ডাটা সেন্টারের সেবা গ্রহণ সংক্রান্ত সাধারণ নির্দেশনাবলী:

(১) ভিপিএস / ক্লাউড / ইমেইল (অ্যাডমিন প্যানেল) সেবার সাথে অবশ্যই SSL ভিপিএন সংযোগ নিতে হবে (একাধিক ভিপিএন সংযোগ নেওয়া যাবে, নমুনা পত্রটি সংযুক্ত)।

(২) CA Certificate-এর মাধ্যমে SSL ভিপিএন সংযোগ সক্রিয় করতে হবে (CA Certificate ক্রয়ের জন্য প্রয়োজনীয় লিংক সরবরাহ করা হবে)।

(৩) CA Certificate অবশ্যই ব্যক্তি নামে হবে এই জন্য NID নম্বর দরকার (কোন প্রতিষ্ঠানের নামে হবে না)।

(৪) সেবা গ্রহণ সংক্রান্ত প্রতিটি ফর্মে সরকারি ডোমেনের ই-মেইল এর নাম উল্লেখ করতে হবে (G-Mail, Yahoo গ্রহণযোগ্য নয়)।

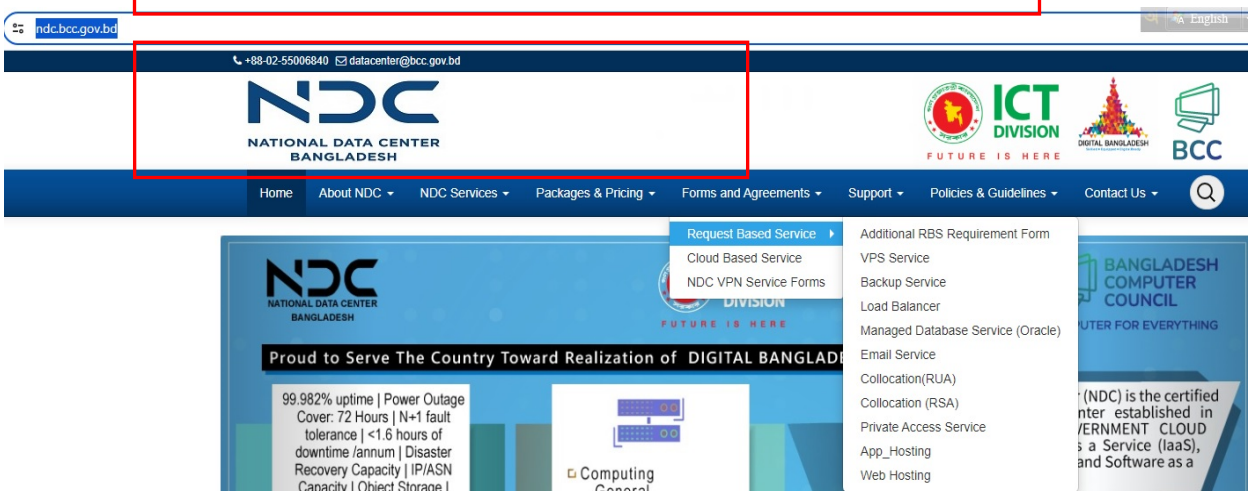
(৫) বর্তমানে বিসিসি সরকারী পর্যায়ে ডাটা সেন্টারের সেবা সরবরাহ করে তাই গ্রহণকৃত সেবাটি যদি Vendor Company কর্তৃক পরিচালনা করা হয় সেক্ষেত্রে সেবা গ্রহণকারী অফিসের প্যাডে বিসিসি বরাবর Authorization Letter দিতে হবে (অফিসের নাম, কর্মকর্তার নাম পদবী, মোবাইল নং, ই-মেইল ও NID নম্বর সহ) (নমুনা পত্রটি সংযুক্ত)।

(৬) ০১ বছর মেয়াদী প্রতিটি CA Certificate এর মূল্য ৫৭৫/- টাকা সরকারি অফিসের জন্য এবং ৩৪৫০/- টাকা সার্পোট সার্ভিস প্রতিষ্ঠানের জন্য (ভ্যাট ও ট্যাক্স সহ)। মেয়াদান্তে পুনরায় CA Certificate এর জন্য আবেদন করতে হবে।

(৭) ডি-নথির মাধ্যমে বিসিসি'র নির্বাহী পরিচালক বরাবর আবেদন গ্রহণযোগ্য।

(৮) সেবা গ্রহণের জন্য নিমোক্ত সকল ডকুমেন্টগুলোর প্রতিটি পৃষ্ঠা স্বাক্ষর করে (অফিসিয়াল সিল সহ) বিসিসি'র নির্বাহী পরিচালক বরাবর দাখিল করতে হবে ।

(৯) ডাটা সেন্টারের সেবা গ্রহণ সংক্রান্ত প্রয়োজনীয় ডকুমেন্টের জন্য এই লিংক এ প্রবেশ করুন https://ndc.bcc.gov.bd



Sample Forwarding Letter (সেবা গ্রহণকারী অফিসের প্যাডে আবেদন করতে হবে)

স্মারক নং---------- তারিখ----------

নির্বাহী পরিচালক
বাংলাদেশ কম্পিউটার কাউন্সিল
ই-১৪/এক্স,আইসিটি টাওয়ার
আগারগাঁও, শেরেবাংলা নগর, ঢাকা-১২০৭

বিষয়: বিসিসির ডাটা সেন্টার হতে ক্লাউড/ হোস্টিং/ ইমেইল/ ভিপিএস /ডাটাবেজ/ কো-লোকেশন সেবা গ্রহণ প্রসঙ্গে।
(বিষয়ের অংশে ডাটা সেন্টার হতে যে সেবাটি নিতে আগ্রহী সেই সেবাটির নাম উল্লেখ করুন)

দৃষ্টি আকর্ষণ: পরিচালক জাতীয় ডাটা সেন্টার, বিসিসি।

অনুলিপি: মেইনটেন্যান্স ইঞ্জিনিয়ার, ডাটা সেন্টার, বিসিসি।

মহোদয়,
উপর্যুক্ত বিষয়ের প্রতি দৃষ্টি আকর্ষণ পূর্বক জানানো যাচ্ছে যে, ----------
---

বাংলাদেশ কম্পিউটার কাউন্সিলের ডাটা সেন্টার হতে ক্লাউড/ হোস্টিং/ ইমেইল/ ভিপিএস সেবা গ্রহণ সংক্রান্ত প্রয়োজনীয় ফরমসমূহ পূরণ এবং প্রতি পৃষ্ঠা সিলমোহর সহ স্বাক্ষর করা হয়েছে (সংযুক্ত) এই বিষয়ে প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য অনুরোধ করা হলো। যোগাযোগের সুবিধার্থে পত্রে আমাদের টেকনিক্যাল অফিসারের নাম, পদবী ও মোবাইল নম্বর উল্লেখ করা হলো প্রয়োজনে তার সাথে যোগাযোগের অনুরোধ করা হল (নাম---------- পদবী---------- ই-মেইল---------- মোবাইল নাম্বার----------)।

সংযুক্তি:
১). Service-Kyc-form
২). Service-Frame-agreement
৩). Resource-Requirement-form
৪). Service Related Appendix

নাম:----------
পদবী:----------
ফোন:
ইমেইল:

(***) ডি-নথির মাধ্যমে নির্বাহী পরিচালক বরাবর আবেদন গ্রহণযোগ্য। সেবা গ্রহণ সংক্রান্ত কাগজপত্রাদির প্রতিটি পৃষ্ঠা স্বাক্ষর করতে হবে অফিসিয়াল সিল সহ।

KYC Form

Appendix – 2

A. Organization Details

Organization Type	:	☐ Revenue or ☐ Project
Project Name (if Required)	:	
Customer Organization Name	:	
Ministry/Division Name	:	
Web URL of Customer Organization	:	

B. Service Owner Details

Service Name	
Service Owner Name	:
Designation	:
NID Number	:
Email	:
Phone (Official)	:
Signature & Seal	:

C. Billing & Administrative Details

Primary Billing Contact Name	:
Designation	:
Email	:
Phone (Official)	:
Mobile Phone	:
Secondary Billing Contact Name	:
Designation	:
Email	:
Phone (Official)	:
Mobile Phone	:

D. Technical Details

Primary Technical Contact Name	:
Designation	:
Email	:
Phone (Official)	:
Mobile Phone	:
Secondary Technical Contact Name	:
Designation	:
Email	:
Phone (Official)	:
Mobile Phone	:

Note: Email Address has to be government email address and shall be under the registered domain of the customer organization.

Bangladesh Computer Council
Data Center Service
Frame Agreement

This document constitutes an agreement (herein after called "Frame Agreement") made on the _____ day of _____, 20 ____ between:

Bangladesh Computer Council ("BCC"), ICT Tower, Agargaon, Sher-e-Bangla Nagar, Dhaka, Bangladesh as the 1st Party (Data Center Service Provider),

and

_____

(Please fill up)

as the 2nd Party (Data Center Service Customer)

Hereinafter, collectively referred to as the "Parties"

The purpose of this Frame Agreement between the Parties is to agree on the general terms and conditions and service level agreement (SLA) set forth for using Data Center Services provided by National Data Center (NDC), BCC. This agreement is applicable for all the services provided by BCC under the Data Center Service Catalog regardless of the specific services chosen by the customer. In consideration of the mutual covenants and agreements contained herein, the Parties hereby agree to follow the general terms and conditions as described in section 1 to 12:

1. Services Information

1.1. The 1st Party shall provide the following Data Center Services as chosen by the 2nd Party from NDC Service Catalog and submitted to 1st Party in Technical Service Information Form,

a) Request based service (VPS, Backup, Load Balancer, E-mail, Co-location, Hosting, Managed Database, etc.)

b) Cloud service;

c) Modified service and resources as requested by the 2nd Party within the scope of the service catalog.

1.2. The 2nd Party acknowledges that it shall be solely responsible for availing the services provided by the 1st Party and shall cooperate with the 1st Party in all matters relating to the services.

2. Commencement and Validity

2.1. This Agreement shall commence on the date of signing by the Parties and shall valid till [*insert date DD-MM-YYYY*];

2.2. Either Party may terminate the agreement before the expiration of the validity period according to Section 6: Termination of the Agreement;

2.3. Upon mutual written agreement of all the Parties, this agreement may be extended for a further period upon such terms and conditions as may be agreed upon in writing by the Parties;

2.4. If none of the Parties provides written notice of termination as specified in this agreement, this agreement shall automatically renew for successive periods of 3 (three) months unless otherwise terminated in accordance with the terms herein.

3. Communication between the Parties

3.1. Communication between the Parties shall take place via contact person as indicated in the Service Level Agreement document or as agreed between the Parties;

3.2. Communication between the Parties shall be done through the communication media which includes: official letter or official e-mail or in any other form reproducible in writing.

4. Relationship between the Parties

4.1. The relations between 1st Party and the 2nd Party shall be governed by the laws and regulations of the People's Republic of Bangladesh, this Agreement, the General Terms and Conditions and the Service Level Agreement (SLA).

5. Modification of the Agreement

5.1. 1st Party has the right to unilaterally change or modify the terms at any time as a result of legislation or practice, a decision of a national authority, technical or substantive developments in a particular area or services, economic needs after providing adequate notice to 2nd Party;

5.2. 1st Party shall notify the 2nd Party at least one (1) month in advance for the amendment of the Terms and Conditions that directly change the terms and conditions of the existing Agreement.

6. Termination of the Agreement and Services

2nd Party reserves the right to terminate or cancel this agreement at any point of time and for any reason by providing an official service termination letter or notice to 1st Party. But such letter or notice must be issued 30 days before the said termination or cancellation date. Acknowledgement of the receipt of such termination letter or notice shall be preserved by the 2nd Party.

On the other hand, 1st Party reserves the right to terminate or cancel the agreement if the 2nd Party fails to comply with the terms and conditions stipulated herein.

Moreover, 1st Party reserves the right to immediate suspension of the whole or part of the services of 2nd Party for temporarily or permanently under the following reasons:

a) If the information system of the 2nd Party generates or disseminates any malware or virus or worm or malicious code;

b) If the information system of the 2nd Party generates inbound or outbound Distributed Denial-of-Service (DDoS) traffic;

c) If the information system of the 2nd Party generates unexpectedly high traffic packet which disrupts overall data center services;

d) If the information system of the 2nd Party interrupts other hosted services in the data center.

e) If 2nd Party does not pay the service fee to the 1st Party for 3 consecutive months;

1st Party shall notify 2nd Party with reasons of such suspension via e-mail before effecting the suspension.

After termination of the agreement, 2nd Party is responsible to retrieve or transfer or migrate their information systems and all relevant data. 1st Party is not liable for preserving the information system resources and data of the 2nd Party after termination of the agreement and related services.

7. Rights and Obligations of the Parties

7.1. Rights of the 1st Party

a) 1st Party reserves the rights to restrict or suspend the provision of the service to the 2nd Party in the event that the 2nd Party breaches the terms of this agreement;

b) 1st Party has the rights to restrict or suspend the services if there are any circumstances which is beyond the control (e.g. attacks on the applications systems of the 2nd Party) of 1st Party or may significantly disrupt the services of other customers of 1st Party, provided that the situation cannot be reasonably eliminated by less burdensome measures on the 2nd Party;

c) 1st Party reserves the right to claim payment from 2nd Party for the services provided under this agreement;

d) 1st Party has the rights to conduct vulnerability test of the application systems of the 2nd Party with the proper concern of 2nd Party if deems required due to any regulatory requirements or to find any root cause of any attack generated from or targeted to the information system of 2nd Party. During the activity, a representative from 2nd Party will be there always to coordinate and support. 1st Party will notify the 2nd Party on such cases and share the reports accordingly;

e) 1st Party reserves the rights to share logs with the law enforcing agencies or regulatory agencies for the purpose of any investigation on the information system of 2nd Party. Both party collaboration is mandatory for this activity. 1st party will provide prior notification (email/phone) to the 2nd party on such cases and share the same logs accordingly;

7.2. Obligations of the 1st Party

a) The 1st Party shall provide the services covered under this agreement according to the Service Level Agreement (SLA) attached as Annexure-1;

b) Necessary services requested by the 2nd Party from the service catalog of NDC, shall be provisioned by the 1st Party and handed over to 2nd Party for deploying the information system in data center;

c) Necessary knowledge transfer session for operating the government cloud console and managing the resources shall be provided by the 1st Party preferably using online platform;

d) During initial on boarding, 1st Party shall provide proactive and prompt support for the accessibility of the request based services and cloud services of NDC, after the services has been provisioned support services shall be provided according to the Service Level Agreement (SLA);

e) The 1st Party is responsible for implementing necessary network perimeter level security measures to protect the cloud services and request based services infrastructure, 1st Party may also implement certain web application level security with its application centric security systems after discussion with 2nd Party;

f) 1st Party may ensure backup of the data for the services provided to 2nd Party after necessary technical discussion on backup policy with 2nd Party;

g) 1st Party may need to perform routine maintenance and software updates on the cloud infrastructure or its other infrastructure. However, 1st Party shall communicate for scheduled maintenance in advance to minimize disruptions to the 2nd Party's operations;

h) If the 1st Party becomes aware of any security breaches or unauthorized access to the 2nd Party's data, 1st Party must promptly inform the 2nd Party and take appropriate remedial actions;

i) If the 2nd Party decides to terminate the agreement by submitting an official letter, the 1st Party should provide necessary possible assistance for the purpose of data migration and retrieval from 1st Party's infrastructure;

j) The 1st Party must provide services in compliance with all applicable laws, regulations, and guideline of the Government of Bangladesh relevant to the data center services and cloud services.

7.3. Rights of 2nd Party

The 2nd Party reserves the right to accept and use all services and related resources as per the terms and conditions of this agreement as well as SLA. 2nd Party also reserves the rights to delegate the access rights of the service resources to the 3rd Party (if needed, on behalf of 2nd Party) for the purpose managing and day to day operation of the service infrastructure. However, relationship between 2nd and 3rd Party shall be governed by an underpinning agreement. The 2nd Party shall inform the 1st Party about such an agreement and seek approval.

7.4. Obligations of the 2nd Party

a) 2nd Party must adhere to all the terms and conditions outlined in the agreement or terms of service provided by the 1st Party. This includes usage policies, restrictions, and guidelines for using the data center services;

b) 2nd Party must comply with other relevant law or policies as and when published by the Government of Bangladesh;

c) 2nd Party shall ensure that all underlying software system and stack for their application systems are properly licensed or free to use (proprietary/open source);

d) 2nd Party shall ensure that their appointed service provider (if any) i.e. 3rd Party is taking reasonable security measures to secure their virtual/cloud servers, application system and relevant infrastructure from any type of internet threats;

e) 2nd Party is obligated to use the data center services for lawful purposes only. They must ensure that they are not doing in any illegal, unethical, or harmful activities using the services;

f) 2nd Party shall ensure that no illegal applications are installed and no illegal content is hosted on their servers and related infrastructure;

g) 2nd Party shall ensure that no TCP/UDP ports are opened for their internal systems and services that could negatively affect the stability of the system;

h) If the 2nd Party is storing or processing any personal or sensitive data using the infrastructure of the 1st Party, 2nd Party must ensure reasonable protection is in place for the protection of those personal data;

i) 2nd Party shall ensure vulnerability and penetration test for the application system before deploying the system in production environment provided by 1st Party under this agreement;

j) 2nd Party shall maintain regular information security test including vulnerability test of their application system for stability of the application;

k) 2nd Party is responsible to monitor the backups of their data; related restoration of backups shall also be monitored periodically by the 2nd Party;

l) 2nd Party must ensure that they are not taking any action that may results in any disruption or alteration of the functionality of the service without their consent;

m) 2nd Party is responsible for maintaining the security and confidentiality of their user accounts and access credentials provided by 1st Party. They must not share their login information with unauthorized individuals and promptly inform the 1st Party in case of any security breaches or suspected unauthorized access;

n) 2nd Party shall ensure strong password and authentication policies for their systems;

o) If there is issues or problems with the data center services, 2nd Party shall promptly report to the 1st Party's support team or designated contact according to the SLA;

p) The 2nd Party shall take the liability for the damages caused to 1st Party by violation of the obligations arising from this agreements, including the damage caused by the application user and any third Party;

q) Unless otherwise agreed in writing between the Parties, the 2nd Party undertakes not to resell or transfer in any means or to use (including in part) the service for purposes other than intended government applications or transfer any user rights (including licenses) offered under it;

r) When using the Services, 2nd Party shall be solely responsible for the information generated from their application system and transmitted through communications networks;

s) If 2nd Party wants to avail more NDC services in future regardless of the Cloud based service or request based service then the customer can get the services within the scope of the existing Frame Agreement. All necessary service specific forms shall be duly filled by the customer and forward to NDC with official Letter.

t) 2nd Party shall not make 1st Party liable for any damages, if it is caused by:

   i. A power failure not dependent on the infrastructure of 1st Party;

   ii. Any unpredictable or abnormal risk situation which is not familiar to 1st Party or 2nd Party, however, in such cases combined decision of the Parties will be treated as final decision to reduce the risk and to normalize the situation;

   iii. Failure of communication lines not within the jurisdiction of 1st Party (including data communications provider);

   iv. Incorrect or unlawful information provided by 2nd Party or their stakeholders;

   v. Wrong selection of service or inadequate use of service resources of NDC by the 2nd Party;

   vi. Failure of the 2nd Party to implement organizational, physical and IT security measures;

   vii. Failure of the 3rd Party to implement necessary organizational, physical and IT security measures for protecting the application system of the 2nd Party;

   viii. Any other scenario that 1st Party states as beyond their control.

u) 2nd Party must ensure timely settling of the payment of the 1st Party based on the fees of the data center services.

7.5. Obligations of the 3rd Party

a) The 3rd Party must comply with all terms and conditions or terms of service provided by the 1st Party as set forth in this agreement. This includes usage policies, restrictions, and guidelines for using the data center services;

b) 3rd Party must comply with other relevant law or policies as and when published by the Government of Bangladesh;

c) 3rd Party shall follow or shall assist to follow all the obligations outlined for 2nd Party.

d) In general scenario, 3rd Party shall communicate with the 1st Party via 2nd Party for the service request or for reporting any issues or problem. However, for emergency issues 3rd Party can directly communicate with 1st Party keeping 2nd Party in the communication process.

8. Billing & Metering

According to the service fee schedule approved by the competent authority, the billing for the services will be calculated in monthly basis. There is no hourly metering system for the provided services. Moreover, for request based services, the metering is according the service plan chosen by the 1st Party from day 1 and for cloud based service the metering shall be based on both allocations based and pay as usage based depending on the type of cloud services.

Any outstanding fees may be resolved under this agreement and mutual negotiation between both parties.

9. Confidentiality and Data Protection

9.1. The Parties undertake to preserve the confidentiality of any information, including trade secrets, which has become known to them in connection with the conclusion and performance of the Frame Agreements, the disclosure of which to the public or to third Parties may in any way harm the other Party. The obligation of confidentiality does not extend to information that is designated to the public, is generally known, or otherwise cannot be confidential in nature or is to be transmitted in accordance with law;

9.2. All Parties agree to keep any confidential information received from each other in the course of this Agreement confidential and shall not disclose such information to any third Party without prior written consent, except as required by law.

9.3. The data or content in the information system of the 2nd Party is the data of the corresponding 2nd Party; 1st Party does not have any ownership and liability for the service, data or content managed by the 2nd Party.

10. Circumstances of Force Majeure

Failure or delay in performance of a Party's obligations shall not be considered a breach of the Frame Agreement if it was caused by circumstances of force majeure. Given the specific nature of service, technological disaster nationwide or global, natural disasters, acts of war, terrorism, etc., which render the Frame Agreement physically impossible, shall be considered as force majeure, but if they occur, the Parties shall make every effort to comply with their contractual obligations.

11. Disclaimer

1st Party cannot be held liable for damages under any circumstances not specifically identified in this Frame Agreement. 1st Party cannot be held liable for the data or file that is stored or processed in the cloud or request based service resources provided by NDC.

12. Dispute Resolution Process:

12.1. Both Parties shall take steps to settle the dispute through negotiation if any dispute arises while the contract is in existence.

12.2. If the dispute is not resolved under Section 12.1, dispute resolution may be initiated through the Ministry/Division of either Party, as agreed by 1st Party and 2nd Party.

By entering into the Frame Agreement, the Parties confirms that they have read, understood, accepted and agrees with the terms and conditions and undertakes to fulfill the obligations set out in the frame agreement.

1st Party (BCC as Government NDC Service Provider):

Name:

Designation:

Signature with Seal:

2nd Party (Representative of Government Organization as Customer):

Name:

Designation:

Signature with Seal:

Appendix-1

National Data Center Service

Service Level Agreement

1. Description of this Service Level Agreement

This Service Level Agreement (SLA) sets forth the commitments provided by the National Data Center of Bangladesh Computer Council (BCC) to the customer. By signing this SLA, the Customer acknowledges that (s)he has read, understood, and agreed with all information mentioned in this SLA.

2. Data Center Service Descriptions

This Service Level Agreement is applicable for all the services provided by BCC under the Data Center Service Catalog regardless of any specific services chosen by the customer.

3. Service Provider Agreement

3.1 Service Availability

Since the data center is a tier-III standard data center, BCC ensures 99.982% uptime which is about 1 Hour and 35 minutes' downtime in a year. However, this uptime is applicable for power and HVAC system only.

The network availability is ensured through redundant network and internet backbone from three different IIG operators of Bangladesh. Apart from network, power and infrastructure availability is also ensured by BCC. The service availability mostly depends on the applications and on the underlying computing, network and storage infrastructure which is not part of the responsibility of BCC in this particular SLA.

3.2 Schedule Maintenance

BCC conducts schedule maintenance of its infrastructure during when the service may not be available or the server response time may get slower. BCC will make every effort to limit the interruption of the service due to such maintenance. The maintenance period is always in the weekend and after the typical office hours. The Customer will be notified by email beforehand in such cases.

3.3 Emergency Maintenance

In case of any emergency maintenance required by BCC for NDC which may impact the service of the customer will be notified through email and mobile to the technical contacts provided.

3.4 Non-emergency Enhancements

Enhancements and changes that do not require a service outage and that do not affect user workflow are implemented upon completion. Enhancements and changes that require a service outage are scheduled outside business hours. Users are notified at

least two working days in advance when a non-emergency service outage is required to implement an enhancement or change.

4. Incident/Service Request Management & Response Time

BCC (1st Party) is committed to provide a satisfactory level of support for the whole life cycle of Customer services. BCC's 24/7/365 Critical Issues Support Line will be always ready to respond critical and non-critical issues that the Customer might be experiencing with the service. Considering the severity and time of reporting the Service request (SR), the Mean Time to Attend (MTTA) and Mean Time to Resolve (MTTR) targets for the service is given below:

Priority Code	Definition	MTTA (Mins)	MTTR (Hrs)
P1	Critical / Major	15	6
P2	High	30	10
P3	Medium	60	24
P4	Low	120	48

Service Request (SR) can be raised by the Customer in any of the following form:

Email Assistance : datacenter@bcc.gov.bd; support@bcc.gov.bd
Online Support : support.bcc.gov.bd, servicedesk.bcc.gov.bd
Phone Number : 02-55006840

Notes on Priority Definitions:

Priority	Description
Critical / Major	The Incident has caused a stoppage or has the potential to cause a stoppage on all or majority of the services being provided by the National Data Center.
High	The Incident has resulted in a work stoppage and has significantly impaired the user's ability to perform their normal business operation. A workaround is not available.
Medium	The Incident has not resulted in a work stoppage but has impaired the user's ability to perform their normal business operation. A workaround is available.
Low	The Incident has not impeded or disrupted the service and is more of an inconvenience, or all incidents that don't fit the Medium, High, or Critical definition.

5. Service Continuity

This section defines how BCC ensures service continuity in case of failure of any of its DC infrastructure or its entire DC infrastructure. Infrastructure and Managed Database Infrastructure within DC is built on using redundant component at each level to ensure highest availability. However, if there's any unforeseen failure at component level which interrupts the service availability, BCC is committed to make the services online with highest priority (P1). If the failure occurs for the entire infrastructure and database or in the entire data center or may exceed the expected restoration time, services can be switch over to DR center according to the decision made by the customer in discussion with BCC.

To ensure service continuity it is important to have both backup and DR facility for any infrastructure. The government cloud of BCC has disaster recovery service known as Cloud Disaster Recovery Service (CDRS) available from its disaster recovery center located at Jashore. The service is available for the customer to be used in accordance with their application architecture and business requirement. However, in case services are switchover to DR, there might be some performance degradation of service (e.g. bandwidth, volume of resources, etc.) as the DR facility is not entirely equal to DC facility. As recovery point objectives (RPO) and recovery time objectives (RTO) for service continuity depends on the customer application architecture it is suggested for the customer to set their RPO and RTO in cooperation with BCC and validate it through service continuity drill or test.

In case of managed database service, there will be asynchronous replication of database to the disaster recovery site using the native feature of the database system. BCC will closely monitor the replication status between the primary and disaster recovery site to ensure there's no gap between the primary and standby database. BCC will also conduct at least one and not more than two database switchover test (DR drill) in a year. In case of gap observed between sites which is not resolving automatically, BCC will immediately notify the customer and initiate gap resolution process.

Apart from DR service, to ensure backup of cloud data, BCC has backup service available for the customer to be used to take backup cloud server. BCC also provides separate agent based backup service for taking backup of file system data which is available for managed database service. BCC provides assistance to the customer, if customer wants to perform restoration test within the NDC infrastructure which is recommended to perform at least once in a year by the customer. Customers are also recommended to collect offline backup of their important data in a periodic manner over virtual private network or physically.

6. Escalation Matrix

In the event of dissatisfaction with the services rendered, Customer may contact the Business Relationship Manager, National Data Center, BCC. Following is the escalation matrix:

Escalation Level	When to Escalate	Role	Contacts
Level 1	If SLA target is breached	Business Relationship Manager	Name: Engr. Md. Firoz Alom Mobile: +8801716502665 Email: firoz.alom@bcc.gov.bd
Level 2	Level 1 remained unresponsive for 3 days without providing any resolution	Management Representative	Name: Md. Hossain Bin Amin Mobile: +8801712213853 Email: hossain.amin@bcc.gov.bd
Level 3	Level 2 remained unresponsive for 2 days without providing any resolution	Director (National Data Center)	Name: Md. Mahbub Karim Mobile: +8801850444127 Email: mahbub.karim@bcc.gov.bd

In case of any disagreement while defining any service, severity or understanding service scope, authorized technical representatives from both the parties will finalize this issue and if the representatives fail to settle this issue, such cases will be escalated to the Top Management of the Customer and Top Management of NDC.

7. Ownership of Data

The data or content in the information system is the data of the corresponding Customer; BCC does not have any ownership and liability for the service, data or content managed by the Customer.

8. Service(s) Fee

Service Fee for Cloud Services and Request Based Services of the NDC is stipulated in Appendix-3. Negotiations with both parties can lead to adjustments in these fees.

9. Dispute Policy

The Customer agrees to be bound by BCC Dispute Policy ("Dispute Policy"), which is hereby incorporated by reference and made a part of this Agreement. Any disputes regarding service are subject to the Dispute Policy provisions in effect at the time this agreement has signed. The Customer also agrees that, in the event a dispute arises with any third party, Customer will indemnify and hold BCC harmless pursuant to the indemnification provision.

10. Revisions of this SLA

This Service Level Agreement (SLA) will remain in effect indefinitely but may be replaced by a revised SLA, at the discretion of BCC. In such cases, both parties will engage in negotiations to resolve any changes. Additionally, customers are welcome to request adjustments or modifications to the SLA to meet their specific requirements. Any revisions to this SLA will be communicated to the Customer via email and official letter at least one month prior to the implementation of the changes.

11. Disclaimer

BCC cannot be held liable for damages under any circumstances not specifically identified in this agreement. BCC cannot be held liable for the data or files that found on Customers data.

12. Special Notices

Any notices required to be given under this Agreement by BCC will be deemed to have been given if delivered in accordance with the contact information the Customer has provided.

NDC
NATIONAL DATA CENTER
BANGLADESH

BCC

Resource Requirement of Customer in e-Government Cloud

Appendix – 4

Sl.	Project Name[1]	vCPU	Memory	Production Storage (EVS)	Backup Storage (VBS & CSBS)	Object Storage	Cloud Server Disaster Recovery (CSDR) [Yes/No]	Auto Scaling (AS) [Yes/NO]	No. of Elastic Load Balancer (ELB)	No. of EIP[2]	No. of Subnet[3]	VPN account name (If you have any, provided from NDC)
1.												
2.												
3.												
4.												
5.												
6.												

Note:

This is an initial requirement form to get idea about the size of your Virtual Data Center (VDC). You can always increase or decrease resources if you want.

[1] Project in cloud is something you can use to isolate resource allocation and access permission among different group or team. You will have a Virtual Data Center (VDC) in the cloud for your ministry/division and you can have multiple projects for different initiatives directly under your ministry or initiative under department/organizations under the jurisdiction of your ministry/division.

[2] IP required to be accessible from public network, outside of the cloud network i.e. from internet or intranet

[3] Subnets is isolation of network within your project VPC, you can then have virtual firewall between subnets. Usually we suggest to have Web Server, Application Server, Database Server subnets to be different at least.

BCC

NDC
NATIONAL DATA CENTER
BANGLADESH

Customer
SSL VPN Account Request Form

Please fill up the name information by following your NID information

First Name

Last Name

Designation

Email (Email must be under own organization domain)

Customer Organization Type

Ministry/Divisioin

Name of Organization

Name of Ministry/Division

Do you have Class 2 type TLS Client Authentication Certificate (mandatory for SSL VPN)?

Yes
No

If no is selected, please enroll and get TLS client authentication certificate from CA

Account Validity

days (put 0 for unlimited access)

Existing Account ID (if any)

Destination network address with destination port information

(e.g. single host: 10.1.1.1:80,443, 22; subnet: 10.2.2.0/24:80,8080,22 or put 0 for all ports) *Use newline for multiple entry

Signature

Customer letter Head

Memo No.: **Date:** DD-MM-YYYY

To
The Executive Director
Bangladesh Computer Council (BCC)
[**Attention:** Director, National Data Center, Bangladesh Computer Council]

Subject: Authorization letter for (vendor/partner) to access the NDC provided (VPS/Cloud/Email/DB/Hosting) services through VPN connection.

Sir,
According to the letter sent on (DD-MM-YYYY), we've already received the NDC provided (VPS/Cloud/Email/DB/Hosting) Service. To maintain the mentioned (VPS/Cloud/Email/DB/Hosting) service we've already make a contract with (vendor/partner company name). As per contract (vendor/partner company name) will maintain the NDC provided (VPS/Cloud/Email/DB/Hosting) service for us. To maintain the NDC provided (VPS/Cloud/Email/DB/Hosting) service they need to access the NDC network through NDC provided VPN connection. In this state please allow VPN connection for the below mentioned table concern person

Sl.No	Contact Person	Company Name	Contact Person's Designation	Email and Mobile Number	National Identification Number or Passport Number
1.					
2.					

** please input the information of vendor or partner who will work for your project to maintain your services in the above table.

As we've an agreement between (vendor/partner company name) and (Customer Organization Name) to maintain our service, so we are requesting to take necessary action to provide VPN access.
Thank you for your co-operation.

Sincerely Yours

Customer Sign
Customer Name
Customer Designation
Mobile No:
Email(official):

Attachment: **ssl-vpn-customer-form** with vendor information according to above mentioned table information.

**** This authorization can be provided by the Customer Service Owner or Customer Service Technical Owner ****