PIONEER
LAW ASSOCIATES

Data Centre and Cloud Services (Operation and Management) Directive 2081 – Brief

The Data Centre and Cloud Services (Operation & Management) Directive 2081 (the "Directive'') is issued by the Government of Nepal, Ministry of Communication and Information Technology, under Section 79 of the Electronic Transactions Act, 2063. The Directive was issued on 10 February 2025.

1) Listing with the Department of Information and Technology (the "Department")

A) The Directive mandates that Data Centers and Cloud Service Providers (the "Service Providers") must be registered with the Department of Information and Technology before offering their services.

B) The Directive defines Cloud Services as refers to the integrated technology that enables the hosting of information processing systems developed by government, public, and private sectors using data center services or other sources, incorporating both hardware and software. Likewise, the Data center has been defined as a facility that includes the necessary infrastructure to store and operate data and information technology systems developed by government, public, and private sectors

C) The Company/Firm (Organization) that want to operate or provide services as Service Providers must be listed in the Department. In order to list in the Department, the concerned company/firms need apply (in the prescribed format) to the Department along with the following details:

<table>
<tr><th>Data Centre</th><th>Cloud Services</th></tr>
<tr><td colspan="2">Certificate of Incorporation of Company/Firm
Security and Privacy Policy of the Organization
Documents related to Business Continuity Plan
Details of IP Pool available in your name</td></tr>
<tr><td>Ensuring Fire Safety
Building Completion Certificate
Map of the location of the Data Centre
Details regarding tier of the Data Centre Details of technical manpower involved in data center operations
Details of methods and procedures to be adapted for the physical security of the data center
High level electricity design
For Data Centers currently in operation, a certificate related to Information Security Standards for both DC and DR must be submitted within the 6 months of listing.</td><td>Details of the technical manpower involved in the operation of the cloud service
Map of the location of the data center where the cloud service is operated.
Agreement with the data center.
Details regarding affiliation with ISP/NSP
For Cloud Services currently in operation, a certificate related to Information Security Standards and Information Technology Service Management Standards must be submitted within 6 months of listing.</td></tr>
</table>

D) Service Providers currently in operation must submit an application to the Department with the required documents (provided above) **within six months** of issuance of this Directive's initiation. Additionally, Data Center Operators must provide certificate related to Information Security Related Standard for both DC and DR and Cloud Service operators must provide certificate related to Information Security Related Standard and Information Technology Service Management Standard.

E) During the examination and inspection of applications, the Department may request additional documents from Service Providers. It is the responsibility of Service Providers to provide the required documents. If the necessary procedures are completed following the inspection, the Department may list the Data Center and Cloud Services within one month. **Note**: Service Providers operating both Data Center and Cloud Services must apply for separate listings.

F) Service Providers must update their details in the means as prescribed by the Department every year at the end of Month of Poush (Mid-January).

2) Removal from Listing of the Department

A) Service Providers listed by the Department may be removed in the following cases:
a) Non-compliance with the Directive's rules
b) Misuse of data stored in the Data Center or Cloud Service Center
c) Dissolution of the Company/Firm
d) Request for cancellation of registration by the Service Providers.

B) The Service Provider will be given **15 days** to submit their justification before removal from the list. The Department will investigate the response. If no justification is received, or if the investigation of the justification deems removal necessary, the Department will remove the provider from the list within **7 days**. If the Data Center or Cloud Service provider applies for cancellation of registration, the Department may remove it after completing the necessary procedures. The Department will publish the details of removed providers in a national newspaper and on its website.

3) Tier Rating of Data Center

A) Data Centers will receive a "Tier Rating" based on their physical infrastructure and services, categorized as:

Tier-1	**Tier-2**
• 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 of power backup for all equipment inside the datacenter in case of electricity breakage	• Distribution path Power and Cooling:1 • Redundant Active Component: N • Redundancy Backbone: NO • Redundancy Horizontal Cabling: No • UPS/Generator: Yes • Concurrently Maintainable: No • Fault Tolerance: No • Availability (uptime within year): 99.749% • Downtime should be less than 22 hours a year • 12-24 hours of power backup for all equipment inside the datacenter in case of electricity breakage
Tier-3	**Tier-4**
• 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 of power backup for all equipment inside the datacenter in case of electricity breakage	• 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 or more of power backup for all equipment inside the datacenter in case of electricity breakage

B) The Data Center Service Provider must submit the tier rating certificate to the Department within one year of listing. Further, any Data Center storing governmental data must have at least 3 tier rating or above.

4) Compliance Requirements for Service Providers

- Service Providers must offer equal access opportunities to all
- Must adopt necessary security standards for data storage in the data center and cloud.
- Must implement security measures to protect customer data and prevent unauthorized access.
- Should ensure service continuity.
- In case of unauthorized access, despite adequate security, it must be reported to the regulatory body immediately, and actions should be taken to eliminate the breach.
- Must appoint a Compliance Officer or obtain services from an organization to ensure compliance with international standards
- Must submit the requested details to the Department within the specified time
- A security audit of their infrastructure must be conducted at least annually.
- When operating a system through cloud services, the security and backup of the system and data should be outlined in a bilateral agreement.
- Must follow instructions received from the Department and law enforcement agencies.
- If an entity/person wishes to remove infrastructure or transfer hosted systems to another location, necessary assistance must be provided.
- If terminated under prevailing laws or if a transfer is requested, secure transfer must be ensured.
- In addition to the responsibilities and obligations outlined in the Directive service providers must manage the following aspects as necessary:

a) Provision of suitable server racks for server placement,
b) Availability of network equipment such as Firewalls, Routers, Switches,
c) Availability of servers and storage devices for data storage,
d) Proper arrangement for HVAC (Heat, Ventilation, and Air Conditioning),
e) Adequate provision for fire safety, including Fire Extinguishers,
f) Arrangement for adequate and regular availability of Internet and electricity,
g) Availability of an IP pool in the name of the data center operator,
h) Availability of required technical personnel,

i) Provision of an Access Control System at the location of the data center servers,
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, along with a system for monitoring data center infrastructure.
l) A provision for a Network Operation Center (NOC) to regularly monitor network equipment such as Firewalls, Routers, and Switches.
m) Proper arrangement of security devices as needed to ensure the security of the data stored in the data center.
n) Provisions for server colocation for clients for data storage.
o) Arrangements for regular backup of the stored data.
p) The technical staff must have certification or experience in the relevant subject matter.
q) Must be a system in place to allow only authorized personnel to access the server location.
r) Must be a system to maintain a record of visitors who visit the data center.
s) Must be a system in place to store Closed-Circuit Television (CCTV) data for at least three months.
t) If hard disks need to be destroyed, there must be arrangements to ensure that the data cannot be recovered.

Pioneer Law Associates Pvt. Ltd.
Regd. No. 38549/062/063
Pioneer House, 246-Sahayog Marg,
Anamnagar, Kathmandu, Nepal.

Phone No.: +977-1-5705340, +977-1-5707102
Email: info@pioneerlaw.com,
www.pioneerlaw.com

PIONEER
LAW ASSOCIATES