PRADHAN & ASSOCIATES
ATTORNEYS AT LAW

Client Briefing
February 26, 2025

Data Center and Cloud Service (Operation and Management) Directive, 2081 (2025 A.D.)

Introduction

On February 10, 2025, the Ministry of Communication and Information Technology ("MOCIT"), published the Data Center and Cloud Service (Operation and Management) Directives 2081 (2025 A.D.) ("DCCS Directives"). The DCCS Directive, enacted under the authority conferred by the Electronic Transactions Act, 2063 (2006 A.D.), establishes the foundational legal framework to regulate data centers ("Data Centers") and cloud services ("Cloud Services") (collectively "Service Providers") in Nepal. Nepali version of DCCS Directives can be accessed here.

This Briefing aims to highlight the major provisions of DCCS Directives.

Definitions

Key definitions of DCCS Directives include:

- **Cloud Service**: The infrastructure, including hardware and software, developed by data center service providers or other entities for hosting information technology systems developed by the government, public or private sectors.
- **Data:** The presentation of information, knowledge, concepts, or instructions formally prepared or created, or produced by computers, computer systems, or computer networks in the form of letters, numbers, images, sound, or audiovisual content for use in computers, computer systems, or computer networks.
- **Data Centre:** A facility equipped with the necessary infrastructure for the storage of data and the operation of information technology systems, developed by the government, public or private sectors.

Enrollment Requirements

DCCS Directives require Service Providers to be enrolled with the Department of Information Technology ("DOIT"). In order to enroll with DOIT, a Service Provider must submit an application along with the company/firm registration certificate, security and privacy policy, business continuity plan documents, location map, technical personnel details, and IP pool details, etc.

In addition, Data Centers must submit additional documents including fire safety assurance, building completion certificate, data center tier details, physical security methods, high-level electrical design, and an agreement with the land/building owner (if applicable). Similarly, Cloud Services must submit agreements with the data center and ISP/NSP affiliation details. An entity, that wishes to engage in both services, must enroll separately for each service.

Service Providers, who are already in operation, must submit their enrollment application to DOIT within six months from the date of enactment of DCCS Directives.
Data centers are required to provide an Information Security Standard certificate for both DC and DR, while Cloud Services must submit Information Security Related Standard and Information Technology Service Management Standard certificates.

DOIT will issue certificates of enrollment within one month after physical inspection of the infrastructure. DOIT reserves the authority to cancel the enrollment if it finds that a Service Provider is in violation of DCCS Directives.

Responsibilities of Service Providers

Service providers are under an obligation to ensure equal access, service continuity, and security for all users. Service Providers are also under an obligation to control unauthorized access, report breaches, and take corrective actions. In order to comply with international standards, Service providers must appoint a compliance officer or partner with an authorized institution. Service Providers are required to submit annual details to DOIT and also must conduct security audits annually.

Security and backup for cloud-hosted systems must be ensured through bilateral agreements. Service Providers are under an obligation to comply with instructions of DOIT and law enforcement agencies. They must also assist with the removal or transfer of infrastructure securely when decommissioning or relocating infrastructure.

Technical Requirements for Service Providers

Service Providers are required to fulfill the following technical requirements:

- Provide server racks, network equipment, servers, storage, and HVAC systems.
- Ensure fire safety, physical security, and sufficient technical personnel.
- Ensure reliable internet, electricity, and establish access control system and maintain IP pool.
- Install CCTV surveillance, store CCTV footage for 3 months, maintain visitor logs, and monitor infrastructure regularly.
- Set up a Network Operations Center (NOC) to monitor network equipment.
- Use security devices to protect data and offer colocation services.
- Securely destroy hard disks to prevent data recovery.

Data Center Tiers

Data Centers must conduct tier rating based on their physical infrastructures and submit a Certificate of Tier Rating to DOIT within a year from the enrollment. Data Centers that are engaged in storing government data must have a minimum of a Tier 3 rating.

Rights and Duties of Customers

- Customers must use services only from Service Providers enrolled with DOIT.
- If a Service Provider is removed from the enrollment list, customers must securely transfer their systems to another provider.
- In case of unauthorized access, customers must notify the Service Provider, consider security measures, and report to the National Cyber Security Center.
- Customers must follow system security guidelines.

Integrated Data Management Center

The Integrated Data Management Center ("Center") is responsible for preparing the infrastructure and ensuring colocation space for government IT services. The Center ensures the continuity of cloud/virtual resources for government systems and also ensures service continuity through SLAs.

Regulatory Supervision

DOIT

DOIT shall be the regulatory agency with the power to monitor the performances of Service Providers. It also coordinates with Service Providers to resolve operational issues.

Directorate Committee

The management and coordination of Data Centers and Cloud Services will be overseen by the Directorate Committee ("Committee"), chaired by the Secretary of MOCIT. Committee is primarily responsible for coordinating with various entities to manage and operate Data Centers and Cloud Services.

MOCIT

MOCIT is responsible for monitoring the implementation of DCCS Directives. The effectiveness of DCCS Directives will be evaluated after two years from the date of its enforcement. Similarly, MOCIT is granted with the authority to provide interpretation of DCCS Directives in case of ambiguity.

This Briefing is authored by:

Aadittya J. Kansakar
Associate Partner

Yagyadi Acharya
Associate

Mamata Thapa
Trainee Associate

For further information about the subjects covered in this Briefing, please contact:

Yagyadi Acharya
Associate
Tel: +977 1 545 5606 (Ext. 111)

For further information about the subjects covered in this Briefing, please contact:

PRADHAN & ASSOCIATES
ATTORNEYS AT LAW

Pradhan & Associates Pvt. Ltd.
559, Bakhundole Marg (Maitri Marg), Bakhundole – 3
Lalitpur - 44770, Nepal
Tel: +977 1 545 1900 | Fax: +977 1 543 3344
Email: info@pradhanlaw.com
Web: www.pradhanlaw.com