Terms of Reference (ToR) for Establishment of a New Cloud Infrastructure under Joint Venture (JV) with BDCCL

Assignment Title	Establishment of a New Cloud Infrastructure in BDCCL
Assignment Duration	Initial Agreement for 07 (Seven) Years; After completion of initial agreement, Renewal Basis 03 (Three) Years (On the basis of Mutual Agreement)
Primary Assignment Location	IV Tier Data Center, Kaliakoir Hi-Tech City, Gazipur,
Funding Source	The investor firm will provide all investment related to establishing new cloud infrastructure and related services.
Contracting Entity	Bangladesh Data Center Company Limited (BDCCL), Information and Technology Division, Ministry of Posts, Telecommunications and Information Technology

Section 1 – Background

Technology industries are establishing data centers all over the world to ensure redundancy and reliability of data and flow of information. To follow the trend Government of Bangladesh initiated the project titled "Establishment of Tier IV Certified National Data Center" in 2016. Built on seven acres of land in Kaliakoir Hi-Tech City, Gazipur, the Data Center is the first and only Tier IV certified facility in Bangladesh, featuring 604 rack spaces in 04 physically separated Cage Halls with 2N+1 redundancy in power, cooling, and passive infrastructure to ensure the highest levels of reliability and availability.
To manage this state-of-the-art facility, the Government of Bangladesh established Bangladesh Data Center Company Limited (BDCCL) on 16 September 2020 as a state-owned company, where Information and Communication Technology (ICT) Division is the custodian of the company on behalf of the Government. Classified as a KPI 1-A category establishment and designated as a Critical Information Infrastructure (CII), BDCCL serves as the only government company authorized to provide data center services to both public and private organizations.

BDCCL offers a comprehensive portfolio of services, including cloud, colocation, and managed services. Its cloud portfolio includes a government cloud established at one of the Cage Halls, featuring a dedicated region cloud deployment within the Data Center premises, where BDCCL provides cloud services supported by specialized technical expertise. In addition, BDCCL has introduced another cloud platform developed under a joint venture agreement, built on open-source technologies by the local talent pool. Alongside its cloud offerings, BDCCL provides colocation services established at Cage Hall-1, allowing both government and private organizations to host their own servers. A total of 136 4KW and 18 10KW 42U rack spaces have been allocated for colocation, with 55 4KW and 5 10KW 42U rack spaces still available.

Amongst 04 Cage Halls one (Cage Hall-2) remains empty that presents an opportunity for new investment and can be rendered operational through modest upgrades to the existing passive facilities. Besides, another among these 04 Cage Halls is Cage Hall-4, which has some vacant containments that are running an End of Life (EoL) Cloud Service and already has the necessary passive

facilities in place. Together with the currently vacant cage hall, and the vacant containments from the EoL Cloud Service, it is a timely opportunity for BDCCL to establish a new cloud platform. This investment is crucial for BDCCL to solidify its position as the trusted provider of digital infrastructure in Bangladesh, diversify its service offerings, and ensure the long-term profitability of the Tier IV National Data Center.

Section 2 – Objective

The aim of this initiative is to introduce a brand-new cloud infrastructure in BDCCL by putting in place an advanced, high-performance, on-premises cloud architecture. To implement the new cloud, BDCCL will provide a necessary infrastructural support related to power, cooling and other passive infrastructure and the investor firm will provide with the cloud stack according to the technical specification. This upgrade will support BDCCL's expanding business demands and act as the foundation for BDCCL's digital transformation strategy.

This initiative aims to:

a. To Introduce a resilient, cost-effective separate Public and Private cloud system with the existing data center infrastructure.
b. To strategically utilize the unallocated space turning unused assets into revenue-generating resources.
c. To Optimize the existing data center infrastructure with power usage and cooling efficiency for seamless integration and robust support for newly deployed cloud system.
d. To expand BDCCL's cloud portfolio beyond existing service offerings to meet diverse client needs, focusing on both Public and Private sector, as well as migrate any workload from existing cloud platforms.
e. To Implement comprehensive training, operational runbooks, and knowledge transfer to strengthen BDCCL's in-house capabilities.
f. To Improve the overall security posture by integrating advanced security tools to protect against evolving cyber threats.
g. To invest in a scalable and reliable platform that ensures long-term profitability and secures BDCCL's/JV's market position.
h. To avail any other business opportunities to utilize idle space in consultation and with prior approval from BDCCL.

Section 3 – Scope of Service

Bangladesh Data Center Company Limited (BDCCL) will engage in a Joint Venture to establish a sovereign cloud platform within its Data Center to deliver secure, scalable, and future-ready services for government, enterprise, and commercial clients. The cloud will deliver Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and emerging Anything-as-a-Service (XaaS) capabilities. It will ensure compliance with Bangladesh ICT regulations and international cybersecurity standards, while enabling expansion into next-generation technologies such as artificial intelligence (AI), the Internet of Things (IoT), 5G, and edge computing.

There will be separate public and private cloud stack in this cloud platform that will have hardware level separation with rack isolation enabling data isolation, privacy and enhanced cyber security.

a. Technical Requirements

The investor firm must demonstrate proven technical capacity to meet the requirements below, supported by relevant certifications, completed projects, and availability of qualified experts.

Ser	Category	Requirements
1)	Architecture	The platform will comprise of public and private cloud stack.
		Public cloud stack will serve all types of government ministries, establishments, organizations, companies, universities, educational establishments, banks, non-bank financial organizations, etc.
		Private cloud stack will serve all other private entities.
		The platform shall maintain hardware level separation with rack isolation while provisioning the cloud stack, in case of network transmission at least logical level separation is essential.
		The disaster recovery site including all data stored and maintained must also have hardware level separation with rack isolation.
2)	Compute Resource Provisioning	The platform shall enable allocation, scheduling, and lifecycle management (start, stop, suspend, terminate) of isolated compute units on demand.
		The platform shall support dynamic scaling of compute resources up and down.
		The platform shall support virtual machines (VM), bare-metal, and containerized workloads.
		The platform shall support orchestration of container workloads, including scheduling, scaling, service discovery, and lifecycle management.
		The platform shall support trending compute services, including: - Serverless functions (FaaS) - GPU/accelerated

Ser	Category	Requirements
		compute for AI/ML, HPC, and graphics - Edge compute support - Hybrid compute models
		The platform shall provide Infrastructure as a Service (IaaS) for compute, storage, and networking.
		The platform shall provide Platform as a Service (PaaS) for managed databases, middleware, container orchestration, and developer services.
		The platform shall support multiple operating systems, both licensed (enterprise/commercial) and free/open source.
		The platform shall support multiple databases, both licensed (commercial RDBMS/NoSQL) and free/open source.
		The platform shall support Bring Your Own License (BYOL) for Operating Systems under IaaS.
		The platform shall support Bring Your Own License (BYOL) for Databases and middleware under PaaS.
3)	Persistent Storage Services	The platform shall provide durable block storage with redundancy.
		The platform shall offer multiple performance tiers (NVMe, SSD, SATA).
		The platform shall support snapshots, versioning, and restores.
		The platform shall provide an application-aware, Hyper Converged Infrastructure (HCI) native Software-Defined Storage (SDS) that manages data and application metadata (e.g., Kubernetes namespaces/objects, secrets) to simplify backup/restore, snapshots, replication, and cloning.
4)	Object /Unstructured Data Storage	The platform shall provide scalable object storage for unstructured data.
		The platform shall ensure redundancy and durability of objects.
5)	Management and Automation	The platform shall support concurrent operation of VMs and containers in the same clusters with unified scheduling, policies, monitoring, and lifecycle management, including support for GPU-accelerated workloads.
		The platform shall provide intent-based orchestration enabling declarative onboarding ("one-click" or equivalent) and full Day-0/1/2 automation (deploy, upgrade, heal, migrate, scale) across compute, storage, and network.
		The platform shall support Container as a Service (CaaS), Virtual Machine as a Service (VmaaS), and GPU-as-a-Service on the same platform, managed through a common control plane, with multi-tenant isolation and per-tenant quotas/chargeback

Ser	Category	Requirements
6)	AI functionality	The platform shall have dedicated servers equipped with high-performance Graphics Processing Units (GPUs) or specialized Artificial Intelligence (AI) accelerators.
		The platform shall have separate node categories for large-scale model training, parameter-efficient fine-tuning, and low-latency inference workloads.
		The platform shall have a POSIX-compliant high-performance parallel file system for handling training checkpoints, intermediate data, and logs.
		The platform shall have unified tools for experiment tracking, model version control, and artifact storage through a centralized model registry.
7)	Networking & Connectivity	The platform shall support both IPv4 and IPv6 addressing to ensure full compatibility with existing and future networks.
		The platform shall support Bring Your Own IP (BYOIP) for enhanced flexibility in network management.
		The platform shall support Bring Your Own ASN (BYOASN) to facilitate seamless integration with existing network configurations.
		The platform shall support private network extension to customer-owned data centers, allowing secure hybrid connectivity without public internet exposure, leveraging proven secure solutions.
		The platform shall support tenant network isolation.
		The platform shall support dedicated private connectivity options (leased line, MPLS, secure tunnels that meet enterprise-grade standards.).
		The platform shall provide VPN services for secure remote access, utilizing established security protocols recognized in the industry.
		The platform shall support streaming services with low-latency delivery, specifically optimized for real-time applications.
		The Platform shall support True Stateless Computing with Service Profiles.
		The Platform should be built on a Zero Trust model and support advanced segmentation at multiple levels—across applications, containers, and the operating system.
		The platform shall provide centralized Elastic IP management to dynamically allocate/associate/release public IPs across VMs, containers, and services, with high availability control plane and policy-based assignment (e.g., per tenant/namespace).

Bangladesh Data Center Company Limited
BDCCL
ICT Division

Ser	Category	Requirements
		The platform shall support Single pane policy-driven management that can provide a single platform to manage cross-form-factor hardware and fabric-on-prem or in the cloud.
		The platform shall provide a virtual routing/gateway function with stateful L3/L4 firewalling and optional application-layer inspection, tenant segmentation with reusable policy templates, and optional DPI for telco-grade threat filtering.
		The platform shall integrate with a central policy engine for automated enforcement.
8)	Identity, Access & Authorization	The platform shall support multi-tenant identity management.
		The platform shall support Role-Based Access Control (RBAC) with hierarchical roles (admin, operator, tenant, resource-owner).
		The platform shall support Attribute-Based Access Control (ABAC) based on attributes such as user identity, role, group, location, resource type, or sensitivity classification.
		The platform shall enforce granular access management up to the individual resource level (e.g., VM, container, database, storage bucket, network segment).
		The platform shall allow resource-level delegation so that tenants can assign access rights within their environment.
		The platform shall log all administrative and user access actions for auditing.
9)	API, Interfaces & Portals	The platform shall provide REST APIs, CLI tools, and tenant portal for provisioning and automation.
		Interfaces shall support tenant-level customization and self-service.
		The platform shall provide a Cloud Management Portal for administrators to manage underlying hardware, infrastructure, and cloud stack.
		The platform shall provide a Customer Resource Monitoring & Observability Portal, enabling customers to log in and view status, health, and performance of their allocated resources.
		The platform shall provide a Customer Billing Portal, enabling customers to view and analyze billing across all consumed resources (compute, storage, networking, VPN, caching, streaming, PaaS, BaaS).
10)	Usage Tracking, Quotas, and Billing	The platform shall collect usage metrics for compute (VMs, containers, serverless, GPU), storage, networking, VPN, caching, streaming, PaaS, and BaaS.
		The platform shall enforce per-tenant quotas.
		The platform shall support a pay-as-you-go billing model, charging based on actual usage.

Ser	Category	Requirements
		The platform shall support unit pricing per resource type, including CPU-hour, container runtime-hour, GPU-hour, function execution count, GB storage/month, GB data transfer, VPN connection-hour, streaming throughput GB, caching volume GB, archive GB/month, managed service usage (PaaS), and backup protected GB (BaaS).
		The platform shall generate detailed usage reports and invoices per billing cycle.
11)	High Availability & Redundancy	The platform shall eliminate single points of failure.
		The platform shall support redundant components across compute, storage, and networking.
12)	Disaster Recovery & Backup	The platform shall maintain regular backups with defined RPO and RTO.
		The platform shall provide in-platform backup for VMs and containerized applications, supporting application-consistent snapshots, incremental and full backups, policy-driven retention, and cross-zone replication/restore.
		The platform shall support active-passive backup with automated promotion of standby sites.
		The platform shall support automated failover and failback.
		The platform shall provide geographic redundancy.
		The platform shall support self-service backup and restore per customer and per resource (VMs, containers, databases, file systems).
		The platform shall provide granular recovery options (file-level, volume-level, full system restores).
		The platform shall support long-term backup storage policies, including tiering to archival/cold storage.
		The platform shall enforce backup encryption in transit and at rest.
		The platform shall provide multi-tenancy aware backup isolation, so tenant backups remain secure and segregated.
		The platform shall provide usage-based billing for backup services.
13)	Platform Resiliency	The platform shall be designed with resiliency measures to reduce platform-wide failures and minimize downtime.
		The platform shall support self-healing mechanisms, automatically recovering failed services or nodes.
		The platform shall use fault isolation to ensure local failures do not cascade across the system.
		The platform shall support graceful degradation, maintaining partial service availability under component stress or outage.

Ser	Category	Requirements
		The platform shall include capacity headroom to absorb unexpected spikes in load without service interruption.
		The platform shall be continuously tested for resiliency through simulations such as fault injection and failover drills.
14)	Platform and Cloud Security	The platform shall enforce segregation of tenant traffic.
		The platform shall support enterprise grade firewall, packet filtering, IDS/IPS, and DDoS protection.
		The platform shall ensure encrypted communication for all traffic.
		The platform shall enforce isolation of tenants at compute, storage, and orchestration layers.
		The platform shall provide encryption of data at rest with secure key management.
		The platform shall support secure patch management and integrity validation.
		The offering shall include an independent/separate Security Operations Center (SOC), and the platform shall be capable of integrating with it for 24x7 security monitoring and incident management.
		The SoC shall provide threat detection, incident response, and forensic investigation.
		The SoC shall support SIEM with centralized log/event correlation.
		The SoC shall provide dashboards and periodic security posture reporting.
		The SoC shall support a knowledge base of adversary behaviors aligned with frameworks like MITRE ATT&CK, including attack lifecycle phases and target platforms.
		The SoC should natively identify data gaps for ATT&CK and Kill Chain use cases, check data availability, and recommend required data sources for implementing techniques and sub-techniques
		The platform shall use an enterprise grade NGFW from an OEM recognized as a Leader in the Gartner Magic Quadrant or Forrester Wave for Enterprise Firewalls, ensuring proven industry leadership and reliability."
15)	Monitoring, Logging, Alerts & Alarms	The platform shall monitor compute (VMs, containers, serverless), storage, networking, VPN, caching, streaming, and PaaS services.
		The platform shall centralize logs across tenants and resources.
		The platform shall support customizable alarms per customer and per resource, with tenant-defined thresholds.

Ser	Category	Requirements
		The platform shall provide health monitoring per resource and per tenant, visible to both tenants and administrators.
		The platform shall retain historical alarm data for compliance and trend analysis.
16)	Performance & Latency	The platform shall provision compute and network resources within defined latency thresholds.
		The platform shall maintain consistent performance under peak demand.
17)	Scalability	The platform shall scale compute, storage, network, VPN, caching, streaming, PaaS, and BaaS services elastically.
		The platform shall support horizontal expansion without redesign.
18)	Maintainability & Upgradability	The platform shall support rolling upgrades and patches with minimal downtime.
		Maintenance processes shall be documented and repeatable.
19)	Governance & Compliance	The platform shall comply with PCI-DSS for handling cardholder data and secure financial transaction processing.
		The platform shall comply with HIPAA regulations for the protection of electronic protected health information (ePHI), ensuring confidentiality, integrity, and availability in all healthcare data processing and storage.
		The platform shall comply with ISO/IEC 27001:2022 standards for information security management.
		The platform shall comply with the Bangladesh's Personal Data Protection Ordinance (PDPO) 2025 and National Data Governance Ordinance 2025 to ensure proper handling of personal data, data subject rights, and cross-border data transfers.
		The platform shall comply with Bangladesh's Critical Information Infrastructure (CII) Guidelines 2022.
		The platform shall comply with the Bangladesh's Cyber Security Ordinance, 2025 for national cybersecurity, incident reporting, and critical infrastructure protection.
		The platform shall align with BTRC directives on data privacy, telecom security, and lawful interception requirements.
		The platform shall follow ICT Division cybersecurity policies and national cloud computing guidelines.
20)	Operational Management	The platform shall define roles and responsibilities for operators, SOC staff, and tenants.
		The platform shall provide documentation, onboarding, training, and incident playbooks.
21)	Metrics, SLAs, and KPIs	The platform shall define SLA targets for uptime, performance, and response times.

Ser	Category	Requirements
		The platform shall define KPIs including utilization, scaling efficiency, customer satisfaction, security incident rates, and hybrid connectivity stability.
22)	Interoperability & Portability	The platform shall support migration of workloads and data using open formats.
		The platform shall support integration with external billing, monitoring, and IAM systems.
23)	Auditability & Traceability	The platform shall record all administrative and tenant actions.
		The platform shall support compliance audits and forensic investigations.
24)	Adaptability	Cloud-native readiness for AI, IoT, blockchain, and big data analytics.
		The platform shall demonstrate broad multi-vendor interoperability across x86 server platforms, NICs, GPUs, switches, and common enterprise/telco software stacks.
		In the event customer choses to purchase hardware or use existing hardware the cloud infra must support them.

b. Preparation of Cloud Stack

1) The Investor firm shall import, install, and commission the required hardware for the cloud platform. This includes physical inspection of the designated Cage Hall, racking of servers, storage systems, and networking equipment, and establishing connectivity.
2) The phase concludes when all devices are properly mounted, powered on, interconnected, and validated through basic system checks, ensuring readiness for subsequent testing and integration.
3) In the future, if BDCCL issues any directive to increase the Cloud capacity, resources or services to meet national technical or security requirements, the concerned party shall be obligated to implement such directive within a mutually agreed timeframe.

c. Indicative Build Capacity (Total)

Ser	Estimated Build Capacity for IaaS Cloud	Capacity
1.	Physical CPU (Intel X9)	7,000
	Physical CPU (AMD E4)	14,000
2.	Public to Private Cloud Ratio	To be proposed
3.	GPU	To be proposed
4.	Memory (TB)	**500**
5.	Block Storage (PB)	5
6.	Object Storage (PB)	5
7.	File Storage (TB)	150
8.	Network (IP Transit - Gbps)	10

Big Data Center Company Limited
BDCCL
ICT Division

d. Initial Build Capacity and Infrastructure Requirements

Build Capacity- Physical CPU	Intel X9 - **3,000**
	AMD E4 – **6,000**
Public to Private Cloud Ratio	To be proposed
GPU	To be proposed
Memory (TB)	**250**
Block Storage (PB)	**2.5**
Object Storage (PB)	**2.5**
File Storage (TB)	**50**
Transmission and Bandwidth	• 5 Gbps NTTN Transmission between BDCCL and the investor Firm • The investor Firm will connect with 1Gbps Internet from IIG-ISP network to complement its resiliency

Timeline: Not more than 09(Nine) months from the date of signing the contract, subject to mutually agreed business plan.

e. Testing

Testing will confirm that all installed hardware functions correctly and meets performance, stability, and reliability requirements. Activities will include diagnostics on servers, storage, and networking components, verification of redundancy and failover mechanisms, and performance benchmarking. All identified issues must be resolved prior to cloud integration and acceptance testing.

Timeline: Within 15 days of completion of cloud stack preparation.

f. Provisional Acceptance Testing (PAT) & Provisional Acceptance Certificate (PAC)

BDCCL (or an authorized third party) will conduct PAT to validate system functionalities, integrations, and performance benchmarks. Defects, if any, will be documented for resolution. Upon successful completion, BDCCL will issue a Provisional Acceptance Certificate (PAC).

Timeline: Within 1 month of the Testing Phase.

g. Final Acceptance Testing (FAT) & Final Acceptance Certificate (FAC)

FAT will be conducted after the warranty or observation period following PAC. This test will confirm that all defects are resolved, the system remains stable under real operating conditions, and all contractual obligations are fulfilled. Upon successful completion, BDCCL will issue a Final Acceptance Certificate (FAC).

Timeline: Within 15 days of PAC issuance.

h. Go Live/ Commercial Operation

Following issuance of FAC, the cloud platform will be launched for real users. The contract period will commence on the Go Live date. The Investor Firm shall continue fine-tuning system operations throughout the contract duration.

Timeline: Immediately after issuance of FAC.

i. Remaining Build Capacity and Infrastructure Requirements

Any expansion is dependent on the market demand, capacity utilization, client needs etc. Considering the factors mentioned, investment should be made in a modular approach with a minimum 06 (Six) month Leadtime. In case of any special need from the BDCCL or any other Government agencies for immediate transfer of data and storage the Investor company shall be able to deliver it within 09 (nine) months.

Build Capacity- Physical CPU	Intel X9 - **4,000**
	AMD E4 – **8,000**
Public to Private Cloud Ratio	To be proposed
GPU	To be proposed
Memory (TB)	**250**
Block Storage (PB)	**2.5**
Object Storage (PB)	**2.5**
File Storage (TB)	**100**
Transmission and Bandwidth	• 5Gbps NTTN Transmission between BDCCL and the investor Firm • The investor Firm will connect with 1Gbps Internet from IIG-ISP network to complement its resiliency

Section 4 – Business Model

BDCCL and the Investor Firm will establish a Joint Venture (JV) under a Revenue Sharing Model to launch a new cloud platform.

a. Investment and Infrastructure

1) BDCCL will provide necessary data center space including passive infrastructure facilities, such as advanced fire-fighting system, secured rack space, guaranteed power supply (with backup), cooling infrastructure (HVAC), access control and physical security with tier IV certification.
2) The Investor Firm will bear all costs for the active infrastructure and initial operation via an up-front payment. This will cover cloud stack establishment (hardware, software, licenses), logistics and installation, initial manpower, and specific operating utility costs (electricity and transmission/Internet connectivity for new cloud infrastructure).
3) BDCCL will endeavor to provide reasonable office facilities to the Investor on the site for managing operations.

b. Cost Management and Revenue Allocation

1) Operational Expenses will be distributed as per capacity utilization or power consumption or any other basis as may be deemed appropriate among BDCCLs' Existing cloud(s) and New Cloud (JV).
2) Operational Expenses (OPEX) will include but not limited to operational, general maintenance, salary of maintenance related personnel (directly engaged in the work of mechanical, electrical, cooling, plumbing, firefighting and connectivity), environmental maintenance of the site.
3) Charges should start from the date of commercial operation.
4) Revenue will be shared after deducting/adjusting OPEX portion of new cloud/JV.
5) However, till the new cloud/JV commences generating adequate revenue for fully bearing portion said in previous ser. 1) and 2) clauses, the investor firm shall be responsible to pay the same to BDCCL which is not adjusted with the common/JV revenue at any later point in time.

c. Revenue Sharing Model

The remaining fund after all operational costs and facility charges (b) will be paid constitute the net revenue. The net revenue sharing will be applicable from the date of commencement/go live of the cloud. This Net Revenue will be shared according to the following distribution ratio:

Particulars of Investment by JV	JV Step Portion %	Investor Total %	BDCCL Total %
1st up to Tk. **20 crores** investment	To be proposed	At most 75%	At least 25%
Next up to Tk. **20 crores** investment	To be proposed		
Next up to Tk. **40 crores** or above	To be proposed		

Note: The investor firm's revenue share is compensation for the capital expenditure (CAPEX), technology, and ongoing operations.

Bangladesh Data Center Company Limited BDCCL ICT Division

d. Terms and Renewal of JV Agreement

1) The minimum tenure of the Agreement shall be Seven (07) years from the date of commencement.
2) Upon completion of the initial term, the Agreement may be renewed for successive periods of three (03) years each, based on the mutual consent of both parties.
3) In the event of non-renewal or disagreement, the investor firm shall handover the cloud infrastructure (source code and active cloud stack) to BDCCL, along with all necessary training, documentation, and administrative user manuals.
4) No Termination charge will be applicable in case of Investment/JV termination after 07 (seven) years.
5) In case of termination before 07 (seven) years, a mutual settlement will be applicable.
6) In any cases, the investor firm is fully responsible to handover customers cloud resources along with data to BDCCL without any damage as defined in the agreement.

e. Investment Responsibilities

1) In case of agreement termination, migration/cloud handover with existing customer is the responsibility of the investor firm.
2) A 06 (six) month period or actual time is applicable for the migration/cloud handover process as mutually agreed.
3) BDCCL will provide a migration/cloud handover completed certification to the investor firm in this regard.
4) However, in cases of any service-related complexity after migration/cloud handover, the investor firm is responsible to co-operate the BDCCL.

f. Intellectual Property Rights

1) **Intellectual Property Ownership:** All Intellectual Property rights that subsist in the Cloud shall be owned and possessed by BDCCL. It is understood and acknowledged by both the Parties that the investor firm shall be the developer of the cloud, and BDCCL shall be the sole and exclusive owner of the Cloud.
2) **Investor's Participation and Limitations:** For the avoidance of doubt, it is hereby clarified that the investments made by the investor firm are solely for the purpose of forming the Joint Venture and generating revenue in accordance with the terms of the Joint Venture Agreement. However, the investor firm shall not, at any time during or after the term of the Agreement, acquire any ownership rights or interests in the cloud except the items invested by the investor.
3) **Administration and Technical Control:** The Admin ID and Password of the Cloud shall remain in the custody of a designated member nominated by BDCCL. Furthermore, BDCCL shall have control over the Access Key and technical aspects of the overall service providing process from the cloud to the service recipients.

Section 5 – Data, Facilities, and Local Services to be Provided by BDCCL, and Institutional Arrangements

This section outlines the essential data, physical facilities, and local support services that BDCCL will provide to ensure smooth implementation and operation of the proposed cloud solution. It also defines the institutional arrangements, roles, and responsibilities necessary for coordination between BDCCL and the Investor Firm throughout the contract lifecycle.

Category	Requirement	Specification
Rack Size	Standardized dimensions	H 2000 × W 600 × D 1200 (mm)
Device Compatibility	Rack compliance	All equipment must fit within standardized racks
Rack Power Capacity	Maximum supported load	10kW (3-phase) or 4kW (single-phase) per rack
Power Redundancy	Dual power feeds	Independent A & B power supplies per rack
Power Redundancy	Device-level redundancy	All devices must have 2N power input system (two independent power supplies)
Power Redundancy	Backup systems	Supported by UPS and generator backup
Cooling	Thermal management	Precision cooling with hot/cold aisle containment
Cabling	Structured cabling	Fiber & copper cabling with proper tray management
Security	Access control	Biometric authentication, CCTV surveillance, 24/7 monitoring
Fire Protection	Detection & suppression	VESDA detection with FM200 / Novec 1230/NAFS 125 suppression systems
Environmental Control	Monitoring	Continuous temperature & humidity monitoring at rack and room level
Compliance	Standards	Meets Tier IV (Uptime Institute), ISO 27001, PCI DSS

Section 6 – Qualification of Firms

The investor firm must demonstrate proven capability, experience, and resources to provide cloud solutions for enterprise-level data center infrastructure. The qualifications shall include, but are not limited to, the following:

a. **Legal Status and Registration**

1) The investor firm must be a legally registered and licensed national or international entity. International firms, if not incorporated in Bangladesh, must demonstrate the authority to operate and provide services in Bangladesh through a duly authorized local partner/representative. A valid copy of the certificate of incorporation or business registration must be provided.
2) The investor firm, including its directors, owners, or key personnel, must not have any pending criminal charges, or involvement in fraudulent activities. An affidavit or declaration to this effect, duly notarized or legally certified in the country of origin, must be submitted with the proposal.
3) The investor firm must not be under any form of insolvency, liquidation, or bankruptcy proceedings. A self-declaration to this effect, duly sworn and signed by an authorized representative, must be submitted.
4) The investor firm shall submit Audit Reports for the last two (02) financial years, along with a valid Trade License, VAT Registration Certificate, TIN Registration Certificate, and an updated Income Tax Clearance Certificate.

b. **Experience and Track Record**

1) The Investor firm shall have a minimum of three (03) years of relevant experience in providing cloud infrastructure solutions for large-scale enterprises or government institutions, in cases where the Investor firm is operating independently.
2) **Tier III Data Center experience:** Completed at least one Tier III (Uptime Institute–certified) data center build as prime/lead contractor for a reputed international Customer.
3) **Tier III Data Center Operations & Maintenance (O&M):** Minimum three (3) years' operations and maintenance experience for a Tier III facility
4) If the Investor firm is participating as part of a joint venture (JV) or consortium, the following conditions shall apply:
    a) If all entities are local, the Lead Investor firm shall possess a minimum of three (03) years of experience, while the Technical Partner shall possess a minimum of five (05) years of experience in providing cloud /Data Centre/ Cyber Security/ Infrastructure solutions for large-scale enterprises, Telcos or government institutions.
    b) If the joint venture includes an international partner, the Lead Investor firm shall possess a minimum of three (03) years of experience, while the Technical Partner shall possess a minimum of five (07) years of experience in providing cloud /Data Centre/ Cyber Security/ Infrastructure solutions for large-scale enterprises, Telcos or government institutions.
5) In all cases, both the Lead Investor firm and the Technical Partner must have their primary line of business directly related to providing cloud/Data Centre/Cyber Security/ infrastructure development for Large Scale Enterprises/telcos/Government institutes.

Sajjadeesh Data Center Company Limited
BSCCL
ICT Division

6) The Investor firm (or consortium partners, as applicable) must demonstrate proven expertise in hybrid, private, and public cloud environments.

c. **Local Presence**

The Investor Firm must demonstrate strong operational presence in Bangladesh, either through a local office or a joint venture with a local partner, to ensure timely support and service delivery. The firm shall have at least one (01) functional local registered office in Dhaka and must possess adequate logistical capacity to support its operations and commitments under this project.

Section 7 – Qualification of Expertise & Key Expert

The Investor Firm shall provide qualified and experienced professionals to work in close collaboration with BDCCL's existing operations team to ensure knowledge transfer, smooth implementation, and sustainable operations of the cloud.

It is expected that, the following minimum key roles must be made available by the Investor Firm, with evidence of professional certifications, relevant experience in data centers, and large-scale cloud deployments:

Ser.	Category	Requirements	No of Pers.
1)	Chief Information Security Officer (CISO)	Advisory role for cloud security governance, risk management, and compliance with GOB cybersecurity policies	01
2)	Chief Technology Officer (CTO)	Oversight of cloud architecture and alignment with long-term technology strategy	01
3)	Chief Marketing Officer (CMO)	Support for stakeholder communication, outreach, and service positioning	01
4)	Cloud Solution Architect	Design and validation of cloud infrastructure in coordination with BDCCL engineers	02
5)	Cloud Stack Developers	Development and customization of service layers to meet Client requirements	04
6)	DevOps Engineers	Automation, CI/CD, and operational optimization	04
7)	Database Administrators (DBA)	Management and optimization of database platforms	02
8)	Cloud Engineer (Level 2)	Aid in automation, CI/CD, and operational optimization	06
9)	Cyber Security Engineer	Security hardening, monitoring, and incident response support	02
10)	Threat Analyst	Specialized in threat intelligence and vulnerability analysis	02
11)	SoC Team Member	Assist security in monitoring, detection, and response	04
12)	NOC Team Member	Support in ensuring uptime, network performance, and resilience	08
13)	Network Engineer	Assist in network & transmission	03
	Minimum Total no of Persons		**40**

The Investor Firm must demonstrate that these experts hold internationally recognized certifications and possess documented experience in knowledge transfer and joint operations with data center teams.

Section 8 – Transfer of Knowledge (Training)

The **Transfer of Knowledge (ToK)** component of this project is designed to ensure that BDCCL staff acquire the necessary technical skills, operational expertise, and managerial capacity to independently operate, manage, and enhance the cloud service platform once the Investor Firm's (Developer/Partner/Vendor company) engagement is completed. This is critical for ensuring sustainability, reducing dependency on external Investor Firms, and enabling BDCCL to provide reliable, secure, and scalable cloud services to its clients.

a. Training Approach

The Investor Firm shall design and deliver structured training programs that cover both theoretical and practical aspects of cloud service operations. Training will include but not be limited to the following areas:

1) **Cloud Infrastructure Management** – provisioning, scaling, monitoring, and resource optimization.
2) **Security and Compliance** – IAM, data security, encryption, regulatory compliance, and incident response.
3) **Operations and Maintenance** – day-to-day monitoring, troubleshooting, and performance tuning.
4) **Disaster Recovery and Business Continuity** – backup strategies, failover systems, and recovery testing.
5) **Application and Service Deployment** – migration of workloads, automation, integration, and DevOps practices.
6) **Governance and Cost Optimization** – usage policies, billing, cost tracking, and reporting.

The Investor Firm will adopt a **phased approach** to knowledge transfer, consisting of:

1) **Needs Assessment** - identifying the knowledge gaps of BDCCL's technical teams.
2) **Training Delivery** - classroom sessions, workshops, hands-on labs, and on-the-job shadowing.
3) **Documentation** - preparation of training manuals, user guides, and SOPs for reference.
4) **Validation** - post-training assessments, practical exercises, and evaluation of participants' competencies.

b. Roles and Responsibilities

1) **Investor Firm**:
   a) Develop training materials and curriculum tailored to BDCCL's as well as client's cloud service objectives.
   b) Deliver technical and operational training sessions.
   c) Provide documentation, manuals, and best practice guidelines.
   d) Supervise live shadowing exercises during real operations.
2) **BDCCL**:
   a) Nominate appropriate staff to participate in the training.
   b) Ensure staff availability and allocate time for training sessions.
   c) Provide facilities, systems access, and test environments for hands-on practice.