidelines

Each access to the data Centre should be made in compliance with the following guidelines in order to have secured and prolonged existence of systems.

- a. The members of the Composite Team and the Sustenance Team will be treated as the regular users of the WBSDC floor space.
- b. Any other incumbent will be treated as guests and will be given supervisory access for specific business.
- c. Project Manager will have and maintain a list of regular members of both the Composite Team and Sustenance Team.
- d. Proximity cards and secret PIN Code should not be shared between authorized and unauthorized persons.
- e. Vendors, or those wishing to access WBSDC for a specific task, must carry identity cards and appropriate authorization with them.
- f. Under any circumstances any portable devices like laptop, palmtop, camera and media like USB-like devices / CDs / DVDs as well as personally-acquired or owned non-SDC computing devices/Laptops are not allowed without proper authorization. These devices should not be plugged into a data Centre network port without prior approval from the Access Control Authority.
- g. The secured area should only be accessed to meet a business requirement. When such a requirement is met, users should leave the area without loitering in the WBSDC premises.
- h. Any software or hardware resource in the WBSDC (computer, monitor, keyboard, network cable, power cable, cabinet, floorboard, etc.) should be moved only by the person directly responsible for that resource.
- i. Entry in the WBSDC with mobile phone is restricted for all with supervisory access and hence usage of the same is limited to conversation related to the business of WBSDC only.
- j. Food, drink or other fluids must not be introduced to the secured areas. These items promote deterioration of computing hardware through moisture.
- k. All doors to the Data Centre must remain locked at all times and may only be temporarily opened for periods minimally necessary by the Security staffs.

- I. Physical security audit shall be done after certain intervals.

### 9.1.3.3 Levels of Access to the Data Centre:

There are two “Levels of Access” to the Data Centre - Controlling Access and Supervisory Access.

#### 9.1.3.3.1 Controlling Access

**Controlling Access** is given to staffs whose job responsibilities require that they have access to the area. These individuals also have the authority to grant temporary access to the Data Centre and to enable others to enter and leave the Data Centre. People with Controlling Access are responsible for the security of the area, and for any individuals that they allow into the Data Centre. If a person with Controlling Access allows Supervisory Access to an individual, the person granting access is responsible for escorting the individual granted access and seeing to it they sign in and out. Any individual receiving Controlling Access must go through a formal background check. Sharing of access cards without authorization of Project Manager is a punishable act. **Composite Team and sustenance team members only will be considered as staffs and eligible for controlling Access.**

#### 9.1.3.3.2 Supervisory Access

**Supervisory Access** is closely monitored access given to people who have a legitimate business need for infrequent access to WBSDC. They should produce proper identity card to get the temporary visitor card.

A person given Supervisory Access to the area must sign in and out under the direct supervision of a person with Controlling Access. They must also display their issued Visitor Identification Card at all times. A person with Supervisory Access to the area must not allow any other person to enter or leave the area. Visitor Identification Card must be returned before leaving the area. They are not allowed to use any portable media devices as a normal rule.

**Government Officials, Line departments’ personnel who have proper collocation agreement, service providers and / or vendors will be considered**

**as visitors and will be given supervisory access.** Persons having specific business in the highly secured zone like Server Farm, Power supply will be given limited supervisory access. Persons having controlling access will be considered responsible for any damage, change in configuration, and data loss etc due to the persons given supervisory access by him/her.

#### 9.1.3.4 Visitor Management Policy

Visitors to WBSDC can be classified in three categories: Official Visitors related to WBSDC, Official Visitors not related to WBSDC and Personal Visitors.

- a) Official visitors related to WBSDC should be entered in WBSDC with supervisory access depending on the requirement. But this access needs prior approval of the Project Manager, e-Governance Infrastructure assigned for access control.
- b) But, neither the Official visitors (not related to WBSDC) nor the Personal visitors are allowed to enter WBSDC. They should either wait in the Discussion room/ Reception.



#### 9.1.3.5 Collocated Servers

- a) Servers with proper procurement documents and not more than 3 yrs old will only be accepted under proper agreement.
- b) In both the cases Maintenance personnel/Service Provider will enter in Data Centre with Supervisory Access under the supervision of DCO /Composite team members.
- c) Any damage/configuration changes done by LDs can cause breach of co-location agreement.



### 9.1.3.6 Access Control Log

The Data Centre Access Control Log must be properly maintained at all times.

- a) A register should be kept for “sign-in” to the area. This register should record a name, organization, employee identification number, time in, time out, and signature.
- b) Logs should be maintained on every entry and exit and duly signed.
- c) Separate Register should be maintained on highly secured areas where all entries should be recorded and reviewed by the responsible security personnel as assigned by Access Control authority/ Project Manager for the area. All access should be logged, even when a group of persons enters the area.
- d) Each time an individual with Supervisory Access to the Data Centre is admitted to the area, he must properly log in on the Access Control Log at the time of entrance. The person admitting the visitor must countersign and fill out the appropriate section of the form. If they enter with any portable media/ personal laptop it also needed to be mentioned in the register.
- e) Each time an individual with Supervisory Access leaves the area, he must properly log out on the Access Control Log at the time he leaves (even if only for a short time). The person with Controlling Access to the area who allows the visitor to leave must ensure that the “Log Out” section of the Access Control Log is properly filled in.

### 9.1.3.7 Periodic Review and Termination/Revocation of Access:

Periodic (monthly) reviews will be performed of those with any level of access to the Data Centre. If an individual no longer requires Data Centre access, it will be revoked.

Procedures for terminating or revoking Data Centre access include:

- a) Collecting the Card.
- b) Removing name from the Authorized Access List.
- c) Cancellation of the card in case of card-loss reported/ not returned on request.

The results of periodic reviews will be reported to the Project Manager, e-Governance Infrastructure. The report will include an updated list of those allowed access to the Data Centre.

#### **9.1.3.8 Exception Reporting**

When an unauthorized individual is found in the Data Centre it must be reported immediately to proper contact personnel. If this occurs during the non-working hours, a Senior Operator or the Operations Manager should be contacted. The unauthorized individual should be escorted from the Data Centre and a full written report should be immediately submitted to the Project Manager, Composite Team, e-Governance Infrastructure. Any attempt to forcibly or improperly enter of the Data Centre should be immediately reported to the security personnel, who should deal with the situation. Individuals with *Controlling Access* to the area are to monitor the area and remove any individual who appears to be compromising either the security of the area or its activities, or who is disrupting operation. It is particularly important that individuals with *Controlling Access* show initiative in monitoring and maintaining the security of the Data Centre.

#### **9.1.3.9 Escalation**



The Operation Manager, DCO have overall responsibility for the administration of these policies and procedures. If he/she is unable to resolve will be escalated to the Project Manager, Composite Team, e-Governance Infrastructure as appropriate.

#### **9.1.4 Enforcement**

All staffs as well as visitors must aware of this policies and follow it. Failure to comply with this policy may result in revocation of access to all WBSDC managed facilities and appropriate staff disciplinary action. If an individual fails to abide by the data Centre policies and procedures, the Project Manager or assigned Authority by him is responsible for reviewing and revising that individual's access privileges. Any Person found to have caused damage / unauthorized configuration changes / unauthorized use of portable media devices will be punished under the provisions of IT ACT.

## 9.2 Network Security Audit Policy

### 9.2.1 Purpose

The purpose of this policy is to verify the compliance of the Security Policies.

### 9.2.2 Scope

This policy applies to all e-Governance committee.

### 9.2.3 Policy

- a) The network security audit shall be carried out at least once in a year.
- b) The security audit shall verify the compliance of the security policies.
- c) The security audit shall involve risk assessment.
  - I. Vulnerability assessment of the systems and devices
  - II. Non- intrusive External Penetration testing
- d) The security audit shall identify the gaps against best security practices.
- e) The security audit shall suggest modification to the security policies based on the risk assessment and best practices.
- f) SDC Administration or authorized persons/organization to carry out security audit.
- g) Audit SAN in terms of securing from internal threats such as authorised and unauthorised staff from misconfigurations and human error.



### 9.2.4 Enforcement

Any found to have violated this policy may be subjected to disciplinary action under the provisions of IT ACT.

## 9.3 Backup Policy

### 9.3.1 Purpose

In a Data Centre, a backup or the process of backing up refers to making copies of data so that these additional copies may be used to restore the original after a data loss event. These additional copies are typically called 'Backups'. Backups are used primarily for two purposes. The purpose of this policy is to provide direction and guidance in taking backup of computer facilities and systems. The Backup policy tells us the means of Securing Backup Files. Further, Up-to-date backups of all critical items shall be maintained to ensure the continued provision of minimum essential services.

### 9.3.2 Scope

WBSDC has provisioned for SAN Storage, Tape Library, Enterprise backup Server and Backup Software to facilitate data backup in WBSDC. The backup software and licenses have been provisioned to meet the initial requirement.

Backup Policy may help in the restoration of system functioning in the event of any casualty of system break down. It describes the methods for recycling, destruction, erasure and re-use of security backup files.

### 9.3.3 Types of Policy

#### 9.3.3.1 General Data Backup Mechanism

- a) Up-to-date backups of all critical items shall 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.
- b) Back-up procedures shall be documented, scheduled and monitored.

- c) Media should be made available for taking backup of one set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
- d) Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.
- e) The Systems backups shall consist of regular full and incremental backups.
- f) Establish overall system backup responsibilities and assign them.
- g) Backups of the system, application and data shall be performed on a predefined procedure. Backups for application under development are the sole responsibility of the application development team as per recommendation of competent authority.
- h) Critical system data and file server software should have incremental backups taken daily and full backups taken weekly
- i) The backups should be kept in an area physically separate from WBSDC. If critical system data on the LAN represents unique versions of the information assets, then the information backups should be rotated on a periodic basis.
- j) Data backup is required for all systems including servers and distributed systems and databases.
- k) Media rotation mechanism should be used. (Using different disks/tape at each backup and rotating every 2 weeks).
- l) For safety reasons media backup should be taken in duplicate as per availability of backup media.

- m) Backup tapes should be disposed whenever tape starts displaying error in such a way that the stored information should be irretrievable.
- n) All backup storage media should be labelled clearly with relevant information.
- o) Tape and log books should be maintained to include a record of subject, type of back up, time, operator etc..
- p) Each critical LAN/System should have a primary and backup operator to ensure continuity of business operations.
- q) Business continuity/ disaster recovery plan will be detailed as and when notifications available from Gol. It entitles all backups should be mirrored in a different **seismic zone** to avoid data loss due to natural disasters.

#### 9.3.3.2 System Data/Registry Backup



- a) Regular backup of System and registry files should be taken to ensure system configuration and settings recovery.
- b) The systems backup shall be able to restore the integrity of computer systems in the event of hardware/software failure or physical disaster.
- c) The Backup mechanism shall provide a measure of protection against human error or the inadvertent deletion of important files.
- d) Create an emergency repair diskette of the relevant operating system.



### 9.3.3.3 Database Backup

- a) The backup of relevant databases shall be taken up regularly. The database backup shall be taken in either full or incremental pattern.
- b) The backup of the database shall be checked to ensure that all tables and data of the database are restored.

### 9.3.3.4 System Log Backup

- a) The backup of log files of critical systems should be periodically undertaken
- b) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.
- c) System access records should be kept for a period of time as per the decision taken by the competent authority, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.
- d) System records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.
- e) It is advisable that every log backup is stored in different media devices.

### 9.3.3.5 Media Management

- a) Responsibilities for media library management and protection shall be clearly defined and assigned.
- b) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals based on the availability of fireproof cabinet.
- c) Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorised to enter the library shall be maintained.
- d) The media containing sensitive and back up data should be stored at a different physical location other than WBSDC.
- e) As the no. of media is considerably large in line with this policy, responsibility should be assigned properly for accounting of media.
- f) All incoming/outgoing media transfers shall be authorised by management and users.
- g) An independent physical inventory check of all media shall be conducted at least every six months.
- h) All media shall have external volume identification. Internal labels shall be fixed, where available.
- i) Procedures shall be in place to ensure that only authorised addition/removal of media from the library is allowed.

- j) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

#### 9.3.3.6 Media Movement

- a) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.
- b) There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.
- c) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

#### 9.3.3.7 Disaster Recovery/Management

- a) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided.
- b) The disaster recovery framework should include:
  - I. Emergency procedures, describing the immediate action to be taken in case of a major incident
  - II. Fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site
  - III. Restoration procedures, describing the action to be taken to return to normal operation at the original site

- c) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.
- d) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster

### 9.3.4 Backup Retention Period:

- a) 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.
- b) Monthly Backups should be retained for a period for at least One year.
- c) Yearly Backups should retain for at least two years.

### 9.3.5 Responsibilities



- a) All administrators and users are responsible for keeping up-to-date backup of all critical items to ensure that essential services can be restored.
- b) The retention period of backup of all critical items should ensure that latest backup data is stored.

## 9.4 Server Security Policy

### 9.4.1 Purpose

The purpose of this policy is to establish standards for the base configuration of internal servers that are owned and/or operated by WBSDC. This is to assist WBSDC Administration in understanding the fundamental activities performed as part of securing and maintaining the security of servers that provide services over network communications as a main function. This document provides recommendations for implementing, and maintaining the necessary security controls.



### 9.4.2 Scope

This policy applies to server(s) owned and/or operated by State Data Centre and to collocated servers under State Data Centre network domain.

### 9.4.3 Audience

This document has been created primarily for system administrators and security administrators who are responsible for the technical aspects of securing servers. The material in this document is technically oriented, and it is assumed that readers have basic understanding of system and network security.

## 9.4.4 Policy Details

### 9.4.4.1 Ownership and Responsibilities

All internal servers deployed at WBSDC must be owned by an operational group (e.g. data centre) and/or administrators who shall be responsible for System Administration of these servers. Operational group or administrators should monitor implementation and compliance of policy tailored to their environment.

- a) All servers not under the direct ownership of the respective data centre must be identifiable to a particular group and/or administrator.
- b) Configuration changes for production servers must follow the appropriate procedures of individual servers that are prepared by the respective administrator/owner.

### 9.4.4.2 General Configuration Guidelines



- a) Servers shall be physically located in an access-controlled environment.
- b) WBSDC should implement **Server Hardening** in respect of the particular service/application being used to host a specific application. It should be identified by the application development team based on that rest all unnecessary Services, applications, network protocols, default user accounts, manufacturers' documentation etc. including sample content, scripts, and executable code must be removed/disabled in compliance with **STQC Hardening guideline**.
- c) **Remote Administration on servers from uncontrolled areas should usually be prohibited.** However, remote administration of servers where required, it should be allowed only after careful consideration of the risks and in accordance with the **Remote Access Policy**.



- d) **Staging Server** has been implemented with multiple OS environment for each user/stakeholder. All applications must be tested in staging prior to expose in Production Environment. A partially configured and/or patched server should not be exposed to external networks (e.g., the Internet) or external users. In addition, internal network access should be as limited as possible until all software is installed, patched, and configured securely and tested successfully in Staging Environment.
- e) All newly released system software patches, bug fixes and upgrades shall be expediently and regularly reviewed and installed on the web, the only exception being when immediate application of patches will result in denial of service. All patches need to be tested on the staging server first and based on the observation can be pushed to production following approval. Staging Server needs to be identical with the production environment.
- f) Anti-virus agent should be installed in all the Servers in WBSDC Network and updated properly by a Central Management system to ensure Network Security.
- g) Server time shall be synchronized to the standard time of the organization in accordance with the Time Synchronization Policy. The time zone shall be set to IST.
- h) Standard security principles of least required access to perform a function shall always be used as per standard access control mechanism.
- i) Administrative privileges shall not be used when a non-privileged account will do. It is vital that the server application executes only under a unique individual user and group identity with very restrictive access controls.
- j) Administrative privilege account names shall be renamed wherever possible to non trivial names and a record shall be maintained for such changes with the administrator

(and his/her controlling officer).

- k) Administrators shall make and maintain change management procedures, which shall be verified by the respective controlling officers. Change Management procedure should be followed for any changes in Administrative account.
- l) In situations when the administrator is temporarily unavailable, administration along with the administrator password shall be handed over by the controlling officer to an official temporarily designated as system administrator. On reporting back to duty, the administrator shall change the root password.
- m) Admin password cannot be disclosed or shared with people other than Administrators. A copy of all passwords can be shared in sealed envelope and it can't be open until unless it is required and in co-ordination with the competent authority.
- n) Passwords and password management for server accounts shall be in accordance with the Password Policy.
- o) Logs shall be enabled for access methods of the servers (especially for production servers) and audit and Log of activities referring to the operating system, access to the system shall be maintained and archived in accordance with the Audit Log Policy. All rejected accesses and services may also be logged and listed in exception reports for further scrutiny.
- p) Backups of the respective servers shall be taken and maintained in accordance with the Backup Policy.
- q) **Vulnerability Scan** should be carried out periodically by standard tool to scan the overall WBSDC set up for vulnerabilities/weaknesses and corrective measures shall be implemented as well. This shall be undertaken whenever a new service is opened



or enabled. **Periodic security testing** of the OS/System configurations is a vital way to identify vulnerabilities and to ensure that the existing security precautions are effective and that security controls are configured properly.

- r) **Penetration testing** is “security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation”.

The purpose of penetration testing is to exercise system protections (particularly human response to attack indications) using common tools and techniques developed by attackers. This testing is highly recommended for complex or critical servers.

- s) Any maintenance by vendors, on production servers, shall be performed in the presence of the Administrator or authorized representative of the administrator only after filling up **Third Party Access Declaration and WBSDC Access form and (Refer [Annexure-II \(B and C\)](#))**. An approval shall be taken from the controlling officer for any updates and additional software being installed.
- t) Administrators shall maintain the list of all software packages installed on each server that can be verified by the auditor appointed to audit the server. A logbook shall be maintained for the purpose of hardware and software configuration.

#### 9.4.4.3 Monitoring

- a) All security-related events on critical or sensitive systems shall be recorded and maintained. These logs should be retained accordingly to the backup policy.
- b) Security monitoring and analysis will provide necessary inputs to the administrators of the servers, wherever applicable, and from time to time depending on the incidents observed.

- c) Any noticed incident on the server shall be reported to the in accordance with the Incident Reporting Matrix provided by the Stake Holder.

### 9.4.5 Responsibilities

All designated system administrators of servers in the WBSDC/WBSWAN domain are responsible for adhering to these policies.

### 9.4.6 Compliance

- a) Authorized organizations/designated officers of WBSDC will perform audits on the servers on a regular basis.
- b) Effort will be made to prevent audits from causing operational failures or disruptions.

### 9.4.7 Enforcement



Any staff/line department/vendor found to have violated this policy may be subject to disciplinary action.

## 9.5 Firewall Policy

### 9.5.1 Purpose

The purpose of this policy is to ensure implementation of minimum-security configuration for Firewalls.

### 9.5.2 Scope

This policy applies to the Firewalls in WBSDC.

### 9.5.3 Policy Details

#### 9.5.3.1 Firewall shall be placed:

- a) At Entry and Exit points of the network.
- b) Between networks with different security levels.

#### 9.5.3.2 Each of the firewall permit rule must be configured for:

- a) The required services.
- b) The required protocols.
- c) The required direction.
- d) The minimum required source/destination IP address space.
- e) The required users (in case the Firewall supports user-based policies).
- f) The required time interval(s).

#### 9.5.3.3 All traffic by default must be denied through an explicit firewall rule.

#### 9.5.3.4 All traffic destined to the firewall must be denied through an explicit firewall rule.

#### 9.5.3.5 Unused firewall ports must be disabled.

#### 9.5.3.6 Anti-spoofing must be enabled on all interfaces.

**9.5.3.7** The entry/Exit Procedure for traffic should be laid for addition/deletion/alteration of the required entries.

**9.5.3.8** Firewall Administration(If Proper Tool Available):

- a) Administration must be carried out over an encrypted channel.
- b) Administration must be allowed only after successful authentication and authorization of the administrator.
- c) Administration must be permitted from specific IP addresses only.
- d) Separate login-name must be used for privileged access and non-privileged access.
- e) There must be two administrators.
- f) Each administrator must be allocated a separate login-name.

**9.5.3.9** Logging and Monitoring:

- a) Firewall logs should be maintained on a separate server.
- b) The traffic permitted by firewall must be logged.
- c) The traffic denied by firewall must be logged.
- d) Administration activities must be logged.
- e) Access and audit logs shall be analyzed and reviewed on a daily basis.
- f) If SNMP is used on the firewall:
  - I. SNMP must be set for 'Read Only' mode only.
  - II. SNMP access must be permitted from specific IP addresses only.
  - III. Default community string must not be used.
  - IV. SNMP community string must be treated at par with "root" or "administrator" passwords for computers.



## 9.6 Audit Log Policy

### 9.6.1 Purpose



Audit log records make it possible to monitor general activities on a system as well as to identify many types of suspicious attempts (successful or not) on the security of the system. These event log records help in distinguishing between security incidents, failures in hardware or software, and errors in system configuration that may allow or deny access to resources in an inappropriate manner. This policy states various aspects of handling of all audits log records. This is so as to make the logs available for monitoring and auditing purposes for understanding visitor/user activity and base lining system activity; and for forensic analysis to identify reasons for security breaches, carrying out investigations and identifying problems in order to take mitigating steps.

### 9.6.2 Scope



This policy applies to all servers and devices operating in WBSDC/WBSWAN and all applications in the E-Governance domain.

### 9.6.3 Policies

- 9.6.3.1** All network and security devices and systems on WBSDC/ WBSWAN need to generate and maintain audit logs.
- 9.6.3.2** In case of Critical Applications (to be decided by Competent Authority) on WBSDC/ WBSWAN, audit logs should be preferably maintained across all the devices and systems.

- 9.6.3.3** Logs to be maintained in respect of server OS including other components. All servers including web hosting servers, Database servers, application servers, e-mail servers, DNS, DHCP,FTP, antivirus servers, authentication servers, network access providers etc. to generate audit logs.
- 9.6.3.4** Components including OS, applications such as IIS/Apache, middle tier applications, custom applications, and database servers should generate audit logs.
- 9.6.3.5** All servers OS shall have the following events for which recording in logs should be enabled/configured:
- a) User(both application and system) and process logon and logoff
  - b) Failed /Successful logon attempts
  - c) Access to Objects (file system, registry object). Including data/ devices associated with the system if applicable.
  - d) Account management events - Additions, changes or removal of user accounts and groups
  - e) Changes of access rights to system data resources
  - f) System events - Shutdown and restart of system, registering of trusted logon processes, or other activities that affect system security, events effecting system security logs.
  - g) System configuration changes
  - h) Security policies changes
  - i) Actions taken by operations personnel, Administrators, support personnel, outsourced staff.

- j) Other components/services such as used for providing connection/logging to an OS server also shall maintain their audit trails.

**9.6.3.6** Web access Logs should store logs in W3C format and extended W3C format. The following should be included: Date, Time, Client-IP, server IP, user id, URI, method, query string, referring URL, HTTP status.

**9.6.3.7** Database Logs. DB Audit logs should be enabled to capture the following:

- a) Server events (shutdown, pause, start).
- b) DBA Change of Password
- c) Events for execution of Backup restore and bulk data insert commands on the database.
- d) DBA activity in terms of DDL viz. CREATE, ALTER, DROP objects for managing the objects in the database
- e) Security events (grant/revoke/deny, login user/role add/remove/configure).
- f) Where required, DML statements executed such as SELECT, INSERT, UPDATE, EXEC etc.
- g) In all the above, logs to capture
  - I. Date and time of event.
  - II. User who caused the event to occur.
  - III. Type of event.
  - IV. Success or failure of the event.
  - V. The origin of request viz. IP/computer name
  - VI. The name of the object accessed.

**9.6.3.8** Web Application Logs to capture information about events/actions deemed essential in the context of applications. For example :

- a) Failed/Successful login attempts for closed user group application.
- b) Link published in case of Content Management System application.
- c) Operations carried out by an approving officer in case of request received. In each case the Date, time, IP, user id, session id, event invoked are to be captured.

**9.6.3.9 Time Synchronisation.** All the servers, network and security devices should have been time synchronized. The logs across all the components should be time synchronized i.e. the time zone setting of IIS web server, the OS, and firewall, dialup server, syslog server etc. should be set to the same time zone and synchronized.

**9.6.3.10 Periodic verification** Administrators must ensure periodic verification and correlation of audit log recorded across the system, components and devices to be taken up for accuracy of recording of path traversed by request.

**9.6.3.11 Audit Log Archival and Retention.** Audit logs are to be backed up and archived after a designated period of six months to release space or resources in production systems. Archived audit logs should be retained for a minimum period of two years for analysis purposes. Audit logs are to be archived for longer durations as per specific record retention requirement or as desired by compliance requirements as deemed necessary in case of systems/applications.

**9.6.3.12 Tamper proofing Audit Logs.** Measures are to be taken so that audit logs are tamper proof. Any tampering activity or attempts should get detected and reported for analysis purposes.

Measures should be taken such that any deletion of a log entry can be detected. In case of critical systems, other solutions may be considered such as digital signing of audit log data.

**9.6.3.13 Log Review.** Audit logs should be reviewed periodically to understand user activity in the system and baseline drawn on the system activity.

Anomalous activities needed to be identified from the logs by examining malformed entries or unusual entries etc.

**9.6.3.14 Designated Audit Role.** An audit role may be designated for the purpose of review of logs and their analysis.

- a) Study of logs may be taken up by designated person/role for application audit log data.
- b) Use of automated solutions or tools may also be considered for the purpose of baselining of normal system/user activity/behaviour and identifying anomalous entries/behaviour.

**9.6.3.15 Restricted Access.** Access to the log data to be restricted by ACLs. Only privileged role to be allowed read only view of log data. No writing/modifying to be allowed on the audit log data.

**9.6.3.16** Reporting anomalies to security control. Site administrators, owners or individuals in charge of applications and having access to certain sections of audit log data and conducting their own studies/review of logs may report anomalies to security control or SOC.

**9.6.3.17 Log Format Issues.** Systems, devices and applications generate audit log data. A standard log format such as syslog may be used for generating/storing of audit log data. In case where syslog format is not supported ex: windows event log then solutions may be considered for converting to syslog format.

## 9.6.4 Responsibilities

- a) All administrators and operators are responsible for keeping their systems' audit log feature enabled.
- b) The log should be kept for a period of 2 years.
- c) Logs to be kept online for current 6 months log data.

## 9.6.5 Enforcement

Any employee found to have violated this policy should be subjected to disciplinary action as per the rules of the organization.



## 9.7 Portable Media Usage Policy

### Objective

The objective of this policy is to minimize security risks arising out of usage of Removable Media Interfaces for portable storage devices such as USB memory sticks, pen drives, entertainment devices with data storage capacities (with USB, Bluetooth and other interfaces) etc., (herein referred as "Removable Media") within the organization and also establish usage criteria for genuine business requirements.

### Scope

This policy is applicable to all Users in the Organization, and also for all types of removable media devices. WBSDC requirements/agreements detailing the use of removable media shall supersede this baseline policy. Situations warranting the use of Removable Media devices/interfaces for business purposes shall be granted only based on WBSDC concurrence and with due protection to information.

### Policy



- Removable Media ports/interfaces (USB) usage within the organization in general, shall 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.
- Information/Asset owners shall be held accountable for (A) copying WBSDC sensitive information in to any removable media which could cause confidentiality breach (B) causing transmission of malicious code from removable media in to WBSDC work (C) execution of unauthorized software programs from removable media even inadvertently which could potentially lead to security incidents with business impact (D) legal Violations.



- 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. in to the removable media from WBSDC assets.
- Information stored in removable media devices to address genuine business requirements, shall be in an encrypted format.
- Employees shall 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 shall be permitted only after due authorization from WBSDC.
- There shall be a formal process with approval and tracking mechanism for handling genuine business requirement for usage of removable media devices in Desktops, laptops and Servers.
- Authorized users shall not transfer the sensitive or personal information to removable media devices without encrypting the information as per industry best practices.
- Users shall not copy information from removable media (non-company media received from external source) to WBSDC assets (even if for business purposes) without checking the source for any type of malicious code presence.
- There shall be specified time limit for enabling the removable media ports in Desktops & Servers and the access shall be reviewed based on the timeline.
- Removable media access shall be reviewed whenever there is change in responsibility, user, project, and movement of assets.
- 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.

## 9.8 Remote Access Policy

### Objective

The objective of this policy is to provide controlled remote access and safeguard Information systems from unauthorized access in WBSDC.

### Scope

The scope of this policy applies to all Users who are accessing WBSDC IT resources using remote access channels.

### Policy

- Remote access to WBSDCs IT resources from public network shall be allowed only after successful identification and authentication of users.
- Remote access to intranet applications shall be provided only through secured communication channels such as SSL or IPSEC.
- Access to critical applications in the intranet shall be granted only with 2 factor authentication.
- In case of user separation from WBSDC's services, user credentials including SecurID tokens shall be deleted (to be disabled in the case of SecurID tokens) on the last day of the user promptly by the respective Account administration personnel.
- VPN access to WBSDC's resources shall be authenticated by the Active Directory.
- User Authentication for establishing VPN session shall be encrypted.
- Remote access logs shall be maintained for a period of 45 days on file server and then backed up for 3 months on secondary storage.
- Deny access logs on remote access service shall be monitored by Network/ Security Operations staff for taking appropriate Preventive actions.
- Adequate care shall be taken by mobile users when mobile computing facilities are used in public places, meeting rooms and other unprotected areas as defined in Remote access Guidelines.



- Trouble shooting of systems remotely by vendors & systems personnel shall be done as per remote access procedure.
- Remote access users shall not extend access to WBSDC Intranet resources to others such as friends or family in any form.
- Dial-out/Dial-in connectivity from/to the WBSDC backbone as well as restricted network shall be allowed ONLY with written approval from the Network Operations Manager/Security Operations Manager.
- User shall not simultaneously connect the desktop/laptop to any two types of networks in any form. For example, Users shall refrain from connecting WBSDC LAN and Internet using dial-in or VPN or through any other form of connectivity, simultaneously.

## 9.9 Password Policy

### 9.9.1 Purpose

The purpose of the policy is to verify the compliance and adherence of the security policies that has been drawn and finalized.

### 9.9.2 Scope

This policy is applicable for any kind of password management within WBSDC.

### 9.9.3 Policy

- a) The Password must be Case Sensitive and must not be same as the User ID
- b) The Password for all the Computers and Network Devices must be of 8 – 12 characters and should contain both upper and lower case characters (e.g., a-z, A-Z), at least one Special Character (! @ # \$ % ^ and \_)
- c) The Password age will be Forty Five (45) days. The password will automatically expire after 46 days. The User must be alarmed from 30<sup>th</sup>. day of the password age to change the password.
- d) When Changing the Password, any of the last Five used passwords must not be used. Password History must be maintained for this purpose
- e) Account lockout threshold - 3 failed login attempts

### 9.9.4 Enforcement

Any Staff/Employee/Personnel related to WBSDC found to have violated the policy may be subjected to disciplinary actions.

## Annexure-I

### A. Service and Resource Options:

Departments can host their application/ website by choosing any one of the following options of hosting models depending on the size, criticality and requirement of their application.

Three different **hosting models** related to resource & service sharing options are:-

a) **Collocated:**

i. Shares WBSDC physical space only.

The line departments would only require the physical and external connectivity infrastructure of the data center to host their applications. The DCO shall ensure availability of entire core infrastructure and assist in co-location of the application. Respective application infrastructure to be brought by the line departments.

**Example:** Departments having own Application, web and DB Server, network infrastructure, storage, EMS may share only the SDC's physical space. So, they should opt for option a)

ii. May share physical space, bandwidth, network, server/storage:

Application development & maintenance to be taken care by the line department. The DCO with support from CT shall agree upon the operations and management services required by the line department

**Example:** Departments with medium scale application may share SDC's server/storage/network etc. depending on their requirement. So, they should opt for option (b)

b) **Shared:** Shares all WBSDC Resources.

i. DCO will manages the application and the required infrastructure themselves

ii. The DCO with support from CT shall agree upon the operations and management services required by the line department

**Example:** Departments with small non-critical application/static or dynamic website may share all the resources of SDC; thereby they should opt for option (c)

Refer the table given below for detail understanding:-

Model type	Power, Space Cooling	Shared Bandwidth	Shared Network Resource	Shared Server	Shared Storage	FMS
Collocated <sup>*</sup> Resource	✓	✗	✗	✗	✗	As Required
	✓	✓	✓	✗	✗	As Required
	✓	✓	✓	✓	✗	As Required
	✓	✓	✓	✗	✓	As Required
Shared	✓	✓	✓	✓	✓	As Required

Note: <sup>\*</sup> Additional Bandwidth can be arranged on request.

- a) A free space in the WBSDC's Data Centre with redundant battery-backed power, appropriate cooling. The LD needs to make arrangement for hardware and storage, software, and the network including connectivity.
- b) Add network connectivity besides the facility mentioned in (i) above. The LD needs to make arrangement for hardware and storage, software and the network while the required interface for network connectivity will be available.
- c) Add common storage and Rack space besides the facility mentioned in (i) and (ii) above. The LD needs to make arrangement for hardware, software and licenses.

- d) Add shared Server besides the facilities mentioned in (i), (ii) and (ii) above. The LD needs to make arrangement for software and licenses.
- e) Common Staging Server will be available for virtualised staging activities initially for few days. Staging server can be used further for testing activities and patch up gradation purpose on procuring required licenses separately.
- f) Add Internet facility besides the facilities mentioned in (i), (ii), (iii) and (iv) above, which can be arranged either by the LD itself depending on their bandwidth requirement from any service provider or it can be arranged from WBSDC end.
- g) Add VPN facility to all above options except option (i) only.
- h) Following Optional Services can be provided after the corresponding client licenses are made available to WBSDC.

i.	<b>CA EHEALTH</b> for better management of historical records and reports of network devices and servers.
ii.	<b>CA SPECTRUM</b> for real time reports of server and network devices.
iii.	<b>CA ACCESS CONTROL</b> for access related detailed record of servers.
iv.	<b>CA IT CLIENT MANAGER</b> for asset management record of servers.
v.	<b>CA Wily</b> for application performance management.
vi.	<b>CA Database Performance Manager</b> for better management of data.
vii.	<b>EMC Networker</b> for database and storage node backup and restore solutions.
viii.	<b>HIPS SYMC CRITICAL SYSTEM PROTECTION</b> for monitoring, securing and preventing of file system and configuration changes, malicious application behaviour, unauthorized access changes, executables and vulnerability exploits.
ix.	<b>Antivirus SYMC PROTECTION SUITE</b> for protection against virus, Spyware etc.



## B. Operation Cost of DCO

### A: Common Charges

Resource	Unit	WBSDC Operation Cost
Power, Space, Cooling	U(Rack space)	188 Unit*

**Note:** \* Will be applicable after 28<sup>th</sup> February, 2015, as per the applicable rate

### B: Operation Cost of DCO for Shared Model:

At present, there are no charges applicable for the applications hosted on shared basis. However, following charges may be applicable, if decided by Government of West Bengal:

Resource	Unit	DCO Charge(Per Quarter)**
Shared Server	Per Virtual	Rupees 1630/-
Shared Network	Server	Rupees 1800/-
Facility Management		Rupees 1080/-
Storage	Per TB	Rupees 330/-
Backup		Rupees 90/-

### If applicable, simple Example for DCO Charge Calculation for shared hosting model:

For 1 Web Server, 1 Application Server & 1 DB Instance and 1.5TB Storage:

No. of Virtual Servers required: 3

Storage required: 1.5 TB

#### DCO Operation Cost Calculation for Fully Shared Resources:-

##### A) For Shared Server, Network & Facility Management:

$$3*(1630+1800+1080) = 13530$$

##### B) For Storage & Backup:

$$1.5*(330+90) = 630$$

**On above elaboration, total DCO Charges to be payable per Quarter: Rs. 14160/-**

**C: Operation Cost of Data Center Operator (DCO) for Co-located model :**

- i) For any additional hardware and software items, which will be provided by SIA/State Government Departments for installation at SDC, if Wipro needs to provide only integration services with the existing infrastructure, no additional payment will be given to Wipro.
- ii) For additional hardware items (Server, Network, SAN and Backup devices) and monitoring software (CA) which will be provided by SIA / State Government Departments for installation at WBSDC, if DCO needs to provide any one or multiple sets of services like Installation, Monitoring, Administration, Backup, Management and coordination with Line Department & their System Integrator (excluding maintenance support services) including monitoring of Databases and applications using “CA”, DCO will be paid an amount equal to 1.5% + Applicable Taxes on 1.5% per quarter of the specific Hardware and CA license cost of the project (excluding cost of AMC\*, taxes and duties) by the user department through WBEIDCL.
- iii) For additional software items (Operating Systems, Databases & OEM Applications) which will be provided by SIA / State Government Departments for installation at WBSDC as a part of additional infrastructure (excluding the infrastructure created as a part of State Data Center RFP), if DCO needs to provide any one or multiple sets of services like Installation, Monitoring, Administration and Management, DCO will be paid an amount equal to 1.5% + Applicable Taxes on 1.5% per quarter of the specific Software and associated license cost of the project (excluding cost of AMC\*, taxes and duties by the user department through WBEIDCL. This does not cover OEM unsupported software products, for which, only installation, monitoring and technical assistance will be provided.
- iv) If some project needs specialized skills (Like development and customization of application and databases etc.) then additional manpower will be taken from Wipro with specific skill set as per their existing rate contract with NIC and for this additional manpower, separate payments will be given to DCO by the user department through WBEIDCL.

\* If hardware or software items are having AMC, but AMC charges are not mentioned in BOQ of line department, the total effective price (on which cost of 1.5% per qtr. Will be calculated) of the specific item will be arrived after deduction of 5% of total item cost per annum for the entire duration of AMC.

**D: Additional bandwidth Charges:**

Additional Dedicated Internet Bandwidth, if taken, (for sourcing through secondary upstream Service Provider with primary upstream service provider being the National Knowledge Network), an amount of Rupees 9000/- per Mbps/month + Service Tax is to be payable to the Service Provider.

[\*Nation Knowledge Network (NKN), under DeitY, Government of India is the Primary upstream Service Provider connected with WB SDC & WBSWAN]

## C. List of Summary Reports

The following is the comprehensive list of the respective MIS reports that may be required as per the support services requirements of the LD:

### a. **Weekly Reports**

- i. Issues / Complaints Analysis report for virus calls, call trend, call history, etc.
- ii. Summary of systems rebooted.
- iii. Summary of issues / complaints logged with the OEMs.
- iv. Inventory of spare parts in the DC.
- v. Summary of changes undertaken in the Data Centre including major changes like configuration changes, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

### b. **Monthly reports**

- i. Component wise physical as well as IT infrastructure availability and resource utilization
- ii. Consolidated SLA / non-conformance report.
- iii. Summary of component wise Data Centre uptime.
- iv. Summary of changes in the Data Centre.
- v. Log of preventive / scheduled maintenance undertaken
- vi. Log of break-fix maintenance undertaken

### c. **Half-Yearly Reports**

- i. Data Centre Security Audit Report
- ii. IT infrastructure Obsolescence Report

### d. **Incident Reporting**

- i. Detection of security vulnerability with the available solutions / workarounds for fixing.
- ii. Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.
- iii. Software license violations

# **Annexure-II (Forms)**

## Standards

WBSDC, being the latest state of art requires that it is to be managed effectively and efficiently in a disciplined approach. Accordingly, a few standards are introduced as stated below for competent management of resource allocation, services, and user access control & frequent changes.

### **List of Forms:-**

- A. Security Audit certificate of the application software
- B. Application Hosting Request
- C. Access Declaration
- D. Access Request
- E. Change Request
- F. Temporary Application Hosting
- G. VPN Declaration (If needed)
- H. Challan of all Hardware items to be located at SDC
- I. AMC/ Warranty documents of all Hardware items to be located at SDC

## Annexure-II(Forms)

### LIST OF FORMS & TIME OF SUBMISSION OF THE SAME

F o r m  N o .	Form details	Time of submission
1	Questionnaire for Line Department	At the inception of the project, when detailed information are not available to fill up Form 2.
2	Requisition for Application/Web hosting from Line Department	At least 1 week prior to hosting the application at SDC
3	WBSDC Access Request Declaration	Every time line department requires access to State Data Centre
4	WBSDC Access Request Form	Every time line department requires access to State Data Center
5	Online SDC Access Request	Every time line department requires access to State Data Center
6	Change Request	Prior to implementation of any change
7	Declaration for Temporary Usage of WBSDC Resources	Prior to temporary hosting of an application
8	Undertaking for VPN Access	At the time of joining SDC
9	VPN access request form	Every time line department requires VPN access to State Data Center
10	Safe to host certificate for security audit (To be signed by Authorised person of Department)	Prior to hosting the application and each time the application gets any change
11	Undertaking	To be signed before hosting the project at WBSDC.

## Form- 1: Questionnaire for the Line Departments

**Department Name:** .....

**Address:** .....

**Contact Numbers:** .....

**Name of the contact person:** .....

**Designation:** .....

**Prerequisites**

1. The software application to be hosted at SDC must be security audited.
2. Server to be hosted must be rack mounted.
3. Server to be hosted should have proper documentation ( like time of procurement, AMC etc.)
4. Monitoring services are to be taken from WBEIDCL as per the rate contract

**A. Please provide the following information:**

The services like power, cooling, security and facility management for 24X7 is mandatory and comes for all the options given below:

1) Department will require the service of SDC on

Co-located Model – Department will provide some of the hardware, i.e., server, network equipments, Storage etc. and following items will be shared from SDC(tick appropriate one):

- Rack Space  
  Server  
  Network  
  Operating System (Name: \_\_\_\_\_)
- Application Software (Name: \_\_\_\_\_)  
  Database Software (Name: \_\_\_\_\_)
- Storage (Total requirement \_\_\_ GB/TB)  
  Backup facilities
- Intranet (WBSWAN)  
  Internet bandwidth (Total Required \_\_\_ Mbps)

Full Shared basis – Department will share everything from SDC(tick appropriate one):

- Rack Space  
  Server  
  Network  
  Operating System (Name: \_\_\_\_\_)
- Application Software (Name: \_\_\_\_\_)  
  Database Software (Name: \_\_\_\_\_)
- Storage (Total requirement \_\_\_ GB/TB)  
  Backup facilities
- Intranet (WBSWAN)  
  Internet bandwidth (Total Required \_\_\_ Mbps)

2) Brief details of the hardware to be provided (please provide make and model number, if available):

3) Details of the software:

- i) Whether the software to be hosted at SDC, is customized/ developed/ off the shelf software.
- ii) Specific details of the software to be hosted at SDC, like Database used, application server used, front end used and architecture of the software.
- iii) Software licenses as applicable, already taken/ to be taken in future.
- iv) Any other information:

Signature of authorised person from LD: \_\_\_\_\_



## Form 2: Requisition for Application/Web hosting from Line Department

### Contact Details

Department Name _____	
Address: _____	
Contact Numbers: (o) 1: _____ (o)2: _____ Fax: _____	
Officer In Charge/ Primary Contact person/ Nodal Officer Contact:	Name
	Email
	Mobile
	Work phone
Primary Technical Point of Contact:	Name
	Email
	Mobile
	Work phone
Contact person from System Integrator/ Vendor	Name
	Email
	Mobile
	Work phone
Request Date	
Review Date (for office use only)	
Approval Date (for office use only)	

**Period of Operation: Temporary ( ) / Permanent ( )**

If temporary, please mention details as follows:-

- Duration : From \_\_\_\_\_ To \_\_\_\_\_
- Please specify reason of temporary hosting:
- Will the department have any plan for permanent hosting of Application? : (Yes/ NO)

### Pre-requisites

- The software application/ web portal to be hosted at SDC must be security audited.
- Server to be hosted must be rack mounted. If rack is to be provided by Line Department, provide "**Cyber Rack/APW President**", having dimension of 42UX 600mmX1000mm
- Items to be hosted should have proper documentation (like time of procurement, AMC etc.)
- The services like power(including DG), cooling and security on 24X7 basis is mandatory

## Hosting model required by Line Department

 Co-located Model

 Shared Model

### Form 2.1: Checklist

Sr No.	Check list for Items [ as being supplied by line department ]	Quantity/ Details/ (Yes/No)
<b>For servers to be hosted under Co-located model</b>		
1	LAN patch chord (minimum 2 mtr. Length)	
2	FC cable (minimum 10 mtr. Length)	
3	Power cable (For Rack/ Blade server)	
4	Rack mountable KVM switch, monitor, Keyboard and USB mouse	
5	Rack rails for mounting servers	
6	All the required forms (form 2.2, 2.3, 2.4, 2.5) has been filled up as per requirement	
7	CD/DVD media for Licensed Operating system is available	
	CD/DVD media for the packages/ components to be installed are available. Give details below (please attach copies of license for all)	
	a) Database server: (Name: _____)	
	b) Application server: (Name: _____)	
	c) Web Server: (Name: _____)	
	d) Other1: (Name: _____)	
8	e) Other1: (Name: _____)	
	f) Other1: (Name: _____)	
8	List of licenses (procured / to be procured) for monitoring and backup services for LD's resources has been identified, filled up in form 2.3 below and taken	
9	Is the application Web-based? [ If not, please provide details] (Please note that a web based architecture is preferred in SDC environment)	
10	Is the application three layered architecture? (Web-Application-Database) Provide complete architecture in a separate sheet. (Please note that a 3 layered architecture is preferred in SDC environment)	
11	Is the Application audited and certified through STQC or any authorized agency that the same free from any vulnerability and penetration risks. (Please note that without this compliance, the application will not be hosted at SDC. If the same has been done, please fill in the <b>form 9</b> as given below)	
12	Are the changes done for the public hosted domain names (for existing domain names, migrating to SDC)/ has the domain names been created (for new domains)	
13	Have all the documents (procurement documents, Challan / Invoice, License of the software items, Specification details and Warranty / AMC documents) been placed herewith for all the hardware/ software items (Please note that, without the same and without any AMC/ Warranty support, items cannot be installed at SDC)	

14	Is the Service Level Agreement has been signed? [ if not, pls mention the expected date of signing ]	
15	Have the service charges for DCO, as applicable for monitoring and managing the devices been provisioned?	
16	Attach the software and system architecture document with this SLA	
17	Attach the AMC/ Warranty document of Hardware with this SLA	
18	Attach the technical documents related to hardware/ software stating its versions/ upgrades/ patches/ revisions etc.	

Signature of authorised person from LD: \_\_\_\_\_

### Line Department requirements

#### Form 2.2: For Co-located Model

(Following are the details of the items to be exclusively procured/ provided by Line departments, Accordingly provide the details for the required/ applicable item(s) only)

Sl.No	Items	Specifications/ Requirements											
<b>Server Details</b>													
1	Server Name	No.	Make	Model	Proces sor	Cores per proce ssor	RAM	HDD	U space	NIC card details with Firmware version	Blade/ Rack mount	OS with version	Power Consump on in ampere
	a. Database server												
	b. Application server												
	c. Web server												
	d. Directory/ DNS server												
	e.												
	f.												
	g.												

Sl.No	Items	Specifications/ Requirements
-------	-------	------------------------------


**Server Details**

**Network and storage details of the servers**

2	Sr. No. and name of server as mentioned above	Server Zone (Application/ Database etc.)	Ports & protocols to be used for internet/ SWAN	Ports & protocols to be used for internal connectivity (Web to Apps/ Apps to Database)	Cluster (Y/N)	Heartbeat requirements	Partition/Drive Details		Existing SAN Storage requirement (Write N/A, if not required)	
							Mount Point/ Drives	Size	No of LUN Required	Size
	a. Database server									
	b. Application server									
	c. Web server									
	d. Directory/ DNS server									
	e.									
	f.									
	g.									

**Other items which is provided by Department:**

3	No. Of 42 U Racks									
4	SAN storage hardware details (If provided by LD)	Total in TB	DISK Type			No. of LUN				
			SATA( ) FC( ) SAS( ) Solid State ( )			Size of LUNs				
5	Backup device									

Sl.No	Items	Specifications/ Requirements
<b>Server Details</b>		
	details	
	Tape library details	
	Backup policy	
6	Network items details (Router/S witch etc.)	
7	Database Server software details	Make: Version: Patches (If any): Warranty/ ATS/ AMC Duration: License(Processor/ Device/ User based): <span style="float:right">No. of Licenses:</span>
8	Application server software details	 Make: Version: Patches (If any): Warranty/ ATS/ AMC Duration: License(Processor/ Device/ User based): <span style="float:right">No. of Licenses:</span>
9	Web server software details	Make: Version: Patches (If any): Warranty/ ATS/ AMC Duration: License(Processor/ Device/ User based): <span style="float:right">No. of Licenses:</span>
10	Details of antivirus software	Make: Version: Patches (If any): Warranty/ ATS/ AMC Duration: License(Processor/ Device/ User based): <span style="float:right">No. of Licenses:</span>

Sl.No	Items	Specifications/ Requirements
<b>Server Details</b>		
11	Details of any other software( give the name of the above mentioned server, where the same will be installed)	
12	Security item details	
13	Any other items	
<p><b>NOTE:</b></p> <p>➤ For all the above items, please attach the copy of the procurement documents, License of the software items, Specification details and Warranty / AMC documents.</p>		



Signature of authorised person from LD: \_\_\_\_\_

**Form 2.3: For Shared Model**  
(Provide the details for the required/ applicable item(s) only)

Sl. No	Items	Specifications/ Requirements
1.	Staging Services requirement (Virtualised)	( ) YES ( ) NO (If Yes then please specify)
		RAM
		OS Platform ( ) Windows ( ) Linux
		Disk Space
		Swap Space
2.	Web Server requirement	Tenure (Limited to 15 days)
		( ) YES ( ) NO (If Yes then please specify)
		RAM
		OS Platform ( ) Windows ( ) Linux
		Specify the storage requirement
		Apache ( )
Others1 ( )		
Others2 ( )		

3.	Application software requirement	( ) YES ( ) NO (If Yes then please specify)	RAM	
			OS Platform	( ) Windows ( ) Linux
			Specify the storage requirement	
			JBOSS ( )	
			Others1 ( )	
			Others2 ( )	
4.	Database software requirement	( ) YES ( ) NO (If Yes then please specify)	RAM	
			OS Platform	( ) Windows ( ) Linux
			Specify Storage Requirement	
			Oracle 11g ( )	
			MS SQL ( )	
			My SQL ( )	
5.	Requirement of utilization of SAN Storage*	Number of LUN:	Total in GB/ TB:	SATA ( )   FC ( )
9.	Ports to be opened towards internet			
10.	Ports to be opened towards internal connectivity (Web to Apps/ Apps to DB)			
<p>NOTE:                  *SAN interface (HBA) should be procured along with SAN port licenses. Also, if required, SATA/ FC Hard Drives for SAN may require to be procured.                  ** Backup policy document along with Backup media/ tape drive must be provided by the user as per the backup policy of the Line Department.</p>				

Signature of authorised person from LD: \_\_\_\_\_

**Form 2.4: For All Models**  
(Provide the details for the required/ applicable item(s) only)

Sl. No.	Items	Specifications/ Requirements
A-1. Monitoring Services (EMS) for Line Department (please give the names of items from table A-2, page 33)		
1.	Item names	No. of Licenses
A-2. Backup license details (please give the names of items from table A-2, page 34)		
2.	Item names	No. of Licenses

A-3. Training requirement details on CA (please give the names of items from table A-2, page 35)			
3.	No. of persons		
	No. of Days		
B. Other details			
4.	The application will be available:	External-Open to public:	( )YES ( )NO
		Internal Network- LD's own Intranet Users:	( )YES ( )NO
		Internal Network- Only WBSWAN Network Users:	( )YES ( )NO
5.	Application / Website status: (tick the appropriate)	Planned	
		In development	
		Existing	
6.	URL Details	Registered	( )YES ( )NO
		If YES, Please specify the URL:	
7.	Architecture of application:	Web based ( ) Client Server based ( )	
8.	Secure Socket Layers (SSL) required:	( )YES ( )NO	
9.	Requirement of Internet from SDC	Shared ( ) Dedicated ( )	Bandwidth:
10.	Requirement of Backup **	Number of Tape drives required :	Backup policy:
11.	Requirement of Racks	No. Of Racks:	No. Of "U" space:
12.	Antivirus details ***	( )YES ( )NO	
13.	Do you require VPN access*(if required, please fill in the form as per "FORM 8 & 9"	( )YES ( )NO	
14.	Any other requirement (Please specify)		
* Subject to approval			
** Please note that, if required, application developer is required to execute script for providing backup to a destined folder.			
*** Antivirus license is to be provided by the Line Department			
Signature by the authorized person from Line Department			
Name: _____			
Designation: _____			
Signature: _____			



**Form 2.5: For All Models**  
(To be filled up by WBSDC TEAM/ DCO only after complete submission of all the required forms)

Sl.No.	Items	Specifications/ Requirements								
<b>Server Details</b>										
1	Server Name	server no.	IP Address allotment details	Server zone and termination switch details	Ports opened	Backup details*	SAN Storage Details		Deployed EMS Software details**	
							No of LUN Created	Size		
	a. Database server	1								
		2								
	b. Application server	1								
		2								
	c. Web server	1								
		2								
	d. Directory/ DNS server	1								
		2								
	e.	1								
		2								
	f.	1								
		2								
	g.	1								
		2								
		<b>* Backup policy</b>								
		<b>** Details of EMS</b>								
	<b>For shared hosting only:</b>									
	2	Database Server deployment details								

Sl.No.	Items	Specifications/ Requirements
<b>Server Details</b>		
3	Application server deployment details	
4	Web server deployment details	
5	Deployment details of any other software(give the name of the above mentioned server, where the same will be installed)	
<b>Other details:</b>		
6	Allotted public IP (for web applications )	
7	Deployed Security details	
8	VPN Credential details	
9	Any other items	

FOR OFFICE USE ONLY			
Reviewed for hosting by		Approved for hosting by	
Name		Name	
Organization		Organization	
Designation		Designation	
Date		Date	
Signature		Signature	

### Form 3: WBSDC Access Request Declaration

<b>Name :</b>			
<b>Organization :</b>			
<b>Address :</b>		<b>Date:</b>	
<b>Phone:</b>		<b>E-mail:</b>	

#### Third Party Access Declaration


- Users must sign in the register maintained by the security at the reception area.
- Users shall access the only designated physical area of the West Bengal State Data Centre (WBSDC) premise and the respective resources as per prior approval of CT/DCO through a prescribed form namely, "Third Party Access Request".
- Users shall not access any information resources of Data Centre, without prior authorization of the concerned officials of CT/DCO at West Bengal State Data Centre.
- User shall not carry any personal device like palmtop, laptop, tablet etc and storage media like pen-drive, CD, DVD or any other form of removable storage devices into WBSDC secured zones like Server Farm Area and etc. without the permission of the CT/DCO.
- Users shall not capture any photograph in any part of the WBSDC premise.
- Users shall not access any information resources without the appropriate permission and presence of CT/DCO Professional.
- Passwords and access privileges to WBSDC resources shall not be disclosed (under any circumstances) to anyone inside and outside West Bengal State Data Centre.
- Users shall not engage in abusive or improper use of information resources, which includes, but is not limited to, misuse of resource/ privileges, tampering with resource and unauthorized removal of resource components.
- User shall not conduct or permit "cracker" activities. User shall not run "packet sniffers". Users shall not distribute computer viruses, Trojan horses, worms, or any other malicious software
- **User must bring-in photo-id card (company id card/ voter id card/ any other photo id card issued by their company or Govt. Of India/ Govt. Of West Bengal) as their proof of identity.**
- Users violating the above procedure will be brought to the notice of the competent authority for necessary action as per Indian IT Act.

I hereby declare that I have understood the information security practices as mentioned above at the West Bengal State Data Centre, and I shall adhere to the procedures.

Date:

Sign:

### Form 4: WBSDC Access Request Form

<b>Requestor's Name:</b>			
<b>Organization:</b>			
<b>Address:</b>		<b>Date:</b>	
<b>Phone:</b>		<b>E-mail:</b>	
<b>Type of Access</b>	<input type="checkbox"/> Physical <input type="checkbox"/> Logical/Network if Logical, Specify the mode of connectivity	Date of Access Time of Access Duration of Access:	
<p><b>The Service Area to be accessed</b> [<i>Staging/Meeting/NOC/Server Farm / Electrical Room: Access to the Server Farm and Electrical Room is highly restricted</i>]</p>			
<p><b>List of Resources to be accessed:</b></p>			
<p><b>Support Required: Y/N</b>          If yes, please provide details</p>		 राष्ट्रीय ई-गवर्नेंस योजना National e-Governance Plan	
<b>Purpose of Access:</b>			
<b>For Department/Team Head Only:</b>		<b>Remarks:</b>	
Approved: <input type="checkbox"/>	Rejected: <input type="checkbox"/>		
Date Approved:	Approved By:		
<b>For Authorized Usage Only:</b>			
Granted: <input type="checkbox"/>	Rejected: <input type="checkbox"/>		
Date Granted:	Granted By:		
Remarks:			

## Form 5: Online SDC Access Request

The request for physical access to the SDC should be sent as an email to SDC, to the email address – [projectmanager.egov@wb.gov.in](mailto:projectmanager.egov@wb.gov.in) , with the subject line of the email as **'Request for Access to SDC'**:-

1. The email request should be made by the Project Manager/Coordinator of the project/organization of at **least 24 hours** before the date and time at which access to the data centre is required.
2. **The email should clearly mention:**
  - a. Date and Time of visit
  - b. Duration of visit
  - c. Purpose of visit
  - d. SDC area (Server / Staging / Electrical / NOC) Room, etc to which access is required.
  - e. Details of equipment (Laptop, External Hard Disk, etc.,) if any, to be bought into the SDC
  - f. Details of person requesting access –Name, Designation, Organization/Project Name, Contact Phone (Landline and mobile)
  - g. Details of person (s) visiting SDC – Name, Designation, Organization /Project Name, Contact Phone (Landline and mobile)
3. The details mentioned in the email will be cross checked by Project Manager. SDC Team and access will be granted based on confirmation from the person requesting access to SDC.
4. The security team at SDC will verify the credentials of the visitors on the basis of photo-identity card. Hence, please ensure that the visitors carry a photo-identity card like identity card issued by employer or any other suitable photo identity card.
5. If you have questions/concerns please contact SDC Help Desk at [helpdesk.wbsdc@wipro.com](mailto:helpdesk.wbsdc@wipro.com).

### Form 6: Change Request

Project Name/Change description			
Prepared By:		Preparation Date:	

#### 1. Change Proposal Request

<b>Type of Change Request:</b>	Infrastructure	Software	Application	System Process
	Infrastructure			
<b>Priority:</b>	Low	Medium	High	
<b>Kind of request (Temporary/ Permanent)</b>	Temporary/ Permanent	If temporary Timeframe	High	Low
<b>Proposed Date</b>				
<b>Proposer's name</b>				

#### e. Details Required For Change Request

Details of Proposed Change	
Reason for change	
Device Details	

**Note:** Please note that the approval or rejection for the proposed Request for Change will be Communicated With required time to execute (if approved) based on the impact and constraints of resources and operation.

**f. Approval and Reviews**

<b>Approvals</b>			
NIC and Project Manager, Composite Team	Name	Signature	Date
Security Specialist			
Network and Security Expert			
Project Manager			

<b>Reviews</b>			
NIC and Project Manager, Composite Team	Name	Signature	Date
Security Specialist			
Network and Security Expert			
Project Manager			

### Form 7: Declaration for Temporary Usage of WBSDC Resources

<b>Name :</b>			
<b>Declaration for WBSDC Access</b>			
<b>Organization :</b>			
<b>Address :</b>		<b>Date:</b>	
<b>Phone:</b>		<b>E-mail:</b>	
Dear Sir,			
<ol style="list-style-type: none"> <li>1. We will own the responsibility for any downtime of our resources such as hardware, storage, operating system, database management system, application and any other software which may accumulate during the specified temporary period.</li> <li>2. We will not claim any downtime, if any of the common services such as the physical infrastructure, network, Internet, etc. due to any undesired or unforeseen incidents that may occur during the period as mentioned above.</li> <li>3. The following are not applicable / (applicable) as our application is (not) security audited :           <ol style="list-style-type: none"> <li>a. We will own the responsibility in the event of any leakage of our data as the application that will be accommodated within the WBSDC resources purely on temporary basis for a period of ____ months is not audited.</li> <li>b. We declare that we will get it audited by any one of the parties recommended by the CERT-IN authority, GoI within the period as mentioned above and inform the Project Manager, Composite Team, e-Gov Infrastructure, West Bengal.</li> </ol> </li> </ol>			
I hereby declare that I have understood the information security practices as mentioned above at the West Bengal State Data Centre, and I shall adhere to the procedures.			
Date:			
Sign:			



### Form8: Undertaking for VPN Access

The VPN service requested is to facilitate the developers for remote **updating of user sites hosted in WBSDC**. It cannot control the Content being updated and hence the services provided will be not responsible for the contents being updated or security breach of the web sites by exploiting vulnerabilities in the site updating services (Front Page, Scripts, FTP, SSH, SQL) and web services (HTTP). VPN Services offered will not be responsible for security breach of the VPN client software.

#### DECLARATION

I hereby declare that

1. The VPN account requested will solely be used for **updating contents only and there will be no change / insertion of software codes**. Should there be any need to change software / application codes necessary permission will be taken from the Project Manager, NeGP.
2. The User id & Password will be kept safe and will not be shared with others.
3. VPN access as well as its components (software/security token if any) will be safe guarded from any unauthorized use. I will only use the VPN on a computer that has up-to-date virus protection.
4. I will not indulge in any activity that may disrupt WBSDC services and will not disclose information about WBSDC VPN Services.
5. No attempt will be made to gain unauthorized access to other applications and facilities.
6. If at a later stage any information is found to be incorrect or non-compliance with the terms and conditions will result in the cancellation of the WBSDC VPN service.
7. This VPN access is provided based on the current designation/role of a user. If the role changes or an user having the VPN account details leaves the organization, it's my sole responsibility to inform that immediately to the helpdesk-WBSDC.
8. I completely understand the risk involved in VPN access to Servers for updating the websites, hence **WBSDC has no responsibility for data theft/security breach of the website** as a consequence to VPN operation with the web site.

I hereby authorize \_\_\_\_\_ (name) \_\_\_\_\_ (designation) of \_\_\_\_\_ (name of the organization) to fill up "form 9: VPN access request form", every time our department requires VPN access to SDC, unless informed otherwise.

I have read and understand the above conditions under which I may be provided VPN access and agree to abide by them. I further understand that disclosure of any information or non-compliance with the terms and conditions may result in the breach of the WBSDC VPN facilities.

Place: \_\_\_\_\_

Signature of the Subscriber

Date: \_\_\_\_\_

### Form9: VPN access request form

Details of the officer requesting/ authorizing on behalf of the Line Department			
Requestor/ authorizer Name:		Date	
Designation:			
Department:			
Address:			
Phone:		E-mail:	
Details of the person being authorized:			
Name		Designation	
Organization			
Address			
Phone		E-mail	
VPN Access details:			
VPN Access Duration (A maximum of 72 Hrs.)	From Date & Time :-		To Date & Time:-
Specify the port for VPN connectivity			
Specify the activity to be perform through VPN	New Software Installation In Server (On approval only) :		
	Restarting The Server :		
	Content Updation of website:-		
	Other Activities To Be Mentioned :-		
Specify at a time how many user's will access through VPN	Single User :- Yes ( ) No ( )		
	Multiple User's :- Yes ( ) No ( )		
List of Resources to be accessed:			
For office use only (To be filled in by Composite Team/ DCO only)			
Approved By:			
Approval Date & Time:-			

**Form 10: Safe to host certificate for security audit****(To be signed by Authorised person of Department)**

From:

Date:

&lt;Name of the authorized person of the department along with address, contact details etc.&gt;

To:

The Project Manager, Composite Team  
Moni Bhandar, WBEIDCL, Webel Bhavan,  
Sector- V, Salt Lake City, Kolkata -91

Sir,

This is to inform you that the application/ website/ web portal namely “\_\_\_\_\_” which is going to be hosted at West Bengal State Data Center is safe to host at WBSDC and the security audit report(s) is/are attached herewith proving the same.

I would like to request you for hosting the application at SDC environment. I also undertake that if there will be any change in the application, we will again undergo security testing of the application and once we will get security audit clearance, we will again provide this form to you for your record.

With regards,

(Signature of the officer with seal)



### Form 11: Undertaking

#### (To be signed by Authorised person of Department)

I/We hereby declare that I have complied the following guidelines for hosting my/our web-based application at WBSDC.

SR NO	DESCRIPTION	REMARKS (Y/N/NA)
1	Application is securely audited by a third party, e.g. STQC or any other listed in CERT-In of Gol (attach evidence)	
2	An authenticate domain name is being used where applicable	
3	No UNLICENSED version of s/w of any type are in use	
4	No UNSUPPORTED OS, Web Server etc. are being used	
5	Latest LINUX Kernel is installed with all checks & balances (no DEFAULT installation)	
6	Latest security patches are installed	
7	System is HARDENED to the maximum extent possible with only the required services	
8	Vulnerability Assessment (VA) for OS performed	
9	Closed all vulnerability as found from VA	
10	Penetration Test (PT) for Application performed	
11	Closed all vulnerabilities as found from PT	
12	Application software is tuned for optimum performance	
13	Database is tuned for optimum performance	
13	No unwanted s/w is loaded in server	
14	Requisite ANTIVIRUS & ANTISPAM protection enabled	
15	Necessary backup methodology enforced	
16	Post-update vulnerability & dependency of application checked	
17	Agent / Tool is installed to monitor your Application and Database	
18	Host based Intrusion Detection System (AIDE for Linux) installed	
19	File Systems are appropriately organized	
20	Growth of File Systems are estimated and arranged accordingly	

I/We further undertake that the above measures are indicative in nature and in the event of any malfunctioning of web/application/Database server I/we would take appropriate/effective steps proactively to mitigate the same while taking WBSDC into confidence.

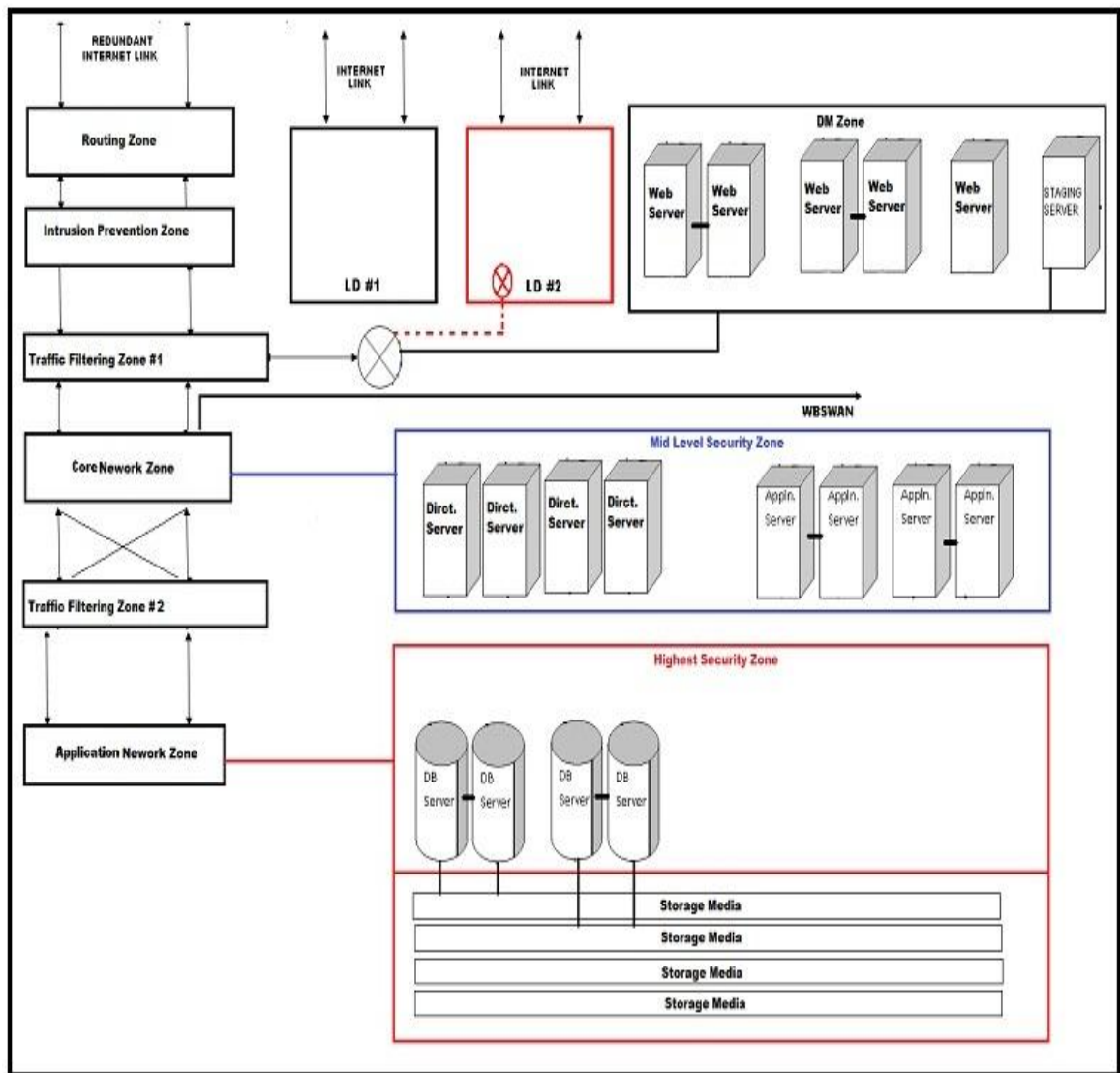
\_\_\_\_\_  
Authorized Signatory

Name :

Department :

## Annexure-III(Positioning of Line Department)

**Fig: Simplified Architecture Diagram**



### **The safe and secured architecture of WBSDC –**

The internal Network Architecture of “West Bengal State Data Centre” (WBSDC) has been divided into several zones to protect the data in the SDC Servers from any vulnerable attacks from the outside world but at the same time the architecture is so designed that an authentic and authorized traffic will get smooth access to the server.

The internal Network has been divided in to the below mentioned zones →

#### **A. Routing Zone –**

The internet traffic or any other external traffic first comes in this zone.

#### **B. Intrusion Prevention Zone –**

- i. After coming to the “Routing Zone” the traffic enters into the “Intrusion Prevention Zone” where the traffic gets it first checking and any unauthorized traffic (especially any unwanted intrusion activity) to the data center area is blocked here from getting in to the next level.
- ii. A separate zone (namely DM Zone) has been created and separated from this are where mainly the Staging Server is placed and the Web Servers are kept. The authentic internet traffics after passing the Intrusion Prevention System comes to the web Servers. The Clusters of Web Servers could also be created hare.
- iii. Any request for accessing the Application / Database / Directory Server from the Web Servers will be passing through the “Traffic Filtering Zone #1” to maintain security and surveillance of the “Mid Level Security Zone”.

C. **Traffic Filtering Zone #1 –**

- i. In this area the traffic that has passed through the checking of the “Intrusion Prevention Zone” and “DM Zone” get checked again before it get in to the “Core Network Zone”.

D. **The Core Network Zone –**

- i. The connectivity from the West Bengal State Wide Area Network (WBSWAN) will be terminated in this area.
- ii. The “Mid Level Security Zone” where mainly the Application / Directory Servers are placed is connected to this zone.

E. **Mid Level Security Zone –**

- i. In this area the Application / Directory Servers are placed.
- ii. The clusters of Application / Directory Servers are also created in this zone.
- iii. Any traffic that will go to the “Highest Security Zone” from the “Mid Level Security Zone” will be passing through the “Core Network Zone”, “Traffic Filtering Zone #2” and “Application Network Zone” for the purpose of security of data.

F. **Traffic Filtering Zone #2 –**

- i. Before getting in to the next level another authenticity of the incoming traffic is checked here in this area.
- ii. Any request from the Application Servers that needs an access to either the Database Server or Storage area will be passed through the “Traffic Filtering Zone #2” for maintaining the security of the Database Server and Storage Network placed in the “Highest Security Zone” connected to the “Application Network Zone” and in turn the valuable data stored there.

**G. Application Network Zone –**

- i. The “Highest Security Zone” is connected to this area.

**H. Highest Security Zone**

- i. This is the most secure area of the Data Center.
- ii. The Database Servers and Storage Networks are placed in this zone.
- iii. The Clusters of Database Servers will be created here

**Application Hosting Options for the LDs under Large scale Category →****LD #1 →**

- i. This is the situation when the Line Department (here in after mentioned as LD) will arrange their entire setup including Servers, Networking Equipments, Internet Links, Firewall, ISP etc
- ii. The LD will only take the Physical Space, Cooling, Battery backed up Power and DG set from the SDC.

**LD #2 →**

- i. In this scenario the LD will arrange their entire setup including Servers, Networking Equipments, Internet Links, Firewall, ISP etc
- ii. The LD will take the Physical Space, Cooling, Battery backed up Power and DG set from the SDC
- iii. The LD has opted for some additional Monitoring / Support Services from the SDC.



### **Application Hosting Options for the LDs under Medium scale Category →**

#### **LD #3 →**

- i. In this scenario the LD will arrange their Servers only (Web Server, Application Server and Database Server)
- ii. The LD will share the common Network Infrastructure of the WBSDC to access their application through Internet.
- iii. The LD will also take the Physical Space, Cooling, Battery backed up Power and DG set from the SDC.
- iv. The LD will share the common Storage Infrastructure of the WBSDC.
- v. The LD might opt for some additional Monitoring / Support Services from the SDC.

#### **LD #4 →**

- i. In this scenario the LD will arrange their Servers only (Web Server, Application Server and Database Server)
- ii. The LD will share the common Network Infrastructure of the WBSDC but they will access their application through Intranet only. The connection in this scenario has to be dedicated Leased Line Connectivity to access their application.
- iii. The LD will share the common Storage Infrastructure of the WBSDC.
- iv. The LD will also take the Physical Space, Cooling, Battery backed up Power and DG set from the SDC
- v. The LD might opt for some additional Monitoring / Support Services from the SDC.

### **Application Hosting Options for the LDs under Small scale Category →**

#### **LD #5 →**

- i. In this scenario the LD will share all the common infrastructure of WBSDC including Server, Network, Internet bandwidth, Storage, Physical Space, Cooling, Battery backed up Power and DG set etc.
- ii. LD might opt for some additional Monitoring / Support Services from the SDC.

### **Annexure-IV(Glossary /Abbreviations)**

<b>AMC</b>	Annual Maintenance Charge
<b>CA</b>	Computer Associates
<b>CAPEX</b>	Capital Expenditure
<b>CT</b>	Composite Team
<b>DCO</b>	Data Centre Operator
<b>DIT</b>	Department of Information Technology
<b>DMZ</b>	De-militarised zone
<b>DR</b>	Disaster Recovery
<b>EGIMC</b>	e-Governance Infrastructure Management Committee
<b>e-Gov</b>	e-Governance
<b>FMS</b>	Facility Management Service
<b>G2B</b>	Government to Business
<b>G2C</b>	Government to Citizen
<b>G2G</b>	Government to Government
<b>GoI</b>	Government of India
<b>GoWB</b>	Government of West Bengal
<b>ICT</b>	Information and Communication Technology
<b>ISMS</b>	information security management system
<b>LD</b>	Line Department
<b>NeGP</b>	National E-Governance Plan
<b>NOC</b>	Network Operation Centre
<b>OS</b>	Operating System
<b>SeMT</b>	State e-Governance Mission Team
<b>SLA</b>	Service Level Agreement
<b>TPA</b>	Third Party Application
<b>WBSDC</b>	West Bengal state Data Centre

## 10. Management

The WBSDC is operated for 24 x 7 x 365 by a Data Centre Operator (DCO), guided and supervised by a Composite Team, led by the Project Manager from National Informatics Centre (NIC), Department of Information Technology, Ministry of Communication & Information Technology, and Government of India. The basic facilities required to run the infrastructure are provided by West Bengal Electronics Industry Development Corporation Limited (WBEIDCL) who is eventually the State Implementation Agency (SIA) worked for establishing such complex infrastructure. Being part of e-Gov infrastructure, it is managed by a Committee, namely, e-Governance Infrastructure Management Committee (EGIMC) under the overall supervision of an Apex Committee headed by the Chief Secretary.

## 11. Conclusion

In a very short tenure since its inception **West Bengal State Data Centre** (WBSDC) has embarked its bold, remarkable and versatile foot prints in the area of supporting the various needs of different departments of the Government. Some to be mentioned here are successful publication of the Results of various examinations like *Madhyamik, Madrasa, Higher Secondary and WBJEE, e-District, Banglar Mukh* etc.

Not only the publications of different examination results but also, has supported other departments and Government initiated and supported projects like *Labour Department, Kolkata Urban Services for Poor (KUSP)*, etc with the highest level of efficiency and effectiveness.

The culture that has been established in WBSDC is solely the Perfection, Performance and Productivity, believing on the team work and finding out a solution for the most mission critical requirements.



It is concluded with the belief that WBSDC will continue to cater and suffice the needs and necessities of the different Government Departments with the resources & services available with it to the best possible extent as per the standard practice.

## 12. References

- i. Websites
  - a. <http://ec.europa.eu/enterprise/contracts-grants>
  - b. [http://its.ucsc.edu/core\\_tech/dco/](http://its.ucsc.edu/core_tech/dco/)
  - c. [http:// www.mit.gov.in/](http://www.mit.gov.in/)
  - d. [http:// www.uis.harvard.edu/](http://www.uis.harvard.edu/)
- ii. National Informatics Centre-Securities & Policies
- iii. Request For Proposal (RFP)
- iv. Solution Document(Provided by DCO)
- v. A Few Minutes of the Meetings
- vi. DCO Contract Copy

Developed by:

**Composite Team**  
**E-Gov Infrastructure**

Published by:

**Information Technology Department**  
**Government of West Bengal**

