OFFICE MEMORANDUM

Subject: Guidelines for cloud selection framework

In addendum to the OM no. 3(26)/2024-EG-II dated 27th November 2024, these guidelines have been prepared to provide guidance to the Central Ministries/Departments for cloud selection framework for hosting applications/data and procurement approaches.

The purpose of this Office Memorandum is to provide guidance to end-user Ministries/Departments to select an appropriate cloud to host applications and data based on their sensitivity and criticality. These guidelines also cover cloud procurement strategy from the various cloud offerings provisioned by various providers.

2.   Ministries/Departments are required to classify their applications and data into the categories of workload defined in the National Information Security Policy & Guidelines (NISPG) of Ministry of Home Affairs (MHA) prior to the selection of the appropriate cloud offered. As per NISPG, workload categorized as Top secret and Secret are not permitted to be hosted on cloud. Applications and data other than Top Secret, and Secret are classified into two categories namely Category A and Category B.

The definitions of the categories of Application and data are given as below:

i. **Category A:** Applications and data, unauthorized disclosure of which could be expected to cause damage to the security of the organization or could be prejudicial to the interest of the organization or could affect the organization in its functioning. Any compromise could cause serious harm to national security or national interests, disrupt government operations, business continuity, and result in significant financial losses.

ii. **Category B:** Applications and data, which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose or requires no protection against disclosure. Any compromise could cause limited operational disruption and minor to significant financial loss.

3.   An indicative approach that maps applications and data categories with cloud deployment options and is outlined in the Table 1 below:

Table 1: Indicative mapping of applications and data classification to cloud deployment options

Category of applications and data	Data sets	Cloud deployment options	Safeguards
Category A	Applications and data that may adversely impact the security, financial aspects, or operational stability Examples: 1) Government of India Examples: Aadhaar, e-Courts, PAN, Passport, Railways, Tax, UPI, Voter ID, etc. 2) State Government Examples: CCTNS, Jail, Land records, Land registration, Revenue Courts, Treasury, etc.	**Option 1:** **Government providers:** - NIC provisioned Data Centre/cloud services - Entities defined in Section 4i(c) - State Data Centres' Data Centre/cloud services	**Government providers:** - DR* setup with Government provider and regular backup
		Option 2: Sovereign cloud providers as and when notified by MeitY	**Private providers:** - DR setup with Government provider and regular backup
Category B	Applications and data which is disclosable under the RTI and subject to the provisions of DPDP Act. Examples: Welfare schemes, websites, public grievance / feedback, events related data	All the above-mentioned cloud deployments under Category A (Option 1 and Option 2) along with the option by private provider as mentioned below may be considered. **Private providers:** - MeitY empaneled CSPs offering VPC*/PC* -DIC/NICSI	**Private providers:** - DR setup and regular backup with redundancy

DR* - Disaster Recovery, VPC* - Virtual Private Cloud, PC*- Public Cloud

4. Procurement approaches

The procurement of cloud services shall be carried out in accordance with the General Financial Rules, 2017. States and other concerned organisations may follow their respective State laws and applicable procurement rules. The above-mentioned deployment options are available to Government departments through the approaches that are mentioned as below:

i. Nomination

For availing such cloud services, purchase orders may be placed on a nomination basis in accordance with Rule 204 of the General Financial Rules, 2017.

a) National Informatics Centre (NIC)

National Informatics Centre (NIC) provides secure and resilient DC/cloud services, including PPP-based hybrid cloud, and co-location facilities.

b) State Data Centres

Various State Data Centres across the country are providing centralized and secure Data Centre and cloud services to State Government departments.

c) Public Sector Undertakings (PSUs) or entities under MeitY offering cloud services

Ministries/Departments may consider PSUs/ MeitY entities offering cloud services under the nomination route, on condition that such organizations have onboarded the Cloud Service Provider (CSP), providing the underlying cloud infrastructure through a fair and transparent procurement process, such as GeM or through an open RFP.

Ministries/Departments can engage with organization such as Bharat Sanchar Nigam Limited (BSNL), Centre for Development of Advanced Computing (CDAC), Indian Telephone Industries (ITI) Limited, Power Grid Corporation of India Limited (PGCIL), RailTel, and Telecommunications Consultants India Limited (TCIL), etc. for procurement.

ii. **Rate Contracting**

a) Digital India Corporation (DIC)/National Informatics Centre Services Incorporated (NICSI)

DIC has already discovered the cloud rates of major hyperscalers through competitive tenders. These rates, which are discovered on time-to-time basis apply to a range of CSPs/MSPs, that ensure transparency, standardization, and cost-efficiency. DIC/NICSI's cloud service rates may be leveraged for rapid procurement, which has periodic re-evaluation to adjust for changes in market conditions and technology offerings. The rates for cloud services offered by DIC are available on https://dic.gov.in/notification/.

iii. **Open RFP/GeM**

a) Cloud Service Providers empaneled by MeitY

MeitY has empaneled the cloud service offerings of CSPs (Private providers, PSUs, MSMEs) to provide cloud services to the Government departments. The list of CSPs offering various deployment options (public cloud; virtual private cloud; and government community cloud) is available on AMBUD portal (www.ambud.meity.gov.in).

5.   Further, in situations where Ministries/Departments require assistance in determining the appropriate cloud deployment options for hosting their applications and data, they may constitute an internal committee, wherein, a representative of MeitY may be nominated to advise on the selection of cloud deployment.

6.   It may be noted that this document is intended to follow best practices for hosting applications and data on a suitable cloud. It does not impose any mandatory obligations or

restrictions on any Government department to comply with the advisory contained herein. It is the prerogative of the end user department to judiciously classify the applications and data of their organisation that may be suitable as per the indicative framework mentioned in Table 1 above.

7. This issues with the approval of competent authority.
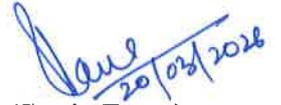
(Sonia Rana)
Under Secretary
Tel: 011-24301554

To:
1. Secretaries in charge of Ministries/Departments, Government of India
2. Chief Secretaries of States
3. Chief Executive Officer, NITI Aayog
4. Chairman and Chief Executive Officer, Railways Board

Copy to:
1. Director General, National Informatics Centre / Centre for Development of Advanced Computing / BISAG-N / Software Technology Parks of India
2. Managing Director, NICSI
3. Managing Director and Chief Executive Officer, Digital India Corporation
4. President and Chief Executive Officer, National e-Governance Division, Digital India Corporation
5. Chief Executive Officer, Bhashini Independent Business Division / India AI Mission, Digital India Corporation