Approved by Ministerial decision Dated: 2025-01-28

Data Center and Cloud Service (Operation and Management) Directives, 2081

Preamble: Whereas it is expedient to encourage the secure and confidential storage of data within the country created by the government, public, and private sectors through the use of information technology, and to make the information technology system reliable, secure, and effective through the listed data centers and cloud service providers and management thereof,

It is, therefore, the Government of Nepal, Ministry of Communication and Information Technology, in exercise of the powers conferred by Section 79 of the Electronic Transactions Act, 2063 (2008), has formulated the following directives.

1. **Short title and commencement:** (1) This Directives may be called as the Data Center and Cloud Service (Operation and Management) Directives, 2081 (2025)."

   (2) These directives shall come into effect from the date of approval by the Government of Nepal, Ministry of Communication and Information Technology.

2. **Definitions:** Unless the subject or the context otherwise requires, in this Directives,-
   (a) "Center" means National Cyber Security Center.
   (b) "Cloud service" means the hardware and software-integrated infrastructure prepared by a data center service provider or other entity to

operate (Host) information technology systems developed by the government, public, and private sectors.

(c) "Data" means a formal representation of information, knowledge, or instructions in the form of letters, numbers, images, sounds, or audio-visuals that are being formally prepared or have been prepared for its use in a computer, computer system, or computer network, or produced by a computer, computer system, or computer network.

(d) "Data Center" means a center with the necessary infrastructure for the storage of data and the operation of information technology systems by the government, public, and private sectors.

(e) "Department" means the Department of Information Technology.

(f) "Ministry" means Ministry of Communication and Information Technology.

(g) "'Government Agency" means a ministries of Government of Nepal, secretariat or offices subordinate to it, constitutional body or offices subordinate to it, judicial authority, provincial government or offices subordinate to it, local level or offices subordinate to it, and this term shall also refer to other offices of a similar nature.

(h) "Public Body" means the following bodies:-

(1) A company, bank, committee or institution fully or partially owned or controlled by the Government of Nepal, provincial government, or a local level; or commission, organization, authority, corporation, enterprise, board, center, council, and other similar incorporated institutions established under prevailing law.

(2) A university, school, research center, and other similar academic or educational institutions operated by the Government of Nepal,

provincial government, or local level, or fully or partially funded by the Government of Nepal, provincial government or a local level.

(3) An institution operated with loans, grants, or guarantees from the Government of Nepal, provincial government, or local level.

(4) An institution fully or partially owned or controlled by, or receiving grants from, the institutions mentioned in sub-sections (1), (2), or (3) and,

(5) Other institutions designated as public body by the Government of Nepal through the publication of a notice in the Nepal Gazette.

3. <u>Listing of Data Center and Cloud Service Providers:</u> (1) Data center and cloud service providers shall be listed with the Department before providing services.

(2) An organization intending to operate a data center and provide services as per sub-section (1) shall submit an application in the format prescribed by the Department, along with the following details:-

(a) Registration certificate of Company/firm,
(b) Assurance of fire safety,
(c) Building completion certificate,
(d) Security and Privacy Policy of the organization,
(e) Documents related to the Business Continuity Plan,
(f) Map of the location where the data center shall be situated,
(g) Details regarding the Tier of the data center,
(h) Details of the technical personnel involved in the operation of the data center,

(i) Details of the methods and procedures adopted for the physical security of the data center,

(j) Details of the IP Pool available in its name,

(k) High-level electrical design,

(l) In case of not owning the building/land, the agreement letter with the building/land owner,

(m) In the case of operational data centers, a certificate related to the Information Security Related Standard for both DC and DR within six months of being listed.

(3) An organization intending to provide services by operating cloud service as per sub-section (1) shall submit an application to the Department along with the following details:-

(a) Registration certificate of Company/firm,

(b) Security and Privacy Policy of the organization,

(c) Details of the technical personnel involved in the operation of the data center,

(d) Documents related to the Business Continuity Plan

(e) Map of the location where the data center shall be situated,

(f) Agreement with the data center,

(g) Details regarding affiliation with ISP/NSP

(h) Details of IP Pool available in one's name, and

(i) Certificate related to Information Security Related Standard and Information Technology Service Management Standard for the cloud services listed in the data center within the last six months.

(4) Data center operators operating at the time of commencement of this directive shall, in accordance with sub-section (2), and cloud service providers shall, in accordance with sub-section (3), submit an application for mandatory registration to the Department within six months from the commencement of this directive, along with the documents related to sub-section (2) or (3).

(5) Data center operators submitting an application as per sub-section (4) shall also attach a certificate related to the *Information Security Related Standard for both DC and DR* and cloud service providers shall attach certificates related to *Information Security Related Standard* and *Information Technology Service Management Standard*.

(6) Notwithstanding anything mentioned in sub-sections (2) or (3), public bodies operating data centers or cloud services are not required to submit a company or firm registration certificate for listing purpose.

(7) In the case of government data centers and cloud service providers, it shall be mandatory for the security agencies of the Government of Nepal to use the data center and cloud services operated by the Integrated Data Management Center.

(8) Notwithstanding anything written in sub-section (7), there shall be no hindrance to operating the infrastructure currently collocated within the integrated data management center at the time of the commencement of this directive.

(9) At the time of the commencement of this directive, government bodies operating agency-wise departmental data centers and cloud services

shall transfer them to the government data center within the timeframe specified by the steering committee. However, if a government body requests to operate a Primary/Secondary Site with sufficient justification, the steering committee may give consent to operate such a site based on its suitability.

(10) For applications received as per sub-sections (2), (3) or (4), the department, upon investigation and physical inspection, may request necessary documents from data center and cloud service providers during the listing process.

(11) It shall be the duty of the applicant to provide certified copies of such documents to the department wherein documents are requested as per Sub-section (10).

(12) If the department, after investigation and physical inspection as per Sub-section (10), finds that the necessary procedures have been completed, it may list the data center and cloud service within one month.

(13) For the purpose of this section, service providers wishing to operate both data center and cloud services shall be listed separately.

4. **Details to be updated:** Data center and cloud service providers listed under Section (3) shall update their details through the medium specified by the department by the end of Poush every year.

5. **Removal from the List**: (1) The department may remove data center and cloud service providers listed by it from the list under the following circumstances:

(a) If it is found that the conditions specified by the department under this directive have not been complied with.

(b) If it is found that data stored in the data center and cloud has been misused.

(c) If the organization is dissolved.

(d) If the data center or cloud service operator applies for cancellation of their listing.

(2) In cases falling under clauses (a) and (b) of Sub-section (1), the data center operator or cloud service provider shall be given fifteen days to present their clarification before being removed from the list.

(3) After receiving the clarification as per Sub-section (2), the department may conduct further necessary investigation regarding the content of that response.

(4) In case the clarification is not received within the time frame specified in Sub-section (2) or it is deemed appropriate to remove the data center and cloud service provider from the list upon investigation of the received clarification as per Sub-section (3), the department shall remove them from the list within seven days.

(5) If the data center or cloud service provider themselves apply for cancellation of their listing, the department may remove them after completing the necessary procedures.

(6) The department shall publish the details of data center and cloud service providers removed from the list under this section in a national daily newspaper and on the department's website.

6. **Tiers of Data Center**: (1) Data centers shall perform tier rating based on the physical infrastructure available and the services they provide.

(2) The minimum criteria for tier rating as per Sub-section (1) shall be as specified in the schedule. Data center service providers shall submit the tier rating certificate to the department within the year their data center is listed.

(3) Data center service providers storing government data shall achieve at least tier three or higher among the tiers mentioned in the schedule.

7. **Conditions needed to be fulfilled by Data Center and Cloud Service Providers:** (1) Data center and cloud service providers shall provide equal access to services for everyone.

(2) In the case of government data centers, arrangements shall be made to store data from government bodies only.

(3) Data center and cloud service providers shall adopt necessary security standards for the security of data stored in the data center and cloud.

(4) Service providers shall make necessary security arrangements to protect client data and control unauthorized use and access without permission.

(5) Data center and cloud service providers shall ensure the continuity of the services they provide.

(5) In case any unauthorized access is found despite sufficient security measures, the regulatory body and the center shall be informed immediately

through the fastest possible means. Additionally, necessary actions shall be taken to neutralize such unauthorized access.

(6) Data center and cloud service providers shall appoint a Compliance Officer to ensure compliance with international standards, or they shall obtain services from an organization related to compliance.

(7) Data center and cloud service providers shall submit the details requested by the department to the department within the specified time.

(8) Data center and cloud service providers shall conduct a security audit of their infrastructure at least once annually.

(9) On operating any system through cloud service, the security and backup of the system and data shall be specified in a bilateral agreement to commence the service.

(10) Data center and cloud service providers shall comply with the directions of the department and law enforcement agencies.

(11) Necessary assistance shall be provided wherein any entity/individual, for any reason, wishes to remove infrastructure placed in the data center and cloud or transfer systems hosted on the cloud elsewhere,

(12) If a data center and cloud service provider is dissolved as per prevailing law, or if the relevant entity/person wishes to move their infrastructure, it shall be securely transferred.

(13) In addition to the responsibilities and obligations mentioned in this directive, data center and cloud service providers shall manage the following as necessary:-

(a) Appropriate server racks for housing servers.
(b) Availability of network equipment such as Firewalls, Routers, and Switches,
(c) Availability of Server and Storage Devices for data storage,
(d) Proper arrangement of HVAC (Heat, Ventilation, and Air Conditioning),
(e) Proper arrangement for fire safety, including Fire Extinguishers,
(f) Arrangements for sufficient and regular availability of internet and electricity,
(g) Availability of an IP Pool in the name of the data center operator,
(h) Availability of necessary technical personnel,
(i) Arrangement of an Access Control System at the server location of the data center,
(j) Arrangement of personnel related to the physical security of the data center,
(k) Proper arrangement of Closed-Circuit Television (CCTV) in the data center, and arrangement for Data Center Infrastructure Monitoring,
(l) Arrangement of a Network Operation Center (NOC) for regular monitoring of Network Equipment such as Firewalls, Routers, and Switches,
(m) Proper arrangement of Security Devices as needed for the security of data stored in the data center,

(n) Arrangement for Colocation of customers' servers for data storage,

(o) Arrangement for regular backup of stored data,

(p) Technical personnel who have gained certification or are experienced in relevant fields,

(q) Arrangement for authorized personnel only to enter the server location,

(r) Arrangement for keeping records of visitors to the data center,

(s) Arrangement for Closed Circuit Television (CCTV) data storage for at least three months prior,

(t) If Hard Disks need to be destroyed, arrangements are made so that data cannot be recovered.

8. **Client's Duties, Responsibilities, and Rights:** (1) Before using data center and cloud services, any client shall only obtain services from providers listed in the department's published list**.**

(2) In case an information is received that a data center and cloud service provider is no longer suitable for receiving services and has been removed from the department's list, their machinery, tools, and systems shall be immediately and securely transferred from such service provider to another equivalent location.

(3) If any unauthorized access to a system is detected, the client shall inform the data center and cloud service provider, pay attention to security arrangements and options for system operation, and immediately notify the center in writing if a forensic investigation is necessary.

(4) The client shall comply with standards related to the secure use of the system.

9. **Duties, Responsibilities and Rights of Department:** The department shall have the following duties, responsibilities, and rights:-

(a) To prepare necessary plans for the management of data center and cloud service providers and submit them to the steering committee,

(b) To coordinate and facilitate the resolution of problems encountered in the operation of data center and cloud services,

(c) To monitor operating data center and cloud service providers,

(d) To inform the concerned bodies if a service provider fails to comply conditions,

(e) To publish the list of data center and cloud service providers on the department's website,

(f) To perform other prescribe tasks designated by the Government of Nepal, ministry and the steering committee for the operation and management of data center and cloud services.

10. **Duties, Responsibilities, and Rights of the Integrated Data Management Center:** (1) The duties, responsibilities, and rights of the Integrated Data Management Center shall be as follows:-

a. To prepare the necessary infrastructure for equipment colocation related to IT service delivery of government bodies and ensure the availability of colocation space**.**

b. To ensure the continuous availability of cloud virtual resources necessary for government bodies to host IT-related systems.

c. To perform necessary SLAs for the colocation services and cloud virtual resource services provided to each government body,

d. To ensure the uninterrupted nature of data center and cloud services through SLAs,

e. To conduct a security audit of data center and cloud services at least once annually.

11. **Functions, Duties, and Rights of the Center:** (1) In the event of unauthorized access to the system of any government body, the Center shall conduct a forensic investigation and provide a report upon request from the concerned system-operating agency. In the case of other agencies, the Center may obtain forensic investigation services from institutions listed by the Center.

(2) The investigation report pursuant to sub-section (1) shall be submitted to the requesting body or individual within one month.

12. **Formation of Steering Committee**: (1) For the management and coordination of data centers and cloud services, there shall be a Steering Committee as follows:-

(a)	Secretary, Ministry of Communication and Information Technology	– Chairperson
(b)	Joint Secretary (Information Technology), Office of the Prime Minister and Council of Ministers	– Member
(c)	Joint Secretary, Ministry of Home Affairs	– Member
(d)	Joint Secretary, Ministry of Finance	– Member

(e)	Joint Secretary, Ministry of Energy, Water Resources and Irrigation	– Member
(f)	Joint Secretary (Information Technology), Ministry of Communication and Information Technology	– Member
(g)	Chief, National Cyber Security Center	– Member
(h)	An expert as designated by the department with at least ten years of experience in data center and cloud services	– Member
(i)	Director General, Department of Information Technology	–Member Secretary

13. **Meeting of Steering Committee:** (1) The meeting of the steering committee shall meet as per necessary.

(2) The date, venue and time of the meeting of the steering committee shall be conducted as determined by chairperson.

(3) The quorum for the meeting of Steering Committee shall be considered met if more than fifty percent of the members are present.

(4) The chairperson of the committee shall preside over the Steering Committee meeting.

(5) The majority opinion shall be valid at the Steering Committee meeting, and the chairperson shall cast the deciding vote in case of a tie.

(6) The member-secretary shall certify the decisions of the Steering Committee meeting.

(7) The Steering Committee may invite subject matter experts as needed.

(8) Other arrangements related to the meeting of Steering Committee shall be as determined by the committee itself.

14. **Duties and Responsibilities of the Steering Committee:** In addition to the duties and responsibilities written elsewhere in this directive, the duties and responsibilities of the Steering Committee shall be as follows:

(a) To coordinate as necessary for the effective implementation of this directive.

(b) To prepare standards for data center and cloud service management and operation and recommend to the Ministry for approval.

(c) To coordinate with relevant ministries for data center and cloud service management and operation.

(d) To coordinate at inter-ministerial level, provinces, and local levels.

(e) To provide necessary directions and coordination regarding the work of the department and the center.

(f) To perform other necessary works related to data center and cloud services management and operation

15. **Monitoring and Evaluation**: (1) The Ministry shall monitor the implementation of this directive.

(2) The effectiveness of this directive's implementation shall be evaluated at least two years from the date it comes into force.

16. **Power to Interpret**: The Ministry shall provide necessary interpretation in cases where there is any ambiguity regarding the implementation of this directive.

Schedule

(Related to sub-section (2) of Section 6)

Tier	**Features to be included in the Data Center** (Note: Reference taken from Uptime Institute)
Tier One	• Distribution path Power and Cooling: 1 • Redundant Active Component: N • Redundancy Backbone: No • Redundancy Horizontal Cabling: No • UPS/Generator: Optional • Concurrently Maintainable: No • Fault Tolerant: No • Availability (uptime within year): 99.671% • Downtime should be less than 28.8 hours a year • 12 hours power backup for all equipment inside the data center in case of electricity breakage
Tier Two	• Distribution path Power and Cooling: 1 • Redundant Active Component: N

	• Redundancy Backbone: No • Redundancy Horizontal Cabling: No • UPS/Generator: Yes • Concurrently Maintainable: No • Fault Tolerant: No • Availability (uptime within year): 99.749% • Downtime should be less than 22 hours a year • 12-24 hours power backup for all equipment inside the data center in case of electricity breakage
Tier Three	• Distribution path Power and Cooling: 1 active/1 alternative • Redundant Active Component: N+1 • Redundancy Backbone: yes • Redundancy Horizontal Cabling: No • UPS/Generator: Yes • Concurrently Maintainable: Yes • Fault Tolerant: No • Availability (uptime within year): 99.982% • Downtime should be less than 1.6 hours a year • 24-48 hours power backup for all equipment inside the data center in case of electricity breakage
Tier Four	• Distribution path Power and Cooling: 2 active • Redundant Active Component: 2(N+1) • Redundancy Backbone: yes • Redundancy Horizontal Cabling: Optional

	• UPS/Generator: Dual • Concurrently Maintainable: Yes • Fault Tolerant: yes • Availability (uptime within year): 99.995% • Downtime should be less than 26.3 minutes per year • 48 hours power backup for all equipment inside the data center in case of electricity breakage