

Dated

31st August 2026

MASTER AGREEMENT

FOR

Core Business Application Takeover, Transition, Implementation, Enhancement, Database Administration, Managed Services, and IaaS Based Hosting with Software Provisioning for the CDNS CBA on Turnkey Management & Implementation Model at NTC Data Centre

Between

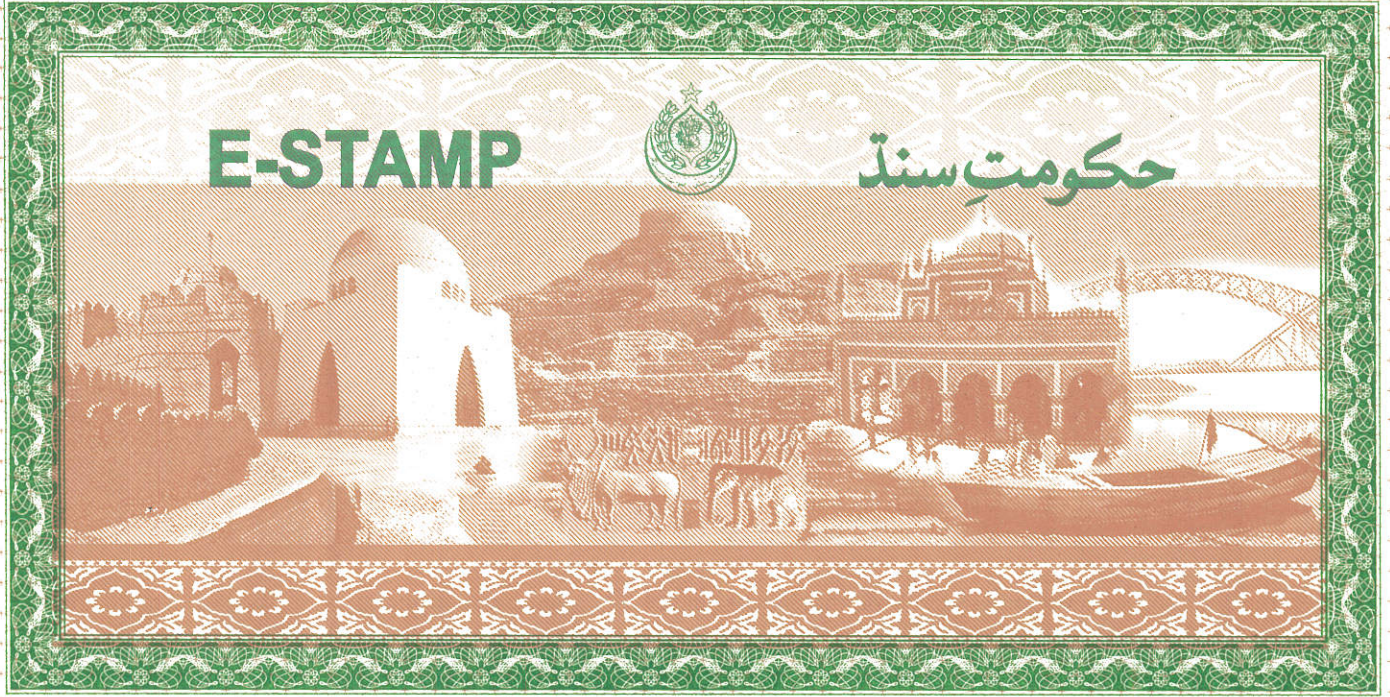
Central Directorate of National Savings
as Customer

And

PAYSYS LABS
as Service Provider



A handwritten signature in blue ink, consisting of a stylized, cursive script.



BOP-0812-978558

GoS-KHI-4D8162296C03107C

Non-Judicial

Rs 5,000/-

Description	: Contract - 15(a)
Principal	: Central Directorate of National Savings [90112067]
Contractor	: Paysys Labs (Pvt) Ltd [72559440]
Applicant	: Mohammad Haris [42301-2668433-9]
Stamp Duty Paid by	: Paysys Labs (Pvt) Ltd [72559440]
Issue Date	: 20-Aug-2026, 11:43:34 AM
Paid Through Challan	: 20263D0F759275D7
Amount in Words	: Five Thousand Rupees Only

Please Write Below This Line

You can verify your e-Stamp paper by scanning the QR code or online at www.estamps.gos.pk using the 'Verification Through Web' option.

MASTER AGREEMENT

FOR

**Core Business Application Takeover, Transition, Implementation,
Enhancement, Database Administration, Managed Services, and IaaS Based
Hosting with Software Provisioning for the CDNS CBA on Turnkey
Management & Implementation Model at NTC Data Centre**

This agreement is entered into at Islamabad, Pakistan on 31st August 2026, and shall be deemed effective from the signing date, herein after defined as **“Effective Date”**.

By and Between

The President of the Islamic Republic of Pakistan represented through the Central Directorate of National Savings, an Attached Department of the Ministry of Finance, Government of Pakistan having its Head Office at 23-N, Savings House, Melody Market, G-6 Markaz Islamabad, Pakistan (hereinafter referred to as "CDNS" or "The Customer", which expression is deemed to include its successors-in interest and assigns)

And

PAYSYS LABS (Pvt.) Ltd, a company incorporated under the laws of Pakistan, with its registered office at 188 1-A Block II, PECHS, Nursery Shahrah-e-Faisal, Karachi, Pakistan. (Hereinafter referred to as **“PAYSYS”** or **“PAYSYS LABS”** or **“SERVICE PROVIDER”**).



("PAYSYS" and "CDNS" may hereinafter collectively be referred to as the "Parties" and singly as a "Party").

WHEREAS

- A. CDNS wishes to engage the SERVICE PROVIDER for the Core Business Application Takeover, Transition, Implementation, Enhancement, Database Administration, Managed Services, and IaaS Based Hosting with Software Provisioning for the CDNS CBA on Turnkey Management and Implementation Model at NTC Data Centre, in line with the published Tender Notice / RFP (Bid No. P11783), the approved bid, and subsequent correspondence with the Service Provider.
- B. CDNS has operated and managed its Core Business Application ("CBA") since December 2020 under agreements with Paysys Labs (Pvt.) Limited. This Agreement supersedes and replaces all prior contractual arrangements related to the CBA, subject to the transition-in provisions herein, and constitutes the entire and comprehensive understanding between the Parties for the scope defined herein.
- C. The Service Provider agreed to provide the CDNS the intended services in return for good and valuable consideration, as set out in this Agreement and its Annexures.
- D. CDNS has accepted the Bid/proposal submitted by the SERVICE PROVIDER, subject to terms and conditions as have been defined in this Agreement, the Tender Documents / RFP, the approved bid, subsequent letters / correspondence, and the terms and conditions thereof. The RFP/ Bidding/ Tender documents, submitted technical and financial bids are integral part of this agreement and anything missed can be referred back to the foundational documents.
- E. The Parties are duly authorized and have the capacity to enter into and perform this Agreement.
- F. NOW, THEREFORE, THIS AGREEMENT WITNESSETH for good and valuable consideration, the adequacy whereof is hereby confirmed and the mutual benefits to be derived therefrom, the representations and warranties, covenants, conditions and promises contained herein, and intending to be legally bound, the Parties hereby agree as follows:



A handwritten signature in blue ink, consisting of a stylized 'P' followed by a series of loops and a final horizontal stroke.

1 DEFINITIONS

- 1.1. **“Agreement”** means this Master Agreement and all provisions contained herein and any Exhibits/Annexures attached thereto signed and effective between the Parties, which shall be treated as an integral document to this Agreement.
- 1.1.1. [Annexure A – Scope of Work](#)
- 1.1.2. [Annexure B – Commercial and Payment Terms](#)
- 1.1.3. [Annexure C – Core Business Application Service Level Agreement \(SLA\)](#)
- 1.1.4. [Annexure D – Change Request Form](#)
- 1.2. **"Applicable Law"** Means the laws and any other instruments having the force of law in the Islamic Republic of Pakistan, as they may be issued and in force from time to time.
- 1.3. **“Business Day”** means a day for which both the Customer and Paysys are open for business in Pakistan:
- 1.4. **“Business Hours”** means 9:00 AM to 6:00 PM of the respective Business Day.
- 1.5. **"CBA" / "Software"** Means the Core Business Application of CDNS (including its backend database, set of instructions, integrations, APIs, functionalities, and the Entire Solution), as developed and managed by the Service Provider and used to operate/function CDNS operations, including all existing modules/enhancements and future enhancements under this Agreement.
- 1.6. **"CBA Takeover"** Means the process of formal handover, verification, and acceptance of the CBA, source code, databases, infrastructure, interfaces, middleware, and all supporting systems and documentation from the outgoing service provider to the incoming Service Provider, as described in [Annexure A-1 CBA Application Takeover and Transition-In](#)
- 1.7. **"Change Request" (CR)** Means any enhancement, modification, or alteration required in the CBA or in the specification on which the CBA is operating, or in the Scope of Work, processed through the Change Management Process defined in [Annexure A-2 – Change Management & CBA Enhancement Policy](#)
- 1.8. **"CDNS"** Means the Central Directorate of National Savings, Ministry of Finance, Islamic Republic of Pakistan.
- 1.9. **“Confidential Information”** means any confidential, trade secret, know-how or other intellectual proprietary information and know-how, disclosed by one Party to the other under this Agreement or which may be obtained directly or indirectly by one Party hereto

from the other Party hereto, whether in writing or in electronic format, or pursuant to discussions held between the Parties, or which is marked confidential or if disclosed orally, expressed to be confidential at the time of disclosure, and subsequently confirmed as confidential in writing to the other Party, or which can be obtained by examination, testing, visual inspection or analyses, including, without limitation terms of this Agreement, Intellectual Property, Know-how and documentation, technical information, software, applications, business information or other materials of a confidential nature except any information that: (i) is public knowledge at the time of disclosure, (ii) was known by the receiving Party before disclosure by the disclosing Party, or becomes public knowledge or otherwise known to the receiving Party after such disclosure, other than by breach of a confidentiality obligation (iii) is independently developed by the receiving Party by persons without access to Confidential Information of the disclosing Party, or (iv) has been or is to be disclosed pursuant to an order or requirement of an administrative agency, other government body, order of a judicial or quasi-judicial body or an obligation imposed by local law, local regulation, in which case the disclosing Party shall notify the other Party of any such disclosure or impending disclosure.

- 1.10. **“Commissioning and Provisioning Date”**: means the date on which the proposed Hardware and Software Infrastructure as a service (as detailed in Annexure A-4) by Paysys Labs is made available for use within NTC Data Centers in Islamabad and Lahore.
- 1.11. **"Data Centre" / "NTC Data Centre"** means the physical facility, together with its associated infrastructure, provided and operated by NTC at its Lahore and Islamabad locations, where the Hardware and Software Infrastructure under this Agreement is hosted, including the primary (PR) and disaster recovery (DR) sites, along with the power, cooling, connectivity, physical security, and environmental controls necessary for the hosting and operation of the CBA and related services.
- 1.12. **“Data Purging”** means the transfer of applicable CDNS Data (including transactional, customer, operational, or any other data) from the production environment to offline or archival storage (such as tape or similar media). Data Purging does not mean deletion of data; the data shall be removed from the production environment only after successful transfer to archival storage, and shall remain available for retrieval or restoration upon request in accordance with the agreed recovery TATs.

- 1.13. **"Defect" / "Defects"** Means service faults, functionality or feature of the Software/ Hardware which is deficient and not as per proper functionality of the CBA and related infrastructure arising from defective design or workmanship or from any act or omission of the Service Provider.
- 1.14. **"Deliverables"** means any item, work or development carried out and delivered pursuant to and as part of this agreement,
- 1.15. **"DR" / "DR Site"** Means Disaster Recovery site located at NTC Lahore Data Centre, serving as the secondary failover environment for the CBA
- 1.16. **"Effective Date"** shall be as per Clause 2 of this agreement.
- 1.17. **"Enhancements"** Means any new modules, features, functionalities, or customizations developed and incorporated into the CBA under this Agreement or through the Change Request process.
- 1.18. **"Fees"** means the fees payable by the Customer to the Service Provider in respect of the Services as detailed in the [ANNEXURE B – COMMERCIALS AND PAYMENT TERMS](#).
- 1.19. **"Force Majeure Event"** Means an event beyond the reasonable control of a Party that makes that Party's performance of its obligations under the Agreement impossible or impractical.
- 1.20. **"Go-Live"** Means the activity performed by the Service Provider to carry the Software/module into the Production Environment.
- 1.21. **"Go-Live Date"** means the date on which any or all use cases are made available in the CDNS CBA's Production environment for live business transactions.
- 1.22. **"Government" / "GoP"** Means the Government of the Islamic Republic of Pakistan.
- 1.23. **"IaaS"** Means Infrastructure as a Service – the provisioning and management of hardware and software infrastructure (servers, storage, networking, security tools, virtualization, and system software) at NTC Data Centers by the Service Provider on a managed basis, as described in [Annexure A-4 IaaS — Proposed Hardware and Software Infrastructure](#) and [Annexure A-5 Infrastructure Managed Services](#)
- 1.24. **"Intellectual Property Right(s)"** means any patent, petty patent, copyright, including but not limited to literary and artistic works computer programs; databases

algorithms, trade mark, trade name, rights in know-how, or any similar right in any part of the world and shall include any applications for the registration of any patents or trade mark or trade name or copyrights or similar rights capable of registration in any part of the world.

- 1.25. **"JIRA"** Means the issue/project tracking tool used for ticket logging, Change Request tracking, and SLA monitoring.
- 1.26. **"Jira Ticket"** refers to support/detail requests submitted by CDNS through the Paysys JIRA system, which is the designated platform for tracking and managing all service requests.
- 1.27. **"Managed Services"** Means the ongoing end-to-end management, monitoring, maintenance, administration, and support services provided by the Service Provider for the CBA, its database, and the infrastructure (both existing CDNS hardware and Provided Infrastructure as IaaS), as described in [Annexures A-3 CBA Annual Maintenance and Support](#) and [A-5 Infrastructure Managed Services](#).
- 1.28. **"Man-Day Rate"** Means the daily cost rate per resource category, inclusive of all applicable taxes, as agreed in [Annexure A-2 \(Change Management and CBA Enhancement Policy\)](#), used for pricing Change Requests and Enhancements.
- 1.29. **"Milestone"** Means a significant event or task set by both Parties under the Project/Work Plan, upon the completion of which associated payments shall be released to the Service Provider.
- 1.30. **"Ministry of Finance"** Means the Ministry of Finance, Revenue and Economic Affairs of the Government of Pakistan.
- 1.31. **"NADRA"** Means the National Database and Registration Authority, an autonomous body under the Interior Ministry of Pakistan.
- 1.32. **"NTC"** Means the National Telecommunication Corporation of Pakistan, operator of the data centers where the CBA shall be hosted under this Agreement.
- 1.33. **"Primary Contact"** means the person described in [Escalation Matrix of Annexure C](#) or his or her successor or supervisor notified in writing to the other Party.
- 1.34. **"PBG" / "Performance Guarantee"** Means the Performance Bank Guarantee, an unconditional and irrevocable guarantee issued by a scheduled bank in Pakistan, to be submitted by the Service Provider as security for performance.

- 1.35. **"PKR"** Abbreviation for Pakistani Rupee.
- 1.36. **"PR" / "PR Site"** Means the Primary Data Centre site located at NTC Islamabad.
- 1.37. **"Project/Work Plan"** Means a document, including the timeframe, responsibilities, dependencies, activities, and tasks of each party, linked with the Scope of Work.
- 1.38. **"SBP"** Means the State Bank of Pakistan.
- 1.39. **"RAAST"** means the instant payment system operated by the State Bank of Pakistan enabling real-time fund transfers.
- 1.40. **"Residual Value"** means estimated worth of the Group II Infrastructure-as-a-Service (IaaS) at the end of its useful service life
- 1.41. **"Secondary Contact"** means the person described in [Escalation Matrix of Annexure C](#) or his or her successor supervisor notified in writing to the other Party.
- 1.42. **"Severity Levels"** Means the classification of reported issues (Level 4 – Emergency being the most severe through Level 1 – Minor) that determines the applicable response and resolution timeframes under Annexure C.
- 1.43. **"Scope of Work"** means the scope of work as agreed to between the Parties pursuant to [Annexure A Scope of Work](#)
- 1.44. **"SIT (System Integration Testing)"** means the testing conducted to verify that different components of the Solution integrate and function together as intended.
- 1.45. **"Service Level Agreement (SLA)"** Means the enforceable service performance standards applicable to all services under this Agreement, as described [in Annexure C Core Business Application Service Level Agreement \(SLA\)](#)
- 1.46. **"Service Provider"** Means M/s Paysys Labs (Pvt.) Limited, the company awarded this Agreement for provision of services.
- 1.47. **"Subcontractor"** Means any entity to which the Service Provider sub-contracts any part of the Services, subject to prior written consent of CDNS.
- 1.48. **"TAT"** Means Turn Around Time
- 1.49. **"Use Case"** means a documented business scenario that describes how a user interacts with the System to perform a specific function or business process, including the expected inputs, processing, outputs, and system responses under this agreement.

- 1.50. **“UAT (User Acceptance Testing)”** means the testing conducted by the CDNS and Paysys to verify that the Solution meets the agreed business and functional requirements before Go-Live.

2 TERM OF AGREEMENT

- 2.1. The Annual Maintenance and Support for the CBA and any CBA enhancements (comprising Group I in Clause 5 - Scope of Work) shall commence on the Date of completion of transition-in phase (the “Effective Date for Group I”) as described in clause 29.8.1 for an initial term of one (1) year. Subject to the satisfactory performance and approval of CDNS, this Agreement is extendable on an annual basis upon the same terms, approved pricing and applicable annual escalation rates, for a total cumulative term up to five (5) years. Upon expiration or termination of the term, a Transition-Out period of up to six (6) months shall apply.
- 2.2. Notwithstanding Clause 2.1, the term applicable to Infrastructure as a Service (“IaaS”), comprising Group II as defined in Clause 5, shall commence on the date of successful provisioning and commissioning (the “Effective Date for Group II”) and shall continue for an initial Service Year of one (1) year. Thereafter, Group II shall continue for successive periods of one (1) year, up to a maximum cumulative period of five (5) years from the Effective Date for Group II, unless the conditions mentioned in termination clause. Continuation into each subsequent Service Year shall be recorded through a written continuation notice, such notice shall not require renegotiation of the Scope of Work, approved pricing or any escalation.
- 2.3. Notwithstanding Clause 2.1 and Clause 2.2, the term applicable to Managed Services for CDNS Hardware, comprising Group III as defined in Clause 5, shall commence on the date of signing of this contract (the “Effective Date for Group III”) and shall continue for an initial Service Year of one (1) year. Thereafter, Group III shall continue for successive periods of one (1) year, up to a maximum cumulative period of five (5) years from the Effective Date for Group III, unless the conditions mentioned in termination clause.
- 2.4. Expiry, termination, suspension or non-renewal of Group I or Group III shall not, by itself, affect the continuation of Group II. Group II shall remain independently operable and shall continue until separately expired or terminated in accordance with this Clause and the termination provisions applicable to Group II.

3 PAYSYS LABS RESPONSIBILITIES

- 3.1. In accordance with the terms of this Agreement, Paysys agrees to and shall manage, execute, and complete the Project and shall allocate sufficient resources to enable it to comply with its obligations under this Agreement, the tender documents, and the proposal submitted by Paysys as defined to the satisfaction of the Customer.
- 3.2. Paysys shall ensure that each member of its Project Team assigned to the Project has the relevant industry standard skills and training to be able to perform the Services in a competent and professional manner to the satisfaction of the Customer.
- 3.3. Paysys shall be available to attend all service calls from the Customer pertaining to the Services during the defined Business Hours and TATs in Annexure C Core Business Application Service Level Agreement (SLA).
- 3.4. The Service Provider shall not make any promises, representations or warranties or give any guarantees in the name of, or on behalf of, the Customer.
- 3.5. Paysys shall ensure, at all times, compliance with all applicable laws, rules, regulations, and directives issued by the Government of Pakistan, the State Bank of Pakistan, Ministry of Finance and any and all other relevant regulatory or statutory authorities in relation to the performance of the Services under this Agreement.

4 CDNS'S RESPONSIBILITIES

- 4.1. In accordance with the terms of this Agreement, CDNS agrees to and shall provide Paysys with timely access to all necessary information, systems, facilities, and personnel reasonably required for the execution of the Project.
- 4.2. CDNS shall ensure that any information that pertains solely to CDNS's own procedures or policies, as required by Paysys Labs for the provision of services under this contract, is provided to Paysys and is accurate, complete, and up to date.
- 4.3. CDNS shall nominate point of contact for coordination relating to the Project so that deliverables are achieved in a timely manner.
- 4.4. CDNS shall ensure, at all times, compliance with all applicable laws, rules, regulations, and directives issued by the Government of Pakistan, the State Bank of Pakistan, and any other relevant regulatory or statutory authorities in relation to its obligations under this Agreement.

5 SCOPE OF WORK

5.1. The full and detailed Scope of Work for this Agreement is set out in Annexure A of this Agreement, which is deemed as an integral part of this Agreement:

Group/Domain	Description
Group I – CBA Application Takeover and Transition-In	Application Takeover, Transition-In, End-to-End Support & Development of New Modules/Capabilities
Group I – CBA Change Management and Enhancements	Enhancements, Customizations, Change Requests & Change Management Process (Man-Day Rates)
Group I – CBA Annual Maintenance and Support	Service Level Agreement – Performance Standards, Measurement & Penalties
Group II – IaaS – Proposed Hardware and Software Infrastructure	Infrastructure as a Service – Hardware & Software Provisioning at NTC Data Centers (PR & DR)
Group III – Infrastructure Managed Services	Managed Services of Existing and Provided Infrastructure as IaaS

5.2. The Service Provider agrees to provide the services for the successful execution of all components of the Scope of Work set out in [Annexure A Scope of Work](#).

6 CHANGE MANAGEMENT

6.1. All changes to the scope of work, system configurations, application modules, infrastructure, or operational processes under this Agreement shall be governed exclusively by the Change Management and CBA Enhancement Policy set out in [Annexure A-2 \(Change Management & CBA Enhancement Policy\)](#) of this Agreement, including the [six-step CR delivery cycle](#), governance procedures, and payment terms defined therein.

6.2. Man-Day rates applicable to all Change Requests shall be as quoted in [Annexure B - Commercials and Payment Terms](#) of this Agreement.

- 6.3. No change shall be binding on either Party unless formally approved in writing through the Change Request process defined in Annexure [A-2 Change Management & CBA Enhancement Policy](#).

7 CHARGES AND PAYMENT

- 7.1. CDNS shall pay the Fees within 45 Days upon receipt of each undisputed invoice properly issued and submitted by Service Provider in accordance with the Payment Schedule.
- 7.2. CDNS shall notify Paysys within Ten (10) Business Days of receiving the invoice of any discrepancy/objection to an invoice, which shall be rectified by Paysys within Ten (10) Business Days whereupon a corrected/amended invoice shall be issued/submitted by Paysys.
- 7.3. All fees, charges, and expenses specified under this Agreement are inclusive of the prevailing Islamabad Capital Territory Sales Tax on Services (at the applicable rate of 5%), levied pursuant to the Islamabad Capital Territory Sales Tax on Services Ordinance, 2001.
- 7.4. Whereas, pursuant to clause E 1 (Change in Applicable Law) of the General Conditions of Contract of the tender documents, any changes in the applicable taxes or duties, or the applicability or interpretation of them thereof, then the fee payable to Paysys Labs under this Contract shall be increased or decreased accordingly by agreement between the Parties.
- 7.5. All invoices shall be raised in PKR.
- 7.6. All invoices shall be submitted by the Service Provider through the approved channels (email/ courier/self-delivery) accompanied by the relevant milestone completion evidence. CDNS shall notify Paysys within Ten (10) Business Days of receiving the invoice of any discrepancy/objection to an invoice, which shall be rectified by Paysys within Ten (10) Business Days whereupon a corrected/amended invoice shall be issued/submitted by Paysys and payment shall be made by CDNS within Forty-Five (45) days of invoice approval.

7.7. Liquidated Damages

7.7.1. Payments of Liquidated Damages

- 7.7.1.1. Paysys shall pay liquidated damages to CDNS at the rates per day stated in the SCC for each day that the Completion Date is later than the Intended Completion Date. The total amount of liquidated damages shall not exceed the

amount defined in the SCC of the tender documents. CDNS may deduct liquidated damages from payments due to the Service Provider. Payment of liquidated damages shall not affect the Service Provider's liabilities.

7.7.2. Correction for Over-payment

7.7.2.1. If the Intended Completion Date is extended after liquidated damages have been paid, CDNS shall correct any overpayment of liquidated damages by the Service Provider by adjusting the next payment certificate. The Service Provider shall be paid interest on the overpayment, calculated from the date of payment to the date of repayment, at the rates specified in SCC.

7.7.3. Lack of performance penalty

7.7.3.1. If the Service Provider has not corrected a Defect within the time specified in CDNS's notice, a penalty for Lack of performance will be paid by the Service Provider. The amount to be paid will be calculated as a percentage of the cost of having the Defect corrected, assessed as specified in the tender documents.

8 INDEMNITY

8.1. Each Party (the "Indemnitor") shall indemnify and hold harmless the other Party (the "Indemnitee") from and against all actual losses, claims, demands, suits, judgments, and related costs and expenses arising in connection with the work under this Agreement or any Addendum, Change Request, or Order, caused by any act, omission, or liability of the Indemnitor or its agents or employees, including any violation of a third party's Intellectual Property Rights (IPRs). This includes any breach by the Indemnitor of its representations, warranties, or obligations under this Agreement, any failure to comply with applicable laws, and any unauthorized disclosure of Confidential Information. Each Party shall give the other prompt notice of any such potential liability. This clause is without prejudice to any other rights available to either Party under this Agreement or applicable law.

9 REPRESENTATIONS AND WARRANTIES

9.1. The Parties hereby represent and warrant to each other that:

9.1.1. Each Party has the full power and authority to enter into and perform its obligations under this Agreement.

9.1.2. Each Party shall comply with all applicable laws, rules, and regulations in connection with the performance of its obligations under this Agreement.

- 9.1.3. Each Party has, and shall maintain, the requisite expertise, resources, and qualifications to fulfil its respective obligations set forth in this Agreement.
- 9.1.4. Each Party shall perform its respective obligations in accordance with best professional practices and the standards agreed herein.
- 9.1.5. Neither Party shall knowingly infringe the intellectual property rights of any third party in the course of performing its obligations under this Agreement.
- 9.1.6. Neither Party shall use, nor authorize its employees or agents to use, any confidential information or material provided by the other Party for any purpose other than for fulfilling its obligations under this Agreement, unless otherwise agreed in writing.

10 CONFIDENTIALITY, CUSTOMER'S PROPERTY AND DATA PROTECTION

- 10.1. The Service Provider, including its employees, affiliates, agents, advisors, and consultants, shall keep strictly confidential all technical, commercial, or business information received from the Customer (“Confidential Information”), including know-how, specifications, processes, inventions, products, services, operations, and trade secrets. Disclosure is allowed only to those who need the information to perform the Services, and they must be bound by confidentiality obligations equivalent to those in this Agreement.
- 10.2. Confidentiality Obligations: The Service Provider must treat any and all customer data as confidential and will not disclose, misuse and store.
- 10.3. Data Classification: The Service Provider must comply with the customer’s data classification policy (e.g., public, internal, confidential, restricted).
- 10.4. Notwithstanding the foregoing, either Party may disclose any such confidential information:
- a) which is in, or comes into, the public domain or becomes public knowledge otherwise than through any disclosure prohibited by this Agreement.
 - b) that a party is required to disclose by law or regulatory requirements (or for the purpose of any judicial proceedings), provided that if such party is required to make any such disclosure, such party shall, wherever practicable, consult with the other party before making such announcement or disclosure.

- c) to its professional advisers, auditors and insurers provided they have a duty to keep such information confidential.
- 10.5. All materials, tools, designs, and intellectual property supplied by the Customer remain the Customer's property. The Service Provider shall safeguard them, maintain them in good condition, and use them only as authorized in writing by the Customer.
- 10.6. The Service Provider shall not use the Customer's Data other than as authorized pursuant to this Agreement or otherwise by the Customer in writing including:
- a) using the Customer's Data other than in connection with the performance of the Services.
 - b) disclosing, selling, assigning, leasing or commercially exploiting the Customer's Data; or
 - c) otherwise providing Customer's Data to third parties.
- 10.7. The Service Provider shall exercise in relation to the Customer's Data, Confidential Information and/or Intellectual Property Rights no lesser security or control measures and degree of care than those which The Service Provider applies to its own data, confidential information and intellectual property rights. For this purpose, The Service Provider hereby undertakes to provide an adequate level of protection against unauthorized access, loss, alteration, transfer, processing, disclosure, reproduction or use of any Customer's Data, Confidential Information and/or Intellectual Property Rights.
- 10.8. The Service Provider shall ensure that promptly, and in any event within twenty-four (24) hours, notify the Customer about any actual or suspected breach of systems operated by The Service Provider, its affiliates, or any actual or suspected unauthorized access to, or disclosure of the Customer's Data and/or Confidential Information ("Security Breach") and shall:
- 10.8.1. provide full details of such Security Breach to the Customer and update the Customer as the investigation into the Security Breach progresses.
 - 10.8.2. not make any public disclosures with respect to the Security Breach without the Customer's prior written consent; and
 - 10.8.3. implement at its own cost and within time frames agreed mutually with the Customer, any measures necessary for restoring the security and mitigating the

consequences of the Security Breach (including but not limited to any steps reasonably requested by the Customer).

11 AUDIT AND SUPERVISION

- 11.1. The Service Provider shall allow Customer, and its regulators, including the Ministry of Finance, and the Government of Pakistan, to conduct inspections and/or audits of the Services, including without limitation the premises, processes, controls, procedures, security arrangements, systems, used to provide the Services, if Customer shall provide no less than Seven (7) working days written notice to the Service Provider of such inspection and/or audit.

12 TERMINATION

- 12.1. Either Party may, by written notice to the other Party, forthwith terminate this Agreement if the other Party commits a material breach of the terms and conditions of this Agreement and which breach (in case of a remedial breach) shall not have been remedied within Ninety (90) days of receipt of written notice from the other Party, specifying the breach and requiring the same to be remedied, unless the Parties mutually agree to extend this further.
- 12.2. At any time during the term of this Agreement, a Party may immediately terminate this Agreement if the other Party:
- 12.2.1. Voluntarily files a petition under bankruptcy or insolvency law,
 - 12.2.2. Has been the subject of an involuntarily filed petition under bankruptcy or insolvency law, unless such petition is dismissed within Thirty (30) days.
 - 12.2.3. Has an order entered against it either appointing a receiver or trustee for or issuing a levy or attachment against a substantial portion of its assets and this order is not vacated, set aside or stayed within Thirty (30) days from date of entry.
- 12.3. Neither Party may terminate Group II for convenience during the Service Period. Group II may be terminated only: (a) by mutual written agreement; (b) for an uncured material breach; (c) for insolvency; (d) for a material security or confidentiality breach; (e) where continued performance becomes unlawful; (f) pursuant to a binding direction of a competent Government, judicial or regulatory authority; or (g) for prolonged force majeure. No termination shall permit interruption, withholding or removal of

infrastructure while CDNS data remains hosted thereon or before an orderly transition has been completed.

12.4. Group II constitutes a separate and independently operable service component. Expiry, termination, suspension, non-renewal or change in Group I or Group III shall not automatically terminate, suspend or otherwise affect Group II. Group II shall continue for its then-current approved Service Period unless separately terminated in accordance with the provisions expressly applicable to Group II.

12.5. Upon termination of this Agreement for any reason whatsoever:

12.5.1. The rights and obligations of the Parties accrued up till the date of such termination shall remain unaffected.

12.5.2. Any and all payments due under this Agreement shall become immediately payable.

13 OWNERSHIP, HANDOVER AND EXIT MANAGEMENT

13.1 Ownership Rights and Handover of Source Code and Related Documentation

- a) CDNS shall be the sole and exclusive owner of the source code, technical and user documentation, databases, configuration files, and all other components, deliverables, and intellectual property developed, customized, configured, or maintained by Paysys under this Agreement (collectively referred to as the "Assignment Materials").
- b) All rights, title, and interest, including intellectual property rights, in and to the Project Materials shall vest exclusively in the CDNS from the date of their creation. Paysys hereby irrevocably assigns, transfers, and conveys to the CDNS all such rights without any further consideration.
- c) Paysys shall ensure that no third-party proprietary material is incorporated into the Project Materials without the prior written consent of the CDNS, and that all open-source or licensed components are clearly identified, with associated licenses duly disclosed and compatible with perpetual ownership and use by the CDNS.
- d) The hardware and transferable infrastructure software provisioned under Group II shall remain owned by Paysys during the Group II term. CDNS shall have the exclusive ownership and control of its data, configurations, encryption keys, access records and backups. Following commissioning and migration of CDNS production data, Paysys shall not remove, relocate, disconnect, encumber, substitute or materially alter the Group II

infrastructure without CDNS's prior written approval, except for emergency maintenance required to preserve security or service continuity and promptly notified to CDNS.

- e) Upon completion of the service period from the Group II Commissioning and Provisioning Date, or upon any earlier lawful expiry or termination of Group II, CDNS shall have the first right to acquire Group II hardware and software infrastructure at its then-applicable Residual Value. CDNS may exercise the option by written notice within sixty days after receiving the Residual Value Statement and supporting documents from Paysys. Until mutually agreed upon residual value and complete transfer, the terms and conditions of the agreement will remain in full force and effect.
 - i. For clarity, the residual value shall be calculated as the total cost of the Group II Infrastructure-as-a-Service (IaaS), as mentioned in table B.1 of Annexure B for the term of agreement, inclusive of the extended period as per clause 2; — less annual straight-line depreciation at the rate of twenty percent (20%) per annum.
- f) For the avoidance of doubt, the already payable IaaS fee accruals and ongoing payment obligations shall immediately be paid upon the notice of termination. Should the transition, data migration, or determination of the Residual Value extend beyond the effective termination date, M/s Paysys shall continue to host and safeguard CDNS data and grant necessary administrative access; however, as the data of CDNS will still be hosted on the IaaS, hence, CDNS will be liable to continue payment incurred during such interim transition period.
- g) Pending final execution of the asset transfer, all operational, confidentiality, security, and data protection terms of this Agreement shall remain in full force and effect.
- h) Upon the termination, expiry, or completion of this Agreement, Paysys shall, at no additional cost to CDNS, deliver the most recent, complete, and operational versions of all Assignment Materials, including but not limited to:
 - i. Full source code and related build scripts;
 - ii. System and technical documentation;
 - iii. Database schemas, configurations, and deployment instructions; and
 - iv. Any other information or material necessary for the continued operation, maintenance, and enhancement of the Core Business Application.

- i) Paysys shall not retain, copy, or use any portion of the Materials/information/data related to this assignment, whether in physical or electronic form, except with the prior written authorization of the CDNS and solely for purposes consistent with this Agreement.
- j) Paysys shall comply with all applicable government information security, confidentiality, and intellectual property regulations in the development, storage, and handling of the Project Materials.

13.2 Transition Phase Assistance upon Completion/Termination of Agreement

- a) Upon the termination, expiry, or completion of this Agreement, Paysys shall provide all reasonable cooperation, support, and technical assistance to the CDNS, or to any successor service provider designated by CDNS, to facilitate a smooth and uninterrupted transition of services and operations ("Transition Period").
- b) Such transition assistance shall include, but not be limited to, knowledge transfer, data migration, system handover, technical guidance, and coordination activities as may be reasonably required by the CDNS to ensure business continuity.
- c) The Transition Period shall not exceed six (6) months from the effective date of termination or expiry of this Agreement, unless otherwise extended by mutual written consent of the Parties.
- d) During the Transition Period, all services and support provided by Paysys shall be rendered at the same rates, terms, and conditions as specified in this Agreement, without any escalation or surcharge.
- e) Paysys shall not obstruct, delay, or withhold access to any system, data, documentation, or technical information required by CDNS or its authorized representatives, or nominated successors for the purpose of ensuring the seamless continuation of the Core Business Application.
- f) Paysys shall continue to observe all confidentiality and data protection obligations during and after the Transition Period.

13.3 Exit Management and Transition-Out Deliverables

During the Transition Period referred to in Clause 13.2, and in accordance with a mutually agreed Exit Management Plan in writing, the cooperation and handover to be provided by Paysys shall include, but not be limited to, the following:

- a) **Source code and repository.** Handover of the complete, most recent, and operational source code of the CBA, together with the full version-control repository (including commit history, branches, and tags), build and deployment scripts, and all related configuration files, transferred to CDNS or their nominated successor.
- b) **Data and database.** Handover of all CDNS data in Paysys's possession, including the complete database schema, stored procedures, views and objects, together with full and incremental backups, in a documented, restorable format, with deployment and restoration instructions.
- c) **Database synchronization and PR–DR cut-over.** Documented handover of all database synchronization, replication, and Primary-to-Disaster-Recovery (PR–DR) cut-over and fallback procedures, including runbooks, scripts, and configuration required to operate and maintain the PR and DR environments and to perform DR drills independently of Paysys.
- d) **System interfaces and integrations.** Handover of interface and integration documentation for all external systems connected to the CBA, including endpoint configurations, message formats, and connectivity requirements sufficient for continued operation.
- e) **Process and knowledge transfer.** Handover of end-to-end process maps for each business transaction and operational process (covering normal, exception, and reversal scenarios), system and technical documentation, reporting formats, and structured knowledge-transfer sessions to enable CDNS or their nominated successor team to operate, maintain, and enhance the CBA.
- f) **Acceptance.** Completion of the Transition-Out shall be subject to CDNS's or their nominated successor team's verification and formal sign-off of the deliverables set out in this Clause 13.3.

14 ASSIGNMENT AND SUB-CONTRACT

- 14.1. The Service Provider shall not assign or sub-contract whole or any part of the Project at any stage of the Agreement without prior written consent of the CDNS.

15 DELIVERY

- 15.1. The work will be completed within the Project/Work Plan submitted by the Service Provider.

16 INTEGRITY PACT

- 16.1. PAYSYS LABS Pvt hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.
- 16.2. Without limiting the generality of the foregoing PAYSYS LABS Pvt represents and warrants that it has fully declared the brokerage, commission, fee etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultations fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.
- 16.3. Paysys Labs certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representative or warranty.
- 16.4. Paysys Labs accepts full responsibility and strict liability for making and false declaration, not making full disclosure, misrepresenting fact or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.
- 16.5. Notwithstanding any rights and remedies exercised by GoP in this regard Paysys Labs agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent

to ten times the sum of any commission, gratification, bribe, finder's fee or kickback given by Paysys Labs as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

17 Performance Guarantee

- 17.1. The Service Provider shall, within fourteen (14) calendar days from the date of issuance of the Letter of Acceptance or prior to the execution of the Contract Agreement, furnish an unconditional, irrevocable and on-demand Performance Bank Guarantee ("PBG"). The PBG shall be submitted on legal stamp paper of appropriate value as per applicable stamp laws, for an amount equivalent to 3% (three percent) of the total annual contract value for each respective Group/Cost Component, as specified in Annexure-B (Commercials and Payment Terms).
- 17.2. The initial PBG shall remain valid and enforceable for a period of twelve (12) months from the date of signing of the Contract Agreement, plus an additional claim period of ninety (90) days beyond the expiration date.
- 17.3. For an extended contract terms, the Service Provider shall submit a fresh PBG of equal value and validity at least thirty (30) days prior to the expiration of the preceding year's PBG.
- 17.4. CDNS shall discharge and release the PBG for any completed operational year only upon the successful, satisfactory completion of the respective contract year, as certified in writing by CDNS; and the timely receipt and verification of the valid PBG for the subsequent contract year.
- 17.5. The PBG must be issued by a Scheduled Bank operating in Pakistan, acceptable to CDNS. In the event of any pending deliverables, unfulfilled warranty/SLA obligations, or ongoing disputes, the PBG shall remain valid, effective, and enforceable until the final, formal issuance of a Discharge/Completion Certificate by CDNS.
- 17.6. Submission and verification of a valid PBG in accordance with this clause is an absolute pre-condition for the processing or payment of any invoices raised by the Service Provider. CDNS shall have no liability or obligation to process payments or make disbursements until an acceptable PBG is in place.

17.7. CDNS reserves the absolute and unconditional right to encash/forfeit the PBG, in whole or in part, without prior notice or reference to the Service Provider, subject to poor performance, default, or breach of any terms, warranties, or SLA obligations under this Agreement or the published RFP.

17.8. Forfeiture of the PBG shall be without prejudice to any other legal rights or remedies available to CDNS, including but not limited to contract termination, recovery of actual damages, and initiating blacklisting/debarment proceedings against the Service Provider under applicable public procurement rules and prevailing laws of Pakistan.

18 DISPUTE RESOLUTION

18.1 Internal Arbitration

The parties will attempt in good faith to resolve any controversy/ claim/ disagreement through internal arbitration of their respective senior management.

18.2 Independent Arbitration

That any dispute arising out of this Agreement which is not settled through internal arbitration of senior management from both the parties, shall be finally settled by panel of two independent arbitrators. Each of the parties hereto shall select one arbitrator each and the two independent arbitrators shall appoint an umpire. The award of the arbitrators shall be binding on the parties. The venue of arbitration shall be within Pakistan and the proceedings shall be governed by the Arbitration Act 1940. Each Party shall bear its own Arbitration cost.

19 Order of Precedence of Contract Documents

19.1. In the event of any inconsistency, conflict, or ambiguity between the provisions of the Contract Documents, the following order of precedence shall apply, with the document appearing first taking precedence over those listed subsequently:

- 1) This Agreement and Annexures to this Agreement or addendum if any including Approved Change Requests (CRs), to the extent that they specifically amend or supplement the relevant provisions of the Agreement;
- 2) Request for Proposal (RFP), including any amendments, clarifications, and addenda issued thereto;
- 3) Submitted and Approved Technical and Financial Bids

- 4) Mutual discussion and agreement in case the above 4 documents/set of documents do not contain a provision to address the conflict, inconsistency, ambiguity, or if the provisions already provided are incorrect, outdated, become irrelevant, or are no longer applicable etc.

20 Addendum

- 20.1. The Parties may, at any time during the validity of this Agreement, mutually agree to amend, modify, or supplement any provision of this Agreement through a written Addendum duly signed by their authorized representatives. Such Addendum shall become an integral part of this Agreement and shall have the same legal force and effect as the original Agreement. Any amendment shall be made in accordance with the applicable laws, rules, and regulations. In the event of any conflict between an Addendum and this Agreement, the provisions of the Addendum shall prevail only with respect to the matters specifically amended therein.

21 FORCE MAJEURE

- 21.1. Neither Party shall be liable for failure to perform or delay in performing any of its obligations under this Agreement if the failure or delay is caused by any circumstances beyond the reasonable control of the relevant Party, including but not limited to acts of God, war, civil commotion or industrial dispute. In such a case, both the parties will make an effort to ensure the restoration of the critical services on an immediate basis.

22 NETWORK

- 22.1. All data on the internal network is the property of the CDNS and it may reserve the right to inspect this data and to restrict or prevent any transfer to an external network.
- 22.2. Access to both the CDNS' internal and external network will be granted to authorized individuals of PAYSYS on a best effort basis.
- 22.3. Both internal and external networks will only be used for the work contracted out to PAYSYS.

23 GUARANTEES

- 23.1. The Service Provider shall guarantee that the software functionalities supplied shall be according to the Agreed Scope of Work as mentioned in [Annexure A Scope of Work](#). The Service Provider while making any enhancements in the CBA of CDNS under this

agreement will Guarantee that in no case the functionality, performance, impact, outcomes, reports and the Database etc. of existing CBA of CDNS be compromised/affected or degraded whatsoever.

- 23.2. The latest source code of the CBA of CDNS including complete Database Schemas, documentation, configuration details and other allied tools and utilities etc. [reflecting the running CBA of CDNS] will be provided by the Service Provider to THE CDNS and it will become the property of THE CDNS with full technology transfer. This will not include any standard tool used by Service Provider

24 GOVERNING LAW

- 24.1. This Agreement shall be governed by, interpreted and construed in accordance with the laws of the Islamic Republic of Pakistan and courts at Islamabad shall have exclusive jurisdiction.

25 WAIVER

- 25.1. The failure of a Party to enforce at any time the provisions of this Agreement shall not be construed as a waiver of any provision of this Agreement, or of the right of such Party thereafter to enforce each and every provision of this Agreement.

26 NOTICES

- 26.1. That any notice, demand, request or communication required or to be given under this Agreement shall be in writing. Such notice shall be considered sufficiently given when it is

26.1.1. Dispatched through a reputable courier/postal service company for delivery at the addressed to the appropriate party at the address shown on the first page of the Agreement or to such other address as may be designated in writing by such party from time to time or

26.1.2. Is by confirmed facsimile number as may be designated in writing by such party from time to time.

- **To PAYSYS Labs**

Attention: Mr. Mohammad Haris

Designation: Head of Business Development Pakistan

Address: 188 1 A, PECHS Block 2 PECHS, KARACHI

Email: Mohammad.haris@paysyslabs.com

- **To CDNS**

Attention: Director Operations, Central Directorate of National Savings
(CDNS)

Address: 23-N, Savings House, Civic Center, G-6 Markaz, Islamabad.

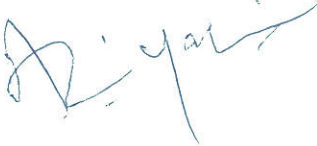
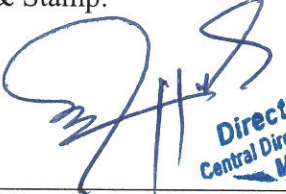
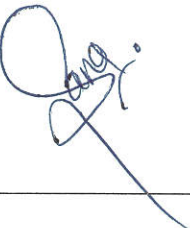
Email: atta@savings.gov.pk

27 ENTIRE AGREEMENT

27.1. This Agreement, including any and all amendments and attachments, contains the entire agreement between the Parties with respect to the matters covered herein, and may not be altered or modified except in writing, signed and mutually agreed to by duly-authorized representatives of each Party. ♦

♦ ♦

IN WITNESS WHEREOF the Parties have hereto agreed to this Agreement to be signed on the date first written above.

FOR & ON BEHALF OF PAYSYS LABS (PVT) LTD	FOR & ON BEHALF OF CENTRAL DIRECTORATE OF NATINOAL SAVINGS
Signature & Stamp: 	Signature & Stamp: 
Name: AZEEM YASEEN	Name: ATTA-ULLAH ZIA
Designation: Chief Technology Officer	Designation: Director (Operations)
Date: Aug 31st, 2026	Date: 31/08/2026.
WITNESS 1	WITNESS 1
Signature: 	Signature: 
Name: SALMAN MUSTAFA	Name: Muhammad Asim Khan Khattab
CNIC: 42201-6157394-7	CNIC: 61101-5559081-3
WITNESS 2	WITNESS 2
Signature: 	Signature: 
Name: MIRZA AHSAN SAEED	Name: SANA ARIF
CNIC: 42000-1761335-9	CNIC: 61101-7782023-2

28 ANNEXURE A – SCOPE OF WORK

28.1 Annexure A-1 – Group I- CBA Application Takeover and Transition-In

28.1.1 Overview and Scope

This Annexure sets out the complete scope of obligations, deliverables, and acceptance criteria governing the Application Takeover and Transition-In of the CDNS Core Business Application ("CBA") under this Agreement. The Service Provider shall assume full end-to-end responsibility for the CBA — including its source code, application modules, front-end and back-end systems, configurations, interfaces, databases, middleware, and the entire underlying technology stack — on an "As-Is-Where-Is" basis, across all operational branches.

The Transition-In phase shall be completed within six (6) months from the Effective Date. Upon formal acceptance of the Transition-In, the Service Provider shall assume complete ongoing responsibility for the managed services, maintenance, and administration of the CBA for the remainder of the Agreement term, as governed by [Annexure C Core Business Application Service Level Agreement \(SLA\)](#) and the post-takeover obligations set out in Section [28.1.9 Post-Takeover Managed Services Obligations](#) of this Annexure.

28.1.2 Business Process Coverage of the CBA

The CBA as it stands at the Effective Date provides a single, centralized, digitally-native system of record covering the full life-cycle of every National Savings product across CDNS's branch network. The Service Provider shall assume responsibility for all business processes currently automated within the CBA, spanning the following domains:

28.1.2.1 Core Banking and Ledger Operations

- i. Product configuration and parameter management — a centralized product factory supporting Defense Savings Certificates (DSC), Special Savings Certificates (SSC), Regular Income Certificates (RIC), Behbood Savings Certificates (BSC), Short Term Savings Certificates (STSC), Savings Accounts (SA, SSA, PBA, SWFA), Sarwa Islamic Savings Schemes (SISA, SITA), Prize Bonds (Bearer and Premium) and National Savings Bonds (NSB), with parameter-driven profit rates, tenures, denominations and eligibility rules.
 1. **Note, the list of products above is non-exhaustive, and any additional products added during the term of the agreement shall also be considered a part of the above-mentioned list.**
- ii. Customer onboarding, KYC/CDD, account opening and certificate issuance including KYC form templates (KYC sets, KYC group sets, KYC validators), biometric verification against NADRA, signature capture, and tagging of denomination-less TDC inventory to customers at the point of issuance.
- iii. Deposit, withdrawal, encashment, profit payment, and cheque operations — routed through the transactional front-end and executed via the transaction engine, with full maker-checker controls.
- iv. Inventory management— certificate inventory, withdrawal slip book inventory, stock orders, stock movement, allocation and holdings across branches and tellers.
- v. Vault management — vault setup configuration, branch/teller/treasury/van vault records, inter-vault movement of cash, prize bonds and instruments, and vault summary and reconciliation reporting.

- vi. Clearing operations — NIFT clearing and RAO cheque handling.
- vii. CRM, customer profiling and certificate life-cycle events — including pledging and release of pledge, transfer of Certificates, nominee operations and foreclosure workflows.

28.1.2.2 Digital, Compliance and Integration Layers

- i. AML/CFT and transaction monitoring — AML customer record, AML organization, AML list configuration and mapping, agency-match customer screening (PEP, NACTA, UNSC, MOFA, OFAC), transaction-rule matching, CTR/STR management and integration with the Reporting Authority for automated regulatory filing.
- ii. Micro Payment Gateway (MPG) / RAAST — MPG registration, pre-validation, payment, processor federation, Store-and-Forward batch processing, reversal and reconciliation; and RAAST Request-to-Pay (RTP) via ISO 20022 including IBAN/BIC title fetch, bank-list/BIC directory and RTP status inquiry.
- iii. Digital Prize Bonds and dematerialization of NSS instruments — virtual inventory, digital issuance, encashment and prize-money routing via MPG.
- iv. CDNS Digital Mobile Application — deployed on a SaaS model and integrated with the CBA via dedicated API contracts.
- v. Integrations currently live in production — NADRA (SOAP/BVS), 1Link (ISO 8583 for IBFT, Bill Payment, Paypak cards), RAAST (ISO 20022), CDC (dematerialization APIs), DMFAS/EAD, FABS, AGPR, , BOP (co-badged credit card issuance), UPI (debit card issuance), SBP, SMTP email relay, SMS gateway (SOAP), and the ADC middleware/CMS/ACS layer.

28.1.3 Solution Architectural Principles

The CBA shall be maintained and operated in accordance with the following core architectural principles throughout the term of the Agreement:

- Microservices-first — every business capability is owned by a single, independently deployable service with a defined API contract. Coupling between services is via REST/JSON rather than shared database access.
- Container-native — all application components shall be packaged as Docker containers and orchestrated on Kubernetes, with Rancher for cluster management and Fennel for network fabric, providing horizontal scalability, rolling upgrades and infrastructure portability.
- Stored-procedure-mediated ledger integrity — all value-bearing transactions shall be executed through Oracle stored procedures that enforce the transactional boundary, the double-entry ledger integrity, and the audit trail within the database itself, regardless of the originating channel.
- Channel-agnostic core — the CBA shall expose uniform transaction APIs consumed by branch counter UIs, the CDNS Digital Mobile Application, ADC channels and external payment rails (RAAST, 1Link, CDC, BOP, UPI).
- Regulator-aligned — the platform shall at all times comply with SBP regulations, FATF/AML-CFT requirements, NACTA/UNSC/MOFA screening obligations, and Government of Pakistan information-security and data-protection policies.

Note: The above-mentioned architectural principles for reference only at the time of contract signing. In case of any changes required to the architectural principles under the change request mechanism, or as a part of Paysys Lab's own enhancement of the CBA, then the changes shall follow secure development and deployment lifecycle, and all changes shall be documented within the detailed CBA documentation that Paysys shall maintain for, and share with CDNS as required.

28.1.4 Transition-In Methodology

The Transition-In phase shall be completed within six (6) months from the Effective Date and shall proceed through the seven milestone categories prescribed below. The Service Provider shall be responsible for the preparation, execution, and delivery of all milestones to the satisfaction of

CDNS. Formal acceptance of the Transition-In phase by CDNS is contingent on successful completion and CDNS approval of deliverables, including the end-to-end process and database mapping documentation required under [Section 28.1.5 Transition-In Milestones](#) of this [Annexure A-1 CBA Application takeover and Transition-In](#). Both parties hereby agree that knowledge transfer and the training of nominated CDNS resources is an extensive task and may continue beyond the 6-month transition-in period, and the continuation or conduction of such training shall not constitute a condition precedent to, nor delay, the initiation of Annual Maintenance and Support Charges and Managed Services Charges.

28.1.5 Transition-In Milestones

The timelines and milestones set out below are indicative only. The Service Provider may complete and deliver any of the Transition-In milestones earlier than the timelines stated below.

Milestone	Timeline	Obligations of the Service Provider
1. Transition Planning & Governance	Month 1	The Service Provider shall deliver a detailed Transition-In Plan within thirty (30) days of the Effective Date. The plan shall cover governance arrangements, dependency mapping, escalation matrix, communication protocols, and complete identification of end-to-end business and system processes, including transaction flows and their linkage with relevant back-end database objects, tables, and procedures.
2. Knowledge & Asset Acquisition	Month 1	The Service Provider shall formally hand over, reconcile, and verify all application, infrastructure, and operational assets. This shall include placing the full source code repository, build scripts, CI/CD pipelines, Oracle schema DDL, configuration files, and deployment runbooks into a CDNS-accessible structure, reconciled and verified by both Parties. The detailed document on process flows in descriptive form along with relevant screens should be prepared for the current state of CBA on as is where is basis.
3. Environment & Infrastructure Validation	Months 1–3	The Service Provider shall validate all application, database, middleware, and infrastructure configurations across production, disaster recovery (DR), and test environments. Where Group II IaaS infrastructure is being concurrently provisioned, the Service Provider shall ensure step-by-step CBA compatibility validation at each stage of hardware commissioning, maintaining continuity on existing infrastructure

Milestone	Timeline	Obligations of the Service Provider
4. System Verification & Stabilization	Months 2–4	The Service Provider shall verify system functionality and baseline performance; identify inherited issues and prepare a remediation plan; and validate end-to-end transaction flows covering application processing, data storage, database updates, and exception handling across the CBA. All issues attributable to the CBA as it exists at the Effective Date shall be remediated by the Service Provider at no additional cost.
5. Knowledge Transfer & CDNS Enablement	Months 2–6	The Service Provider shall conduct a structured training program for CDNS's nominated personnel across four role-based tracks: (a) Business and Operations Track; (b) Database Administration Track; (c) Application and Development Track; and (d) Operations and Support Track. The specific number of sessions, durations, and participant lists shall be agreed with CDNS during the Transition Planning phase. All training materials shall be handed over to CDNS and may be used for internal onboarding during and after the contract term. The Service Provider shall be responsible for ensuring that all documentation and training materials is kept up to date according to any changes and new developments within the CBA.
6. End-to-End Process & Database Mapping	Months 3–6	The Service Provider shall prepare, deliver, and validate through CDNS walkthroughs the complete Business Process Library described in Section 28.1.6 of this annexure A-1 , covering normal, exception, and reversal scenarios for each business transaction and operational process. Acceptance of the Transition-In phase shall be conditional on CDNS approval of these deliverables.
7. Formal Takeover & Acceptance	Month 6	Upon CDNS's written approval of all deliverables under milestones 1–6, the Parties shall jointly execute the Transition-In Acceptance Certificate, formally closing the Transition-In phase and commencing the Post-Takeover Managed Services regime under Annexure C Core Business Application Service Level Agreement (SLA) of this Agreement.

28.1.6 Knowledge Transfer Deliverables

The Service Provider shall prepare the following artefacts as part of the Transition-In phase. All artefacts shall be walked through with CDNS and formally handed over prior to Transition-In acceptance. The artefacts shall be delivered as a version-controlled documentation set and shall remain accessible to CDNS throughout and after the term of the Agreement:

Deliverable	Description and Acceptance Standard
End-to-End Process Maps	Process maps for each major business transaction and operational process, covering normal, exception, and reversal scenarios. Each map shall depict the application flow, the system interfaces involved, and reference the relevant back-end database objects (tables, views, stored procedures) used in the process. Maps shall be validated through walkthroughs with CDNS prior to acceptance.
System Interface Documentation	Complete documentation of all integrations currently live on the CBA — including NADRA, 1Link, RAAST, SBP, CDC, BOP, UPI, FBR, MoF/FABS, EAD, AGPR and the ADC layer — covering the protocol, message format, authentication mechanism, and operational handling procedures for each interface.
Database Schema Reference	A reference document describing the current Oracle 19c database schemas at a level sufficient for CDNS's designated personnel to understand and evaluate the structure, together with the relevant scripts for schema inspection and reporting. This document shall be reviewed and approved by CDNS as a condition of Transition-In acceptance.
Standard Reporting Formats	Hand-over of all structured reporting formats currently in use across the CBA, in the formats and layouts required by CDNS for operational, compliance, and regulatory reporting purposes.
Operational Reference Notes	Reference documentation covering routine operational activities including day-start procedures, end-of-day procedures, exception handling workflows, and reconciliation touch-points with external counterparties.
Training Materials	All training slide decks, handouts, and reference notes prepared for the four training tracks under Section 28.1.5 (point 5) of this Annexure. These materials shall be handed over to CDNS at the conclusion of each track and updated by the Service Provider as each enhancement goes live under this Agreement.

28.1.7 Transition-In Governance

CDNS and the Service Provider shall jointly agree on periodic transition in governance meetings, as and when required, to review and update the transition in tracker and activities, including milestone completion, outstanding actions, SLA baseline metrics, and issue remediation status. The meeting shall be supported by a RAID log (Risks, Assumptions, Issues, Dependencies).

The project management tool required under [Section 28.2.2.3 Project Management Tool of Annexure A-2 \(Change Management & CBA Enhancement Policy\)](#) of this Agreement shall be stood up within the Transition-In phase and shall host all Transition-In deliverables, Change

Requests, AMC tickets, and managed-services support tickets from commencement, providing CDNS with continuous real-time visibility into the engagement.

28.1.8 Transition-In SLA and Penalties

Transition-In penalties shall be governed by the SLA and Penalty framework set out in [Annexure C- Core Business Application Service Level Agreement \(SLA\)](#) of this Agreement. For reference, the key parameters are:

28.1.9 Post-Takeover Managed Services Obligations

Upon formal acceptance of the Transition-In phase, the Service Provider shall assume complete end-to-end responsibility for the ongoing management, administration, and support of the CBA for the remainder of the Agreement term. These obligations are in addition to, and not in derogation of, the SLA obligations set out in [Annexure C Core Business Application Service Level Agreement \(SLA\)](#).

28.1.10 CDNS Responsibilities During Transition-In and Post-Takeover

The following obligations of CDNS are prerequisites for the Service Provider's timely performance of the Transition-In obligations set out in this Annexure. Any failure by CDNS to fulfil these obligations within a reasonable period shall constitute a CDNS-caused delay, entitling the Service Provider to a corresponding extension of the affected milestone timeline:

- Provide the Service Provider with timely access to all existing hardware, software, credentials, configurations, and operational documentation necessary for the Transition-In phase.
- Coordinate with NTC and any other third parties whose cooperation is required for infrastructure validation and handover, including vendors of hardware being replaced under Group II.
- Nominate Personnel with the requisite mandate to take up matters regarding the approval of requirements, validation of deliverables, and UAT and Go Live sign-offs from authorized representatives of CDNS.
- Ensure timely review and approval of the deliverables described in [this Annexure A Scope of Work](#), including providing written feedback within ten (10) Business Days of each deliverable being submitted.
- Procure and maintain Oracle Database and Oracle 19c licenses as required for the CBA.
- Arrange and bear all costs related to rack space, power, cooling, and data center facilities at both the PR site (NTC Islamabad) and DR site (NTC Lahore), and cover all PR–DR linkage and connectivity charges required for replication, backup, and disaster recovery operations.

28.1.11 Scope Boundaries and Restrictions

The following restrictions define the boundaries of the Service Provider's obligations under this Annexure and are agreed by both Parties for the avoidance of doubt:

28.1.11.1 *Integration Scope*

The integrations in scope under this Annexure at the Effective Date are those currently in production, namely: NADRA SOAP/BVS, SMTP email relay, SMS SOAP gateway, 1Link (ISO 8583 and Open APIs), RAAST (ISO 20022), SBP, MoF/Finance Division/FABS, FBR, CDC, DMFAS/ EAD, DMFAS, BOP, UPI, AGPR/FABS, CDNS Mobile Application and Digital Account Opening Portals, and the ADC middleware/CMS/ACS layer. The Service Provider is to provide integrations with bill aggregator and Government's platform as mentioned in [Annexure A-6 Integration with Licensed Bill Aggregators](#) without having to go through the change request mechanism. Any additional integrations requested by CDNS — including with new Bill Aggregators, new government platforms, or new fintech counterparties with the exception of those mentioned in [Annexure A-6 Integration with Licensed Bill Aggregators](#) — shall be executed under the Change Request mechanism in [Annexure A-2 Change Management & CBA Enhancement Policy](#) at the agreed man-day rate.

28.1.11.2 *Cost of Third-Party Integration Services (Scope Restriction)*

The Service Provider's responsibility in respect of the integrations listed in Clause 28.1.11.1, whether currently in production or subsequently implemented, is limited to the design, development, integration and ongoing technical maintenance of the interfaces to the relevant third-party and government platforms. All charges, fees, commissions, per-transaction and per-message charges (including per-SMS charges), subscription, licensing, onboarding, certification and re-certification charges, and any other amounts payable to or levied by the integration counterparties themselves — including without limitation NADRA, 1Link, RAAST, the SMS and SMTP service providers, SBP, and any Bill Aggregator or government platform — shall be borne solely by CDNS (the Customer), whether one-time or recurring.

28.1.11.3 *Third-Party System Availability*

Third-party systems over which the Service Provider has no operational control — including NADRA, 1Link, RAAST/SBP MPG, CDC, bill aggregators, Bank of Punjab, UPI, and internet Suppliers — are assumed available, correctly certified, and stable in accordance with their published operating windows. Downtime, API changes, scheme changes, or certification delays on such third-party systems shall not constitute an SLA breach by the Service Provider.

28.1.11.4 *Training Scope*

Training delivered under the Transition-In phase covers CDNS's nominated Master Trainers and designated IT and operational staff. Subsequent train-the-trainer rollout to branch-level end users across the branch network is the responsibility of CDNS's internal training function. The Service Provider shall provide updated training materials to CDNS as each enhancement goes live under this Agreement.

28.1.11.5 *Business Process Re-Engineering*

Where new business processes are introduced by CDNS — for example, a new savings scheme, a new regulatory obligation, or a new customer-segmentation model — the Service Provider shall perform the technical development to support the process under the Change Request mechanism in [Annexure A-2 Change Management & CBA Enhancement Policy](#) . This includes the design and implementation of application workflows, business logic, validations, maker-checker and other system-enforced controls, data models, reports, and the integrations through which the CBA operates. The Service Provider shall not, however, be responsible for the redesign of CDNS's organizational or departmental structures, roles, staffing, and reporting lines.

28.1.11.6 *Security Incidents Arising from CDNS Credentials*

Security incidents arising from credentials issued by CDNS to its own staff or to third parties — including compromised CDNS user accounts, insider misuse, and unauthorized front-end access by CDNS-nominated users — are the responsibility of CDNS. The Service Provider shall cooperate fully with any investigation and remediation efforts but shall not be subject to SLA penalties in respect of such incidents.

28.1.12 *Transition-In Acceptance Certificate*

Upon formal closure of the Transition-In phase wherein complete documentation is provided by Service Provider on as is where is basis related to CBA software and infrastructure hardware including but not limited to integrations, relevant APIs, database schema, user manual, asset register, FSD etc., the Parties shall execute a Transition-In Acceptance Certificate in the form set out below, confirming that all deliverables under [28.1 Annexure A-1 – CBA Application Takeover and Transition-In](#) have been completed to CDNS's satisfaction.

28.1.13 *Waivers by CDNS in case of third-party dependency:*

Where CDNS, within its own authority, elects to waive any specific deliverable under this Annexure, whether in whole or in part, such waiver shall be recorded in writing and shall be

deemed a completed deliverable for the purpose of the Transition-In Acceptance Certificate.

In either such case, CDNS shall not use the non-delivery or incompleteness of the relevant deliverable as a basis for: (a) refusing or deferring Transition-In sign-off; (b) extending, imposing, or calculating penalties against the Service Provider beyond those attributable solely to the Service Provider's own performance failures; or (c) withholding any payments otherwise due and payable to the Service Provider under this Agreement.

For and on behalf of CDNS	For and on behalf of Paysys Labs (Pvt.) Limited
Name: _____	Name: _____
Designation: _____	Designation: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

28.2 Annexure A-2 – Group I- Change Management & CBA Enhancement Policy

28.2.1 Purpose and Scope

This Annexure sets out the Change Management Policy and CBA Enhancement framework governing all enhancements, customizations, new module developments, and modifications to the Core Business Application ("CBA") requested by CDNS during the term of this Agreement. To strengthen core functions, enhance user experience, improve data-driven operations, and support related integrated modules and functionalities, the CDNS plans to make multiple enhancements/customizations during the tenure of this agreement, introduce new capabilities to improve overall efficiency and analytics within the CBA. All such enhancements shall be catered to as per the man-day rates quoted in [Annexure D Change Request Form](#). This includes all customizations, upgrades, and future requirements as outlined, which will be carried out in accordance with the agreed-upon scope and timelines. CDNS will be responsible for providing the Service Provider with a detailed requirements regarding each change. All such work shall be executed through the Change Request ("CR") mechanism defined herein, at the Man-Day Rate agreed by the Parties and set out in [Annexure A-2 Change Management & CBA Enhancement Policy](#) of this Agreement.

For the avoidance of doubt, routine enhancements, maintenance, or changes to applications, modules, or functionalities already within the scope of the CBA shall not be treated as Change Requests; only new enhancements or customizations specifically requested by CDNS shall constitute Change Requests chargeable at the man-day rates quoted in Annexure D.

28.2.2 Change Management Governance Standard Operating Procedures

The Service Provider and CDNS have jointly agreed and shall maintain, and review as and when required, the following comprehensive Standard Operating Procedures (SOPs) for Change Management, governing all changes to the CBA, its supporting systems, infrastructure configurations, and operational processes that may affect the delivery of services under this Agreement. The SOPs shall serve as the formal framework for managing CRs throughout the term of the Agreement and shall be subject to revision by mutual written agreement of both Parties.

28.2.2.1 Types of CR:

CDNS and the Service Provider hereby agree that Change Requests under this Agreement shall be of two types:

- (i) **Single Phase Change Requests:** Enhancements, or activities that can be delivered as a single, continuous piece of work and shall not be broken into phases; and
- (ii) **Multiple Phase Change Requests** — any significant development or enhancement that, by reason of its scale, complexity, or duration, requires the work to be broken down and delivered in two (2) or more distinct phases, each with its own scope, timeline, and acceptance.

The man day rates of the relevant year will be applicable on single phase or multiple phase change request in which the CR is approved by CDNS. If the work on CR continues for more than a year the man day rates duly approved shall remain fixed.

28.2.2.2 6 Step Delivery Cycle

Every Change Request under this Agreement shall be executed through the following six-Step delivery cycle.

Step	Activity	Deliverables	CDNS Obligations
Step1	Requirements & CR Scoping	CDNS submits the high-level requirement for CR via the project management tool as the first preference or through email to the POC of Paysys for CBA who will create the ticket on project management tool. The Service Provider conducts business-analyst-led requirements sessions and delivers the detailed CR Form, including: a) Scope of work (including process flows, descriptions, and details of the change and its impact). b) Estimated Man-days and Cost c) Project Plan d) Any 3rd Party Dependencies, tools, or services required The CR is formally approved by CDNS before Step 2 commences.	CDNS shall provide high level business requirements including functional scope, regulatory drivers, target users, volume projections, and acceptance criteria. CDNS shall nominate a POC for each CR to take up matters regarding each CR with the authorized representatives of CDNS.
Step 2	Functional & Technical Design	After approval of the CR, the Service Provider shall submit the updated project plan, along with an initial draft FSD for CDNS to review and approve. The initial draft FSD shall be subject to	CDNS shall be responsible for the reviewing and approving the initial draft FSD submitted by Paysys before commencement of development and unit testing.

Step	Activity	Deliverables	CDNS Obligations
		updates or changes as each CR progresses, in case of any additional or incremental use cases, test scenarios, or requirements.	
Step 3	Development & Unit Testing	The Service Provider develops the CR against the approved initial draft FSD using its internal coding standards and CI/CD pipeline. Unit tests and System Integration Testing (SIT) scripts are executed. The Service Provider performs internal UAT testing of draft test cases and submits the internal testing report to CDNS. After review of internal testing Report by CDNS, the Service Provider shall deploy the completed build into the CDNS test environment and notify CDNS in writing that it is ready for UAT. The Service Provider deploys resources and its team and assists CDNS fully during UAT being conducted by CDNS and Paysys.	CDNS shall ensure the development pre-requisites and any third-party APIs, tools, SDKs, or any other services (where required as mentioned in the CR) are available and accessible for the Service Provider during this step. Furthermore, CDNS after reviewing the internal testing report of internal UAT done by Paysys on draft test cases nominates team for UAT testing in collaboration with Paysys Team.
Step 4	User Acceptance Testing (UAT)	The Service Provider shall prepare and submit the initial UAT test cases for CDNS's review. Both parties shall mutually agree upon the UAT test cases prior to commencement of UAT. Service Provider shall conduct UAT sessions with CDNS and support regarding defect identification, investigation, and resolution throughout UAT shall be provided by the Service Provider. During UAT, test cases may be added, modified, or deleted with the mutual agreement of both parties. Upon successful completion of UAT, the Service Provider shall submit the final updated Functional Specification Document (FSD), User Manual, QA Report, and the final UAT test cases incorporating all mutually agreed changes, for CDNS's review and approval. Thereafter, CDNS shall issue the UAT Sign-	CDNS and Paysys shall nominate authorized UAT testers from their respective side. The Service Provider shall facilitate and jointly conduct the UAT with CDNS, including execution support, defect identification, investigation, analysis, and resolution throughout the UAT period. Upon successful completion of UAT, CDNS shall issue the written UAT Sign-off.

Step	Activity	Deliverables	CDNS Obligations
		off, which shall be a mandatory prerequisite for commencement of Step 5.	
Step 5	Production Deployment	The Service Provider executes a controlled deployment into the CDNS production environment, with: (a) a cut-over plan agreed with CDNS; (b) a scheduled and pre-communicated deployment window; and (c) a tested rollback procedure in place. The Go-Live Date is the date on which the CR is made available in the production environment for live business transactions. The production deployment, where applicable shall have a pilot phase, where each deployment shall be done in a dedicated pilot branch/region prior to complete production roll out. As part of this Step, the Service Provider shall be responsible for delivering complete and updated documentation for the CR, including user manuals, technical/configuration documentation, and release notes. Go-Live shall not be treated as complete until this documentation has been delivered to and acknowledged by CDNS.	CDNS shall agree the deployment window and cut-over plan in advance. CDNS shall make available all necessary approvals required for production deployment in pilot region/ branch and later full deployment within the agreed schedule.
Step 6	Warranty Period & Hand-over to AMC	A Warranty Period of Six (6) months commences on the Go-Live Date. During this period: (a) the Service Provider shall monitor the new module and remediate all defects attributable to the CR at no additional cost; (b) any performance degradation, unavailability, or functional failure shall be treated as a warranty defect, not a change request; In case of bug/ warranty defect duly noted in the module developed through this CR or any issue reported in other existing modules of CBA because of the newly deployed change or module, the warranty period for module developed through CR shall restart, provided that the bug	CDNS shall report defects through the project management tool during the Warranty Period. In case of bug/ warranty defect duly noted in the module developed through this CR or any issue reported in other existing modules of CBA the warranty period for module developed through CR shall restart Issues arising from CDNS-initiated configuration changes made without coordination with the Service Provider shall not constitute warranty defects.

Step	Activity	Deliverables	CDNS Obligations
		or issue raised is of a level 3 critical severity level as defined in 30.5.6 Severity Level with Corrective Action . and (c) at the end of the Warranty Period, the module is formally absorbed into the Workstream 1 managed-services regime and becomes subject to AMC charges at the rate quoted in Annexure B, applied to the development cost of the module.	

28.2.2.3 Project Management Tool

The Service Provider shall provide and maintain a JIRA instance as the single platform (along with provision for intimation to Paysys POC through email who will create ticket) for logging, tracking, and managing all Change Requests, enhancements, SLA tickets, and managed-services support tickets for CDNS throughout the term of the Agreement. The tool shall be stood up within the first two weeks of the Transition-In phase.

CDNS shall have full, real-time visibility into the status of all CRs, including approved Man-Day estimates, delivery timelines, phase completion status, UAT sign-off, and go-live dates. No CR shall be actioned by the Service Provider without a corresponding ticket having been raised and approved in the project management tool.

The use of the project management tool shall not preclude or replace correspondence through email or other channels. The Service Provider shall further provide CDNS with access to detailed, customized reports on all tickets generated through the project management tool.

28.2.2.4 Governance Forums

Operational and Steering Committee forums shall be constituted with CDNS. Meeting frequencies and committee composition shall be agreed with CDNS at the start of each CR.

28.2.3 Deliverable/ Milestone Based Payment Terms and Conditions

Payment against each approved Change Request shall be made on a milestone basis as follows:

- i. 15% of the CR Value shall be invoiced upon formal approval of the CR at step 1 after submission of the detailed CR form covering Scope of work (including process flows,

descriptions, and details of the change and its impact), Estimated Man-days and Cost, Project Plan, any 3rd Party Dependencies, tools, or services required,

- ii. 70% of the CR value shall be invoiced upon UAT Signoff by CDNS at step 4.
- iii. 15% of the CR Value shall be invoiced upon Go-Live/ Production Deployment at step 5.

All invoices shall be submitted by the Service Provider through the approved channels (email/courier/self-delivery) accompanied by the relevant milestone completion evidence. CDNS shall notify Paysys within Ten (10) Business Days of receiving the invoice of any discrepancy/objection to an invoice, which shall be rectified by Paysys within Ten (10) Business Days whereupon a corrected/amended invoice shall be issued/submitted by Paysys, and payment shall be made by CDNS within Forty-Five (45) days of invoice approval.

28.2.3.1 Suspension of a CR

Where work on a CR is suspended due to any third-party dependency or CDNS-side factor beyond the reasonable control of the Service Provider, the following shall apply:

- Payments corresponding to milestones already achieved and invoiced prior to suspension shall not be withheld, set off, or reclaimed by CDNS.
- Upon suspension, the Service Provider shall document the final status of the CR, raise the invoice for all milestones achieved to that point, and the CR shall be formally closed.

28.2.4 Changes to Scope of Work

Where CDNS wishes to change or modify the scope of any in-flight CR, or to introduce a new requirement not covered within an existing approved CR, it shall submit a written request to the Service Provider through the project management tool or through email to the POC of Service Provider. The Service Provider shall assess the impact on Man-Days, cost, and timeline within five (5) Business Days, and the revised scope shall be formally approved by both Parties before any additional work is commenced. No change to scope shall be considered authorized unless confirmed in writing. Service Provider shall accommodate scope variations of up to ten percent (10%) of the originally approved Man-Day effort within the existing CR Value without additional charge.

28.2.5 Degradation Clause

Notwithstanding the above, where a delivered and accepted module subsequently fails to perform to the specifications set out in its approved FSD and UAT sign-off — whether during the Warranty Period or thereafter — the Service Provider shall investigate and remediate the root cause. If the

root cause is attributable to the original development, remediation during the Warranty Period shall be at no cost. Post-Warranty Period remediation of development-attributable defects shall be subject to the AMC SLA penalty framework in [ANNEXURE C – CORE BUSINESS APPLICATION SERVICE LEVEL AGREEMENT \(SLA\)](#).

28.3 Annexure A-3 – Group I- CBA Annual Maintenance and Support

28.3.1 Purpose and Applicability

This Annexure sets out the scope of the Annual Maintenance and Support services to be provided by the Service Provider for the Core Business Application ("CBA") The Service Provider's obligations under this Annexure shall commence on the date of execution of the Agreement shall continue for the remainder of the Agreement term, including all extension years.

The detailed Service Level Agreement governing support response times, severity levels, uptime obligations, penalty matrices, and reporting requirements is contained in Annexure C of this Agreement.

28.3.2 Scope of Annual Maintenance and Support

The Service Provider shall provide end-to-end support, maintenance, and management of the CBA on a turnkey basis, covering the following:

28.3.2.1 *System Management and Operational Oversight*

The Service Provider shall be responsible for the installation, configuration, and ongoing maintenance of the entire CBA environment, including all application modules, middleware, and stack components. The Service Provider shall implement and maintain quality assurance controls to ensure system performance, reliability, and compliance with CDNS's operational standards at all times.

28.3.2.2 *Database Administration*

The Service Provider shall provide comprehensive database administration services covering schema design, query and performance optimization, data replication, execution of scheduled and ad-hoc DR drills, and physical database backups including secure off-site backup services. The Service Provider shall maintain full visibility of backup status to CDNS and ensure demonstrable compliance with CDNS's backup and retention requirements throughout the contract term.

28.3.2.3 *Security Hardening and Compliance*

The Service Provider shall implement and continuously enforce security protocols, access controls, and monitoring mechanisms to safeguard the integrity of the CBA and the confidentiality of CDNS's data. Security patches and vulnerability fixes shall be applied within timelines to be agreed between the Parties by severity level, as defined in Annexure C. The Service Provider shall maintain audit logs for all security events

and shall cooperate fully with CDNS in resolving audit findings within mutually agreed timelines.

28.3.2.4 Performance Optimization and Technical Updates

The Service Provider shall proactively monitor CBA performance metrics, identify and address performance bottlenecks, and implement technical updates and bug-fixes as required to maintain system performance in line with the uptime and service credit standards in [Annexure C Core Business Application Service Level Agreement \(SLA\)](#).

The Service Provider and CDNS teams shall jointly define the scope of the required reports, statistics, metrics, and views to be provided to, or made visible to, CDNS. The agreed reports, statistics, metrics, and views shall be developed and provided by the Service Provider.

28.3.2.5 Disaster Recovery

The Service Provider shall conduct two (2) DR drills per contract year, each spanning a minimum of one week, with documented RTO/RPO validation and a post-drill report submitted to CDNS following each drill. In the event of failure to meet defined RTO/RPO parameters during a drill, corrective measures shall be implemented within a mutually agreed remediation timeline. Repeated failure to meet DR performance benchmarks shall be subject to SLA penalties in accordance with [Annexure C Core Business Application Service Level Agreement \(SLA\)](#)

28.3.2.6 Integration Maintenance

The Service Provider shall maintain all integrations enumerated [28.1.2 Business Process Coverage of the CBA of Annexure A-1](#) in live, operational condition throughout the term. Integration failures shall be classified by severity level and responded to within the timeframes set out in [Annexure C Core Business Application Service Level Agreement \(SLA\)](#). Downtime, API changes, or certification delays attributable solely to third-party systems outside the Service Provider's control shall not constitute an SLA breach. The Service Provider shall promptly notify CDNS of any such third-party failures and provide regular status updates until resolution.

28.3.2.7 Reporting

The Service Provider shall submit monthly SLA compliance reports to CDNS within five (5) to seven (7) Business Days of month-end, accompanied by automated

application performance management and monitoring dashboards, backup status logs, replication health reports, and any other documentation required to validate SLA performance for that month.

28.3.3 AMC for Newly Developed Modules

Upon expiry of the Six (6) month Warranty Period following the Go-Live of any CR delivered under [Annexure A-2 Change Management & CBA Enhancement Policy](#), the developed module shall automatically transition into AMC under this Annexure. The scope of AMC for each such module shall include:

- Availability and performance monitoring of the module.
- Incident resolution and defect fixing.
- Compatibility maintenance with changes to the core CBA.
- Security patches and performance tuning.
- Ongoing documentation updates.

AMC charges for developed modules shall be calculated as a percentage of the actual development cost of each module, at the AMC percentage rate quoted in [Annexure B Commercials and Payment Terms](#) of this Agreement. All developed modules under AMC shall be subject to the same uptime and SLA metrics as the core CBA, as defined in [Annexure C Core Business Application Service Level Agreement \(SLA\)](#). If any such module subsequently exhibits performance degradation, unavailability, or functional failure during the AMC period, such degradation shall be treated as an AMC SLA breach and governed by [Annexure C Core Business Application Service Level Agreement \(SLA\)](#), not as a development defect requiring a new Change Request. Penalties for AMC SLA breaches shall be calculated against the AMC value of the affected module and not against its original development cost.

28.3.4 Discontinuation or Closure of a Developed Module

(a) In the event that CDNS decides to discontinue, discard, or close any developed module that is under Annual Maintenance, CDNS shall submit a written request to the Service Provider at least fifteen (15) days prior to the intended date of discontinuation.

(b) The Service Provider shall review the request and respond with any dependencies, processes, or operational impacts arising from the closure of the module, together with the indicative timelines and efforts/costs required where applicable.

(c) The quarterly AMC payments for any module requested to be closed shall not be refunded, in whole or in part, by the Service Provider, and CDNS shall not withhold payments against any invoices already submitted.

(d) Where a discontinuation request is made on or close to the date an invoice falls due, the Parties shall mutually determine whether the next invoice is to be raised, based on the effort and timelines required to close the module.

28.3.5 Support Channels and Ticketing

CDNS shall report all support issues, defects, incidents, and service requests through the JIRA project management tool established under [Annexure A-2 Change Management & CBA Enhancement Policy](#) of this Agreement. Issues shall be raised with the relevant severity classification, and the Service Provider shall acknowledge, respond to, and resolve all issues within the timeframes prescribed by [severity level in Annexure C Core Business Application Service Level Agreement \(SLA\)](#). The Service Provider shall maintain telephone, email, and remote-access support capabilities for all severity levels, with 24x7 availability for Severity Level 4 (Emergency) incidents.

The complete SLA framework applicable to the maintenance and support obligations in this Annexure — including severity level definitions, response and resolution targets, the uptime matrix, the monthly service credit table, the penalty calculation methodology, the penalty cap, and the chronic non-performance provisions — is set out in [Annexure C Core Business Application Service Level Agreement \(SLA\)](#) of this Agreement, which forms an integral part of the AMC regime established by this [Annexure A-3 CBA Annual Maintenance and Support](#).

28.4 Annexure A-4 – Group II- IaaS — Proposed Hardware and Software Infrastructure

28.4.1 Overview and Scope

This Annexure sets out the Infrastructure as a Service ("IaaS") to be provisioned by the Service Provider for CDNS under this Agreement. The IaaS shall provide a high-availability, dual-site hosting environment for the Core Business Application (CBA) and its associated systems at the NTC Data Centre, Islamabad ("Primary Site" or "PR") and the NTC Data Centre, Lahore ("Disaster Recovery Site" or "DR"), in full alignment with CDNS's performance, scalability, security, and regulatory compliance objectives.

28.4.2 CURRENT AND PROJECTED APPLICATION AND INFRASTRUCTURE UTILIZATION DETAILS

28.4.2.1 Software Application details

- Software application is programmed in JAVA
- APACHE Tomcat is used as Web Server where required
- Software application is based on micro-services architecture and runs on Docker based environment and utilizes tools such as Kubernetes, Rancher and Fennel for network fabric.
- REST Interface is used to expose web services where required
- Application also integrates with
 - NADRA on SOAP Interface
 - Email server using SMTP
 - SMS service using SOAP interface
 - 1Link via ISO 8583 and OpenAPIs
 - RAAST via ISO 20022
 - **SBP** – Regulatory reporting, prize bond draw coordination, settlement references
 - **Ministry of Finance** / Finance Division– Fiscal reporting, investment inflows/outflows, government accounting
 - **FBR** – Withholding tax deduction, reporting, and compliance validation
 - **CDC** – Dematerialization, digital securities provisioning, investor records
 - **EAD**– Policy-driven data sharing, financial disclosures, and reporting
 - BOP for co-badged credit card issuance
 - **UPI for debit cards issuance**
 - **AGPR/ FABS – Financial Data Reporting**
 - **ADC Applications like middleware, CMS, ACS**
 - **1Link for ATM issuance, Bill payments, IBFT, and Paypak cards issuance**

The complete source code for the Core Business Application (CBA of CDNS), developed by our vendor, will be provided to the Service Provider via a GitLab repository. The source code was developed as part of the ongoing collaboration with CDNS. Hosting Infrastructure details

- The application currently runs in a high availability cluster mode on HP Blade servers
- The various components of application run on Virtualized environments (VMWare and vSphere is used)
- Database is Oracle 19c – Configured as a 2 Node Oracle RAC which is setup on Physical Servers.
- NGINX is used as Reverse Proxy server and all application access either from Branches or from any other software is routed via NGINX.

28.4.2.2 Current Storage Utilization (Pre-Purging)

The following outlines the current hardware and infrastructure utilized at the Primary (PR) and Disaster Recovery (DR) site of CDNS. These specifications will serve as the minimum reference for the Service Provider when proposing their infrastructure solutions:

As-Is of PR Site (NTC Islamabad):

- **Database (DB):** 32 cores
- Core Business Application (CBA): 96 cores
- **Total Cores:** 128 cores
- **RAM:** 2 TB
- **Utilized Storage:** 110 TB
- **Raw Storage:** 190 TB
- Active VMs- 134
- **Inactive VMs - 37**

As-Is of DR Site (NTC Lahore):

- **Database (DB):** 32 cores
- Core Business Application (CBA): 96 cores
- **Total Cores:** 128 cores
- **RAM:** 2 TB
- **Utilized Storage:** 110 TB
- **Raw Storage:** 190 TB
- Active VMs- 133
- **Inactive VMs - 8**

This current infrastructure sizing, as detailed above, must be taken into consideration when proposing the new infrastructure, ensuring scalability, performance, and compatibility with CDNS’s requirements. The Service Provider shall be responsible for replicating the same infrastructure specifications proposed for the Primary (PR) site at the Disaster Recovery (DR) site, ensuring identical performance, scalability, and reliability across both locations.

28.4.2.3 Current Utilization and Growth Projections

The following table outlines the **current utilization** and **projected growth** for key infrastructure components, including storage, compute and RAM, based on **CDNS’s operational trends** and **future expectations**. This information will assist the Service Provider in estimating the required infrastructure to accommodate both current and future operational demands.

Utilization Metric	Current (2025)	Projected Growth (2026-2030)	Projected Value (2030)
--------------------	----------------	------------------------------	------------------------

Total Number of Customers	3.7 million	+1.3 million (Growth)	5 million
Biometric Transactions (Successful)	1,000,000	~ 500,000	~1,500,000
Total Transactions (Receipts & Payments, Jan-Dec 2025)	74,186,533	+50% (Approx.)	111,280,000
ATM Transactions (Jan-Dec 2025)	4,400,000	+25% (Approx.)	5,500,000
Mobile App Transactions (Jan-Dec 2025)	1,200,000	+30% (Approx.)	1,560,000
System Transactions (Automated accruals, etc.)	25,180,044	+40% (Approx.)	35,250,000

Note: The projections are based on CDNS’s expectation of continued growth in the number of customers and transactions, as outlined above. The Service Provider shall base their estimates for infrastructure sizing, including storage, compute, RAM, and CPU, on the above utilization figures and the projected growth rate.

28.4.3 Hardware & Software Components to be provided by Paysys for this contract

The hardware tier shall be provisioned in dual-redundant configurations at both the PR and DR sites, comprising the following equipment families:

- Compute Servers — dual-socket x86 servers based on Intel Xeon Gold class processors (or equivalent), with on-board ILO/out-of-band management, dual power supplies, and dual fibre-channel HBAs.
- Unified Storage Array (SAN) — dual-controller block storage with NVMe/SSD tier, hot-swap drive shelves, and enterprise data services (deduplication, compression, thin provisioning, snapshots, replication, encryption).
- SAN Fabric Switches — dedicated 16G/32G fibre-channel switches (or equivalent) supporting multipathing, port and WWN zoning, ISL trunking, and fabric segmentation.
- LAN Switches — high-throughput L2/L3 switches (or equivalent) with VxLAN, stacking, clustering/chassis, and full IP routing services.
- Next-Generation Firewalls (NGFW) — physical or virtual NGFW pair (or equivalent) with high availability, IPS, threat protection, IPsec VPN, and SD-WAN capability.
- Rack Infrastructure — full-height racks with structured cabling, intelligent PDUs, and cable management.

28.4.3.1 Server (Compute) Specifications

Attribute	Specification
Socket Capacity	Dual socket
Processor	Intel Xeon Gold class or equivalent
Cores per Socket	12 cores or higher
Memory Type	DDR4 / DDR5 ECC or equivalent
Memory Capacity	256 GB per node (baseline; scalable)
RAID Levels Supported	0, 1, 5, 10
Network Interface	Dual 1G / 10G Ethernet (scalable)
Network Module	Electrical / SFP / SFP+ or equivalent

Attribute	Specification
Fibre Channel HBA	Dual 16G / 32G or equivalent
ILO / Out-of-Band Management	Included
Power Supply	Dual redundant (A+B feed)
Form Factor	Rack-mounted, up to 18U per stack

28.4.3.2 Unified SAN Storage Specifications

Attribute	Specification
Controllers	Dual controllers (active-active, scalable)
FC Port Speed	16G / 32G
FC Ports	8 ports (scalable)
LAN Ports	2 ports for management and replication
Enclosures	1 base enclosure (scalable to multi-shelf)
Disk Capacity	24 drive bays (scalable)
Disk Sizing Options	3.84 TB / 7.68 TB / 15.36 TB per drive; total storage 70–100 TB over the contract period or equivalent capacity
Disk Types	NL-SAS / NVMe SSD / SAS / SATA tiers or equivalent
Hot-Swap Capability	Yes — drives, controllers, power supplies
RAID Levels	5, 6, 10
Power Supply	Dual redundant
Form Factor	Up to 12U
Data Services	Unified storage, deduplication, compression, thin provisioning, hyper-snapshots, replication, WWN profiling, zoning, storage pools, LUN groups, encryption

28.4.3.3 LAN Switch Specifications

Attribute	Specification
Port Count	18 / 24 / 30 ports (scalable)
Port Speed	1G / 10G / 25G
Switching Capacity	500 Gbps or above

Attribute	Specification
Packet Forwarding Rate	500 Mpps or above
CPU	1.5 GHz or above
RAM / Flash	2 GB RAM / 1 GB Flash or above
Module Types	RJ45 / SFP / SFP+ / QSFP or equivalent
Power Supply	Dual
Feature Set	Full L2/L3 standards, VLANs, HA, clustering/chassis, stacking, VxLAN, IP services, routing, multicast, network management

28.4.3.4

Next-Generation Firewall Specifications

Attribute	Specification
Firewall Type	NGFW — Physical or Virtual deployment (or equivalent)
High Availability	Yes — active/passive or active/active
Port Speed	1G / 10G or above
IPS Throughput	8 Gbps or above
NGFW Throughput	5 Gbps or above
Threat Protection Throughput	5 Gbps or above
IPv4 Throughput	50 Gbps or above
Concurrent Sessions	2 million or above
New Sessions per Second	200,000 or above
Firewall Policies	50,000 or above
IPSec VPN Throughput	20 Gbps or above
Routing Capabilities	Static routing, policy routing, SD-WAN
Power Supply (Physical)	Dual
Form Factor (Physical)	Up to 4U

28.4.3.5

SAN Fabric Switch Specifications

Attribute	Specification
Fibre Ports	Up to 24

Attribute	Specification
Speed	16G / 32G
Port Type	SFP / SFP+ or equivalent
Power Supply	Dual
Multipathing	Yes
Port Zoning & WWN Zoning	Yes
ISL & Trunking	Yes
Authentication & Segmentation	Yes
Virtualization Support	Yes
Form Factor	Up to 4U

28.4.3.6 Software Components

The software stack shall be provisioned as set out below.

Software Layer	Proposed Solution	Licensing Model
Operating System	Red Hat Enterprise Linux (latest stable release) or equivalent	Paid (subscription)
Hypervisor / Virtualization	Red Hat Virtualization Datacenter or equivalent	Paid (subscription)
Container Orchestration	Kubernetes (latest stable release) or equivalent	Open source
Network Monitoring	Zabbix / Nagios / Grafana or equivalent	Open source
System Utilities — DNS	PowerDNS or equivalent	Open source
System Utilities — Reverse Proxy / LB	NGINX or equivalent	Open source
Security (XDR / EDR / MDR / Antivirus)	Sophos MDR or equivalent	Paid (subscription)
Vulnerability Management	Tenable Nessus / Nexus or equivalent	Paid (subscription)

Software Layer	Proposed Solution	Licensing Model
2FA Management	Open-source TOTP/HOTP-based 2FA platform (e.g., Guacamole) or equivalent	Open source
Additional Tooling	As per requirement Open source by default; commercial alternatives via Change Request if requested by CDNS.	Open-source by default or commercial/license alternative required due to restrictions imposed by the Government of Pakistan/ CDNS shall be treated as a Change Request.
Oracle Database / Oracle 19c	Excluded from Service Provider scope — CDNS responsibility	CDNS Responsibility

Note: The phrase or equivalent is added to the above hardware and software components. This is in case the EOL or EOS of a certain component is announced or if the Service Provider provisions an upgraded alternative component instead of the one mentioned above. The Service Provider shall be responsible for ensuring that the provided Hardware and Software IAAS shall be compatible with the CBA and meets CDNS’s requirements.

Note: Where CDNS or its regulators like the Government of Pakistan or the Finance Ministry restricts the use of any tool/ software whether open source or licensed, the Service Provider is responsible to propose, arrange and use the permissible alternative as compatible with CDNS requirements. If the alternative tool requires commercials/licensing then the procurement of such shall be treated as a change request

28.4.4 Compatibility with Existing CBA Infrastructure

The proposed IaaS stack shall be fully interoperable with CDNS's existing CBA environment, including the Oracle 19c RAC database tier, the NGINX reverse proxy layer, and the established backup infrastructure (HPE 3PAR storage and HPE MSL tape library). Specifically:

- The proposed stack is x86-based and certified for Red Hat Enterprise Linux, ensuring native compatibility with Oracle 19c RAC and virtualized workloads.
- The fibre-channel SAN fabric shall inter-operate with CDNS's existing HPE 3PAR storage and HPE MSL tape library for backup and on-site high availability.
- The network design shall support VLAN extension and VxLAN overlays, and the NGFW pair shall be interoperable with the existing perimeter to enable parallel staging during cutover.

28.4.5 Installation and Configuration Plan

The Service Provider shall execute the deployment of the IaaS under a phased plan. The following activities shall be carried out by the Service Provider as part of the IaaS provisioning scope:

- Supply, delivery, and commissioning of hardware and associated components at the PR and DR sites.
- Preparation and submission of a High-Level Design (HLD) and Low-Level Design (LLD) for joint sign-off with CDNS's technical team prior to installation.

- Rack mounting, A+B power connectivity, structured cabling, and physical installation of all equipment.
- Installation and configuration of compute, storage, SAN fabric, and network infrastructure.
- Firmware, BIOS, and software upgrades to OEM-recommended stable versions at time of commissioning.
- Configuration of the virtualization platform, HA clusters, and associated services.
- Establishment of network adjacency with the existing rack and connectivity to relevant service-provider links.
- SAN zoning, storage provisioning, RAID configuration, and multipathing implementation.
- Performance optimization, redundancy validation, and failover testing.
- Integration with the existing network, storage, backup, and operational tooling.
- OEM warranty registration, post-deployment support, and stabilization services.

28.4.6 Migration Plan from Existing to New Infrastructure

Migration shall be executed as a low-risk, reversible, phased project prioritizing business continuity, data integrity, and minimal user-visible downtime. The Service Provider shall:

- Prepare migration, rollback, and contingency plans, and conduct a joint walkthrough with CDNS's technical team prior to execution.
- Migrate virtual machines, applications, and workloads to the new environment using OEM-supported and validated tools.
- Migrate and validate database services with minimal downtime, leveraging Oracle Data Guard or RMAN-based techniques.
- Conduct end-to-end validation of all upstream and downstream integrations (NIFT, SBP MPG, ILink, RAAST, NADRA, and others) against a controlled test transaction set before production cutover.
- Maintain a hyper-care support window post-cutover, holding the legacy platform warm for a mutually agreed stabilization period before decommissioning.

28.4.7 Capacity and Scalability

The proposed IaaS architecture shall scale horizontally and vertically across compute, storage, and network tiers to absorb the projected growth in customers, transactions, and system workloads over the contract period.

- Compute clusters shall support node addition without service interruption.
- The storage array shall support controller upgrades, additional drive shelves, and tiered media (NVMe / SSD / NL-SAS) so that capacity and IOPS scale independently.
- The network shall support stacking, VxLAN overlays, and NGFW capacity headroom sufficient for projected transaction volumes.

Storage Sizing Condition:

The Service Provider undertakes that the IaaS storage shall suffice for the CBA and its continued operations is strictly conditional upon that the Service Provider shall provide complete guidelines for the archiving and purging policy. CDNS shall review the policy guidelines, ensure compliance with applicable government policies, obtain formal approval within a reasonable timeframe, and provide the final approved policy to the Service Provider.

The Service Provider shall be responsible for executing the database purging and archiving activities in accordance with the approved policy.

28.4.8 Power, Cooling, and Space Requirements

The indicative physical footprint per site is set out below. These figures are estimations based on current sizing assumptions and indicative OEM thermal and power envelopes. Final requirements shall be jointly confirmed between the Service Provider and CDNS's technical team following OEM order confirmation.

Resource	Indicative Requirement (per site)	Notes
Rack Space	2 full racks	Rack 1: Compute & Storage — Rack 2: Network & Security
Power Allocation	25 Amp per rack (flexible consumption)	Dual A+B feed, intelligent PDUs
Cooling	Sized to rack thermal load	Aligned to OEM thermal envelopes for final hardware ordered
Connectivity	Redundant top-of-rack uplinks and PR–DR link	PR–DR linkage to be arranged and funded by CDNS

CDNS Responsibility: In accordance with this Agreement, CDNS shall arrange and bear all costs related to rack space, power, cooling, and data center facilities at the PR and DR sites, and shall cover all PR–DR linkage and connectivity charges required for replication, backup, and disaster recovery operations.

28.4.9 OEM Warranty and Support Undertaking

The Service Provider hereby undertakes that all hardware and software supplied under this Annexure shall, throughout the contract term, remain under valid OEM SLA coverage and warranty. The Service Provider's standard support construct is a 3+2 model — three (3) years of OEM warranty and support from the date of provisioning, extendable by a further two (2) years — thereby providing continuous, OEM-backed support for the full duration of the Agreement.

Any hardware or software component approaching End-of-Life (EOL) or End-of-Support (EOS) shall be proactively identified by the Service Provider and handled as follows: either through replacement of the affected component at the Service Provider's cost, or through procurement of OEM-issued extended-support contracts with the relevant documentation provided to CDNS. In either case, no service-impacting EOL/EOS event shall occur during the contract term.

OEM certificates, datasheets, and authorization letters for all provisioned hardware and software shall be furnished to CDNS at the contract execution stage and updated whenever a component is substituted or upgraded.

28.4.10 Procurement and Delivery Timeline

Following contract execution, the Service Provider shall lock the final Bill of Materials (BOM), complete HLD/LLD sign-off with CDNS, and proceed with OEM procurement, site preparation, build, integration, migration, and stabilization.

Paysys will be responsible for hardware and software delivery and commissioning on both PR and DR sites within 6 months from effective date of contract (Signing date).

28.4.11 Scope Exclusions

- Oracle Database and Oracle 19c licenses — procured and maintained by CDNS.
- Rack space, power, cooling, and data center facilities at NTC Islamabad and NTC Lahore — CDNS responsibility.
- PR–DR network linkage and connectivity charges — CDNS responsibility.

28.5 Annexure A-5 Group-III- Infrastructure Managed Services

28.5.1 Purpose and Scope

This Annexure sets out the Infrastructure Managed Services to be provided by the Service Provider for the entire infrastructure deployed under this Agreement, covering both the new IaaS stack provisioned under [Annexure A-4 IaaS — Proposed Hardware and Software Infrastructure](#) and the existing CDNS hardware at the NTC Primary Site (PR), Islamabad and the Disaster Recovery Site (DR), Lahore. The managed services shall be delivered on a 24x7x365 basis from the Effective Date of this Agreement.

The detailed SLA framework governing severity levels, response times, resolution targets, penalty matrices, and reporting is contained in [Annexure C Core Business Application Service Level Agreement \(SLA\)](#) of this Agreement. This Annexure A-5 defines the scope of the managed services; Annexure C governs how they are measured and penalized.

28.5.2 Managed Services for Infrastructure as a Service (IaaS)

- The Service Provider shall also be responsible for the ongoing management and maintenance of the entire infrastructure provisioned as IaaS, which includes both hardware and software as well as the existing hardware deployed at NTC PR and DR site. This will include providing 24/7 monitoring, incident management, routine maintenance, troubleshooting, and technical support for the hardware deployed within the NTC Data Centers. The managed services will ensure the reliability, availability, and performance of the infrastructure throughout the lifecycle of the hardware.
- The Service Provider shall provide a comprehensive managed services framework that ensures the hardware remains operational, secure, and compliant with CDNS's evolving business and regulatory requirements. This includes proactive and reactive support, covering all hardware-related issues to prevent service interruptions and reduce downtime.

28.5.3 Key Deliverables for Managed Services:

Note: All of the below shall be applicable for both PR and DR sites of CDNS, with the PR site at NTC Islamabad and DR site at NTC Lahore.

28.5.3.1 24/7 Monitoring and Incident Management:

- **Real-time monitoring** of all infrastructure components, including servers, SANs, switches, network devices, operating systems, network monitoring tools, and security software. The Service Provider will be responsible for providing **real-time**

telemetry of hardware performance, system utilization, temperature, and other key operational metrics.

- **Incident management** processes will be in place to identify, log, and resolve hardware and software issues quickly and effectively, with escalation procedures in place for [emergency incidents \(Severity 4\)](#).
- The Service Provider must provide access to a **ticketing system** that will allow CDNS to log incidents, track progress, and ensure timely resolution of hardware issues.

28.5.3.2 Routine Maintenance and Patching:

- The Service Provider shall perform regular preventative maintenance, including firmware updates, patch management, security updates, and performance optimization. This will ensure that all hardware and software components continue to function at optimal performance and that security vulnerabilities are mitigated as part of the ongoing service.
- A maintenance schedule will be provided, detailing the frequency of maintenance tasks, and the Service Provider shall adhere to this schedule to avoid disruption to CDNS's operations.

28.5.3.3 Troubleshooting and Issue Resolution:

- The Service Provider will be responsible for diagnosing and resolving any hardware-related issues that arise, ensuring minimal downtime and business continuity. This includes handling hardware failures, replacing faulty components, and coordinating with hardware vendors for warranty support or component replacement.
- In the event of a hardware or software failure, the Service Provider will be responsible for providing a quick resolution, including replacing faulty components and restoring full functionality in a timely manner.

28.5.3.4 Disaster Recovery and Backup Management:

- The Service Provider will work with CDNS to establish and maintain disaster recovery procedures for the entire infrastructure (hardware + software). This includes data backup management, ensuring that critical data is backed up regularly and can be restored quickly in the event of a system failure or disaster.
- Offsite backups, cloud backups, and other redundancy mechanisms shall be put in place to safeguard against data loss and ensure business continuity in case of hardware failure

28.5.3.5 Capacity Management and Performance Optimization:

- The Service Provider shall be responsible for monitoring the resource utilization (CPU, memory, disk, network bandwidth) for both hardware and software components and providing recommendations for future scaling based on performance metrics and growth projections.
- Performance optimization shall include regular assessments of hardware usage, identification of bottlenecks, and the provision of solutions to ensure the hardware can meet the evolving demands of CDNS.

28.5.3.6 Lifecycle Management and Infrastructure Replacement:

- As part of lifecycle management, the Service Provider shall be responsible for ensuring that all hardware and software components are backed by OEM warranties (if applicable) for up to three years from the date of contract award/provisioning, and that OEM support is available for the entire contract duration.
- The Service Provider shall maintain an inventory of spare parts and critical hardware components to facilitate immediate replacements if necessary.

28.5.3.7 Security Monitoring and Incident Response:

- The Service Provider will be responsible for implementing security monitoring at the hardware and software level, ensuring compliance with security protocols, and responding swiftly to any security breaches or vulnerabilities that may arise.
- The Service Provider shall work in close collaboration with CDNS's security team to enforce physical and logical security controls, ensuring the integrity of both data and infrastructure.

28.5.3.8 Backup, Archiving, and On-Site High Availability

- All backups, archival storage, and on-site high availability (HA) for the CBA database and related systems shall continue to be supported using CDNS's existing enterprise storage infrastructure, including but not limited to:
 - HPE 3PAR Storage
 - HPE MSL / Tape Library infrastructure
- The selected Service Provider shall be responsible for configuration, integration, and operational management of backups and recovery processes.

28.5.3.9 Rack and Linkage Charges

CDNS shall be responsible for arranging and bearing all costs related to rack space, power, cooling, and data center facilities at both the Primary (PR) and Disaster Recovery (DR) sites. CDNS shall also arrange and cover all PR–DR linkage and connectivity charges required for replication, backup, and disaster recovery operations. The Service Provider shall specify the required network bandwidth, latency, and Quality of Service (QoS) for the infrastructure, and CDNS will be responsible for arranging and ensuring the provision of the specified network capabilities.

28.5.3.10 Dependency and Risk Clarification

Any deviation in actual storage consumption or system behavior arising due to:

- Regulatory retention requirements
- Business-driven data growth
- Additional modules or integrations introduced during the contract term

shall be addressed through the Change Request (CR) mechanism in accordance with the terms of the agreement.

28.5.4 Current System Utilization and Capacity Baseline (Indicative)

For the purpose of transparency and to enable the Service Provider to assess the scale and complexity of the environment, CDNS had shared indicative information on the current compute and storage utilization of the Core Business Application (CBA) ecosystem in the Tender Documents.

This information was shared for reference only and shall not be construed as a prescriptive or restrictive requirement on the proposed hardware architecture.

28.5.5 Hardware Sizing Responsibility and Flexibility

The Service Provider shall retain full autonomy to propose appropriate hardware and software architectures, sizing models, and deployment approaches.

Any shortcomings arising from inaccurate sizing by the Service Provider, which impact the transition, takeover, and migration of the Core Business Application (CBA) to the proposed infrastructure, will be the sole responsibility of the Service Provider. The Service Provider will bear the cost of any corrective actions required to meet CDNS's operational and performance expectations.

The Service Provider must also calculate the maximum storage, RAM, compute, and software requirements based on the current transaction and user trends, as well as the projected growth trends provided by CDNS.

The Service Provider shall ensure that the proposed solution meets or exceeds the hardware and software specifications detailed for both the Primary (PR) and Disaster Recovery (DR) sites, while also allowing for scalability and performance in line with CDNS's expected growth. The Service Provider is responsible for replicating the same specifications for the DR site to maintain identical performance, scalability, and reliability across both locations. Furthermore, DR drills shall span over 1 one week to ensure reliability of the Disaster recovery site.

28.5.6 Duplication of Penalties

If a service disruption occurs due to a single root cause (for example, Infrastructure as a Service failure), no separate penalties shall be applied for other services impacted due to the same issue. The penalty, if applicable, will be considered only once for the actual cause of the disruption.

28.6 Annexure A-6 Integration with Licensed Bill Aggregators

28.6.1 Purpose

The Service Provider shall design, develop, implement, and deploy new functional modules within the Core Business Application (CBA) of CDNS to enable integration with licensed Bill Aggregators operating in Pakistan.

The integration shall facilitate secure and seamless bill presentment, payment processing, confirmation, settlement, reconciliation, and reporting for multiple service categories including,

but not limited to, utilities, telecommunications, government payments, and educational institutions.

28.6.2 Objectives

The Service Provider shall ensure that the developed solution:

- a) Enables real-time bill inquiry (bill fetch) and payment processing through CDNS branch counters.
- b) Integrates the CBA with authorized and SBP-approved Bill Aggregators, including but not limited to 1LINK and other licensed entities.
- c) Enhances operational efficiency through automated settlement and reconciliation mechanisms.
- d) Ensures secure, compliant, auditable, and high-availability transaction processing.
- e) Provides comprehensive reporting and monitoring capabilities for Operations and Finance functions.

28.6.3 Scope of Work

A. System Integration

The Service Provider shall:

- i. Design, develop, configure, test, and implement secure API-based integration between the CBA and selected licensed Bill Aggregators.
- ii. Implement end-to-end transaction workflows covering:
 - Real-time bill inquiry (bill fetch);
 - Payment authorization and posting;
 - Transaction confirmation and receipt generation;
 - Transaction reversal and dispute handling (where applicable).
- iii. Ensure compatibility with the technical, messaging, and security standards prescribed by the respective aggregator(s).
- iv. Implement encryption, digital signatures, and secure communication protocols as required by regulatory and aggregator standards.
- v. Conduct System Integration Testing (SIT), User Acceptance Testing (UAT), and performance testing prior to production deployment

B. Channel Enablement

The Service Provider shall:

- i. Enable bill payment functionality at branch counters through the CBA interface.
- ii. Extend bill payment capability to other designated delivery channels, including but not limited to mobile application and internet banking platforms, where applicable. Ensure consistent transaction validation, limits management, and customer confirmation processes across all enabled channels.
- iii. Implement appropriate maker-checker controls and role-based access mechanisms.

C. Settlement & Reconciliation

The Service Provider shall:

- i. Configure and implement automated settlement processes in accordance with agreed settlement cycles and arrangements with the respective Bill Aggregator(s).
- ii. Implement automated reconciliation mechanisms to ensure transaction-level matching between CDNS records and aggregator reports.
- iii. Provide exception handling workflows for unmatched, failed, reversed, or disputed transactions.
- iv. Generate daily, weekly, and monthly MIS reports for Finance and Operations, including but not limited to:
 - Transaction summaries;
 - Settlement statements;
 - Reconciliation status reports;
 - Exception and aging reports.
- v. Ensure that all reports are exportable in standard formats and are available for audit and regulatory review.

D. Compliance, Security & Audit

The Service Provider shall:

- i. Ensure compliance with relevant industry standards.
- ii. Implement end-to-end audit trails, transaction logging, and system activity logs.
- iii. Provide necessary documentation, logs, and system access required for internal, external, and regulatory audits.

28.6.4 Aggregator Integration Scope

The following table summarizes the licensed Bill Aggregators included within this scope:

Bill Aggregator
NADRA e-SAHULAT
1Bill

28.6.5 Assumptions & Exclusions

The following assumptions underpin this scope:

- CDNS shall obtain the necessary bilateral agreements and API credentials with NADRA e-SAHULAT, and 1Bill, prior to integration commencement.
- Aggregator testing environments will be made available by the aggregators.
- Any biller onboarding beyond the two named aggregators is outside the current scope and will be handled as a change request.

29 ANNEXURE B – COMMERCIALS AND PAYMENT TERMS

29.1 Table: B.1					
S. No	Activity	Base Year-1 Cost (PKR) Exclusive of Taxes	Applicable Tax in PKR*	Year-1 Cost (PKR) Inclusive of Taxes	Fixed Annual Escalation (%)
29.1.1 Group I – Core Business Application					
1	Cost for Application Takeover and Transition-In of the existing Core Business Application (CBA) on an <As-Is-Where-Is basis,	PKR 14,285,714.29	PKR 714,285.71	PKR 15,000,000 For Detailed Bifurcation of Cost see table B.2	N/A
2	Integration with Licensed Bill Aggregators (Mention One-time development cost inc. all applicable taxes in PKR)				N/A
3	End-to-end support, maintenance, and management of the CBA, its data replication, database administration, middleware and stack components, performance optimization, security hardening, technical updates, bug-fixes etc., including switch over and fall back of the CBA and its database as part of routing DR Drills as Managed services i.e AMC on Turnkey Management and Implementation Model	PKR 84,300,000	PKR 4,215,000	PKR 88,515,000	15%
4	Enhancement/Customization in the existing <CBA of CDNS= to meet current and ongoing business and technical requirements of CDNS (Mention Cost in terms of Man Day)	PKR 114,285.71	PKR 5,714.29	PKR 120,000 As per Table B.3 (Sr.# 1)	10%
29.1.2 Group II – IaaS					
5	Cost for the provisioning of required Hardware Infrastructure as a Service (IaaS) for the Core Business Application (CBA) and associated systems, including servers, storage, networking equipment and related software.	PKR 77,275,001.90	PKR 3,863,750.10	PKR 81,138,752 For detailed bifurcation of cost, please see table B.4.1	0%

6	Cost for the provisioning of required Software Infrastructure as a Service (IaaS) for the Core Business Application (CBA) and associated systems, including servers, storage, networking equipment and related software	PKR 80,436,251.43	PKR 4,021,812.57	PKR 84,458,064 <i>For detailed bifurcation of cost, please see Table B.4.2</i>	0%
29.1.3 Group III – Managed Services					
7	Cost for the management of the existing hardware and the provided infrastructure as a service (IaaS) as a managed service including maintenance, monitoring, support, installation, configuration C patch management over the contract period.	PKR 50,580,000	PKR 2,529,000	PKR 53,109,000 <i>For detailed bifurcation of cost, please see table B.5</i>	15%

29.2 Table: B.2

Sr. No	Activity	Base Year-1 Cost (PKR) Exclusive of Taxes	Applicable Tax in PKR*	Year-1 Cost (PKR) Inclusive of Taxes	Label	Fixed Annual Escalation (%)
<u>01</u>	One Time Cost for Application Takeover and Transition-In of the existing Core Business Application (CBA) on an <As-Is-Where-Is= basis	PKR 0.00	PKR 0.00	PKR 0.00	<u>Cos t-A</u>	<u>Not Applicable</u>
<u>02</u>	One Time Cost for Integration with Licensed Bill Aggregators (Mention One-time development cost inc. all applicable taxes in PKR) (Conditions) i. Annual Maintenance Cost for this module shall be applicable as per the percentage quoted in Table B.3. ii. SLA for this module shall be applicable as per details mentioned in Section 9.7 of this RFP	PKR 14,285,714.29	PKR 714,285.71	PKR 15,000,000	<u>Cos tB</u>	<u>Not Applicable</u>

03	Yearly Cost for End-to-end support, maintenance, and management of the CBA, its database administration, data replication, middleware and stack components, performance optimization, security hardening , technical updates, bug- fixes etc., including switch over and fall back of the CBA and its database as part of routing DR Drills as Managed services i.e AMC	PKR 84,300,000	PKR 4,215,000	PKR 88,515,000	<u>Cost C</u>	<u>15.00% (R1)</u>
-----------	--	-----------------------	----------------------	-----------------------	----------------------	---------------------------

29.3 Table: B.3*****

S. No	Description	Base Year-1 Cost (PKR) Exclusive of Taxes	Applicable Tax in PKR	Year-1 Cost (PKR) Inclusive of Taxes	Label
1	Man-Day Cost (PKR)	PKR 114,285.71	PKR 5,714.29	PKR 120,000	CostD
2	AMC (% of development cost)	18.00%			
3	Fixed Annual Escalation on Man-Day Rates	10%			R2

29.4 Table: B.4.1

Sr. No	Activity	Base Year-1 Cost (PKR) Exclusive of Taxes	Applicable Tax in PKR*	Year-1 Cost (PKR) Inclusive of Taxes	Label	Fixed Annual Escalatio n (%) (R3)
01	Yearly Cost for the provisioning of Hardware Infrastructure As A Service required for the Core Business Application (CBA) and associated systems, including servers, storage, networking equipment, etc.	PKR 77,275,001.90	PKR 3,863,750.10	PKR 81,138,752	Cost E	0.00%

29.5 Table: B.4.2

Sr. No	Activity	Base Year-1 Cost (PKR) Exclusive of Taxes	Applicable Tax in PKR*	Year-1 Cost (PKR) Inclusive of Taxes	Label	Fixed Annual Escalati on (%) (R4)
01	Yearly Cost for provisioning of Software Infrastructure as A Service for software required for the CBA infrastructure and associated systems, including OS, network monitoring, security tools, vulnerability management, and virtualization software.	PKR 80,436,251.43	PKR 4,021,812.57	PKR 84,458,064	Cost F	0.00%

29.6 Table:B.5

Sr. No	Activity	Base Year-1 Cost (PKR) Exclusive of Taxes	Applicable Tax in PKR*	Year-1 Cost (PKR) Inclusive of Taxes	Label	Fixed Annual Escalation (%) (R5)
01	Cost for the management of the existing hardware and the provided infrastructure as a service (IaaS) as a managed service including maintenance, monitoring, support, installation, configuration C patch management over the contract period.	PKR 50,580,000	PKR 2,529,000	PKR 53,109,000	Cost G	15.00%

* **Note:** The applicable tax rate mentioned in table B.1 is the currently prevailing and applicable tax rate of 5% under Islamabad Capital Territory Sales Tax on Services Ordinance 2001.

29.7 Terms and Conditions as per Bidding Documents for Change Requests and Enhancements

- *Warranty period will be applicable as mutually agreed in the agreement after the Development of New Module/Capabilities shall be treated under Warranty Period and AMC will start after the completion of warranty period and shall be applicable till the currency of agreement. If during warranty period a defect is identified or due to deployment some other module has defect, of the severity level 3 as defined in Clause 30.5.6, then warranty period will restart.
- **Man-Day Rates (in PKR) inclusive of all Applicable taxes for further enhancements in the application for future business requirements
- *** Resources/personnel for quotation of Man Day Rates shall be considered in accordance with the scope of indicative development
- ***** The Annual Maintenance Charges (AMC) quoted for the development of New Modules/Capabilities (Table B.3) shall be the applicable percentage of the development cost incurred, calculated on the basis of man-day rates table B.3.

29.8 Paysys Labs Terms and Conditions

29.8.1 Core Business Application – Payment Terms

1. Paysys Labs is pleased to waive the costs of Application Takeover and Transition-In of the existing Core Business Application as mentioned in Table B.2, S# 1.
2. The cost for Integration with Licensed Bill Aggregators (S# 2 of Table B.2) shall be invoiced based on the following milestones:
 - a. 15% upon initiation of the project and submission of Scope of work (including process flows, descriptions, and details of the development and its impact), Project Plan, any 3rd Party Dependencies, tools, or services required,
 - b. 70% upon UAT with first bill aggregator
 - c. 15% upon delivery/go-live with first bill aggregator.
 - d. The cost given is contingent on the proposed scope of work in Annexure A-6 of this agreement, which limits integration to the following bill aggregators:
 - i. NADRA
 - ii. 1Link

- e. Any additional integrations shall be charged to CDNS based on man-day rates provided in Table B.3 S# 1.

The Annual Maintenance Cost shall be invoiced in equal monthly installments after go-live and the completion of warranty period.

- 3. The yearly cost for End-to-end support, maintenance, and management of the CBA, as provided in S# 03 of Table B.2, shall be invoiced monthly in arrears in twelve equal invoices, commencing from the date of CDNS's acceptance of the Transition-In phase, which acceptance shall be based on the successful completion and handover of the required documentation. The training of CDNS resources and knowledge transfer (KT) may be completed after such acceptance and shall not be construed as a condition precedent to, or a blocker for, the commencement of invoicing and payment.
 - a. The cost shall be increased after each contract year based on the fixed annual escalation rate provided in S# 03 of Table B.2.

29.8.2 IaaS Payment Terms

- 1) The Yearly Costs for the Provisioning of Hardware Infrastructure as a Service and Software Infrastructure as a Service as provided in Tables B.4.1 and B.4.2 shall be invoiced based on the following terms:
 - a. The annual cost shall be divided into equal monthly installments and invoiced monthly in arrears starting from the date of Infrastructure commissioning for the whole year extendable yearly upon satisfactory performance upto 5 Years.
 - b. Any change in the proposed hardware or software arising due to changes in business requirements, increased business activity, or requirements exceeding the originally proposed capacity shall be managed through a mutually agreed Change Request (CR) process. The cost of any additional hardware and/or software required as a result of such change shall be charged to CDNS accordingly as per section 3.3.1.11 of the bidding documents.
 - c. Both parties agree that where applicable the infrastructure will be depreciated at the rate of 20% annually during the term of the agreement as mentioned in clause 2.

29.8.3 Managed Services Payment Terms

- 1. The Yearly Costs for the Provisioning of Cost for the management of the existing hardware and the provided infrastructure as a service as provided in Table B.5 shall be invoiced based on the following terms:
 - a. The annual cost shall be divided into equal monthly installments and invoiced in arrears at the end of each month.
 - b. The billing period for the first contract year shall initiate from the date of project award or contract signing.
 - c. The cost shall be increased after each contract year based on the fixed annual escalation rate provided in Table B.5.

29.8.4 General Terms and Conditions

- 1. All prices are in PKR and inclusive of the applicable tax rate described after Table B.1 of this annexure B.

2. Whereas the parties hereby agree that clause 7, Charges and Payment, of this agreement shall govern the invoicing and payment structure of this agreement.

3. Whereas, pursuant to clause E 1 (Change in Applicable Law) of the General Conditions of Contract of the tender documents, any changes in the applicable taxes or duties, or the applicability or interpretation of them thereof, then the commercials payable to Paysys Labs under this Contract shall be increased or decreased accordingly by agreement between the Parties.

30 ANNEXURE C – CORE BUSINESS APPLICATION SERVICE LEVEL AGREEMENT (SLA)

30.1 Purpose and Applicability

This Service Level Agreement (SLA) establishes measurable, enforceable, auditable, and financially traceable service performance standards applicable to all services delivered under this RFP, including but not limited to:

- a) Application Takeover and Transition-In of the Core Business Application (CBA)
- b) Managed Services / Annual Maintenance (AMC) of the CBA
- c) Enhancements, Customizations, and Change Requests (CRs) executed on a Man-Day basis
- d) Infrastructure as a Service (IaaS) provisioning (hardware and software)
- e) Managed Services of Infrastructure, including existing hardware and Service Provider-provided IaaS
- f) Disaster Recovery, Business Continuity, Security, and Integration Services

The SLA framework is financially mapped to [Annexure B Commercial and Payment Terms](#), and Annexures [A1 CBA Application Takeover and Transition-In](#), [A2 Change Management & CBA Enhancement Policy](#), [A3 CBA Annual Maintenance and Support](#), & [A5 Infrastructure Managed Services](#)

30.2 SLA Governance, Measurement and Reporting

1. SLA compliance shall be monitored continuously and assessed monthly.
2. CDNS and the Service Provider shall jointly be responsible for SLA interpretation.
3. SLA performance shall be monitored and validated by CDNS. The Service Provider shall provide all necessary logs, reports i.e the Service Provider shall provide automated APM & monitoring tools, dashboards, logs, replication health and other related reports required for SLA validation.
4. The Service Provider shall submit monthly SLA compliance reports within five (05) working days after the month-end.
5. Penalties shall be deducted from the invoice corresponding to the affected financial component Development-phase SLAs and AMC-phase SLAs shall be measured independently.
6. SLA breaches in the Transition-In Phase shall be measured and penalized separately.
7. The Service Provider shall be responsible for designating an accountable service manager, along with a defined [escalation matrix \(see clause 30.7 below\)](#)

CDNS will be responsible for providing the rack space, internet connectivity, bandwidth, network, and all associated components required to ensure proper operation of the infrastructure in the NTC Data Center.

30.3 Maintenance & Support

Paysys has a full-fledged dedicated professional team for its valuable customers providing instant support calls. This section of the document will provide details of the Technical Support Department function relating to the following:

Ongoing support as a part of implementation

- Receiving and logging customer calls related to maintenance.
- Prioritizing and categorizing calls

- Assignment of calls to customer support engineers and/or developers
- Procedure for call-fixes and minor enhancements.
- Procedure for call evaluation and classification
- Procedure for call closure.

Technical Support Department Responsibilities

The Technical Support Department handles all customer support calls and is responsible for the life- cycle management of customer calls. A detailed ticketing system (JIRA) is available that provides the customers with a clear picture of the call being supported. The team is equipped with all the necessary tools to support calls from the customers.

30.4 Call Logging Procedure

Technical calls may be received in various forms including but not limited to:

- Support Ticket logging by customer on JIRA
- Support Ticket logging by customer on email
- Direct phone call by the customer
- Email by the customer
- WhatsApp or text message from the customer

The Service Provider's operations team logs the call in JIRA with all relevant details and informs the customer through email. An email is instantly shared with the customer about the call. The Service Provider's operations team shall not unreasonably delay or deny to initiate a ticket on the customers behalf in cases where the customer logs a technical call via email, phone, or WhatsApp, especially during non-working hours or days.

30.5 High level Support Arrangement Coverage

30.5.1 Incident Management:

Restoration of services in as short a time as possible. Assist troubleshooting in the event of an unplanned interruption of a customer-facing production service.

30.5.2 Problem Management:

Troubleshooting a specific problem during a development phase.

30.5.3 Delivery of Resolution:

In the form of workarounds, hotfixes, and maintenance releases. Facilitate forwarding new feature requests and provide feedback to the Development Team.

30.5.4 Training

Providing manual demos, tutorial, release notes and other relevant information to the customer for a new change or feature.

30.5.5 Support Mechanism

S.no	Descriptin	Response
1.	Remote resources support	Available
2.	Availability of resources	24/7
3.	Hour’s resolution time for Severity 1	3 hours
4.	Hour’s resolution time for Severity 2	24 hours
5.	Hour’s resolution time for Severity 3	120 hours
6	Hour’s resolution time for Severity 4	240 working hours
7.	Support call tracking	Available
8.	Availability on Phone	Available
9.	Hotfixes	Available
10.	No of support request per year	Unlimited
11.	No of Technical contacts for a customer (at any time)	1+1

Support Team: Paysys Labs support team is a dedicated unit for our customers. Each member of the team is a subject matter expert, specialized in either Back-end or Front-end technologies.

If an issue was reported over the telephone, the customer should send a written error description via email. For issues that the customer perceives to be a Level 4 or Level 3 (Please refer to clause below: 30.5.6 Severity Level with Corrective Action), the customer should follow any initial report sent by email or by phone call.

Regular daytime office and contact information is listed below:

Location: Karachi, Pakistan

Business Hours (local time): 9:00am - 6:00 pm

Email address: support@paysyslabs.com

30.5.6 Severity Level with Corrective Action

Severity Level Definitions

The Parties have mutually agreed on four severity levels for the classification of incidents, faults, and service requests under this Agreement. Each incident shall be classified according to the definitions below, which shall govern the applicable response times, resolution timelines, and penalties. The examples provided under each level are illustrative and not exhaustive; where an incident does not clearly fall within a single level, the Parties shall classify it in good faith by

reference to its operational and financial impact, and in particular to the guiding principle of each level set out below.

Level 4 — Emergency

Definition. A Level 4 (Emergency) incident is one in which the entire Core Business Application (CBA), or a significant portion of it, is unavailable, inoperable, or otherwise non-functional, such that core banking operations cannot be carried out. This level applies where multiple core services, or an entire delivery channel, are simultaneously affected, or where a majority of transaction volume is disrupted. Business operations are halted or critically impaired across the institution or across a whole channel, with immediate and widespread impact on customers and operations.



Illustrative examples.

- Complete stoppage of all CMS / ATM transactions;
- Failure or unavailability of the RAAST service;
- An entire delivery channel becoming inoperable, such as digital banking, cards, or branch operations;
- All branches being unable to process transactions;
- Failure of multiple core services occurring simultaneously.

Level 3 — Critical

Definition. A Level 3 (Critical) incident is one in which a single service or a major function of the CBA is down or non-functional, directly impacting customers' ability to make payments, receive funds, or access a key banking service, while the wider CBA and other channels continue to operate. A distinct, customer-facing service or major function is unavailable, but the disruption is confined to that service or function and does not extend across an entire channel or the wider application.



Illustrative examples.

- Branch teller payment function being unavailable;
- A single customer-facing service being down such that customers cannot make or receive a payment through that service;
- Failure of an individual service that directly affects customers' ability to transact, without affecting the wider CBA.

Level 2 — Major

Definition. A Level 2 (Major) incident is one in which core transaction processing continues to operate normally, but a specific downstream, supporting, or ancillary function is not working correctly. Such an incident carries a minor risk for so long as the affected function remains unresolved; however, upon identification and implementation of the resolution, the affected function and any associated pending items can be completed or reprocessed in full, such that the risk is resolved without any resulting financial impact. Live transactions continue to be processed and customers are able to transact, but a supporting function has failed. The risk is recoverable — once fixed, the backlog can be cleared and no permanent financial loss arises.

Illustrative examples.

- The reconciliation process not working;
- RAAST batch processing failing or not completing;
- Profit accruals not being calculated or posted;
- Payouts not being processed, while underlying transactions continue to be recorded;
- Any supporting or downstream function failing while core transaction processing remains operational.

Level 1 — Minor / Routine

Definition. A Level 1 (Minor / Routine) incident is a routine request or a minor defect that does not affect application performance, does not cause downtime, and does not impair customers' ability to transact. Such items can be managed operationally by both Parties in the ordinary course. No impact on availability, performance, or customer transactions; the item is administrative or cosmetic in nature and can be handled through normal operational channels.

Illustrative examples.

- Routine service requests or queries;
- Minor bugs that do not affect application performance or availability;
- Cosmetic or non-functional defects;
- Requests that can be scheduled and managed operationally without urgency.
- Ad-hoc data, stats or any reporting requests other than already agreed reports.

Severity	Description	Response Time	Correction	Target
----------	-------------	---------------	------------	--------

			Process	Resolution
Level 4 Emergency	Level 4 / Emergency — complete unavailability or high financial-loss risk, whether from a failed application module (existing or newly developed through CR), a database/middleware/batch/integration failure, or any hardware/software/network/data-center issue up to a full PR/DR failure.	A support person to contact the customer up to 10 min of receipt of the problem.	Level 4 issues are the most urgent and require immediate attention. Appropriate Paysys management will be notified immediately. Status is reported every 30 minutes. Paysys will continue to work on the problem until it is solved, and the system is functional.	Target resolution in less than 03 hours. Paysys employees will continue to work on Level 4 issues 24 hours a day, 07 days a week until they are resolved.
Level 3 Critical	Services are up and running for customers, but fault tolerance is compromised e.g., Redundant hardware is not working OR 1 network link is down or a certain CBA module is underperforming. Services are degraded for some customers due to infrastructure issue	A support person to contact Customer within one business hour of receipt of the problem.	Paysys will update the Customer with the progress toward the resolution within 1 hour of receipt of the issue. Status is reported every 12 hours. If not delivered in 2 business days, the issue is escalated to a Level 4. After contacting the Customer, appropriate Paysys management is notified, and additional resources are assigned.	Target resolution is less than 01 business day.

Level 2 Major	An important function or process has an error, but the system is functioning. There is a small financial risk, but the issue can be identified and mitigate the risk through operational procedures.	A support person to acknowledge the issue to the Customer within 2 business hours of notification of the issue.	The CSR and the Customer will determine a process to ensure that all proper data and information will be provided to Paysys. Status is reported every 02 days. If a solution is not delivered in 05 days, the issue is escalated to a Level 3. After contacting the Customer, appropriate Paysys management is notified, and additional resources are assigned.	Target resolution is less than 03 business days.
Level 1 Minor	A function or process has an error but exposes the Customer to no financial risk. All minor faults or cosmetic problems. Most support calls are classified as Level 1.	A support person to acknowledge the issue to the Customer within 01 business day of notification of the issue.	Appropriate support staff will be assigned to the issue within 24 hours after all necessary information is received from the Customer or otherwise collected by CSR. Status is reported monthly. If solution is not delivered in 10 days, the issue is escalated to a Level 2.	Target resolution is less than 7 business days.

JIRA is a tool for bug tracking and issue tracking. By using JIRA online service our clients will be able to log all the software related complaints on the URL given below and track them down till its complete resolution.

The severity level of an issue is assigned using a combination of the judgment of the CSR, the Customer's input, and the guidelines below. The severity level is the basis for prioritization of problems and the allocation of resources toward the resolution of those problems.

30.5.7 Level 4 Emergency Problem

- Level 4 Problems are the most urgent and indicate severe action is required. This is generally defined as a Paysys application is completely out of service or there is a high risk of financial loss because of the Paysys application being down. Paysys believes an emergency is one best determined by the Customer. Declaring a problem to be an emergency automatically escalates the problem to Severity Level 4.
- The Customer should inform the CSR answering the call that this is an emergency. If all CSRs are unavailable, a manager will be located who will act on the call and ensure that the call is responded promptly.

30.5.7.1 Corrective Process

- CSR will take immediate action to resolve the issue and maintain communication with the client. Paysys will continue working until the system is operational. A Status Report will be provided every 30 minutes.

30.5.7.1.1 JIRA reporting mechanism

- Our clients can report support tickets and issues via their designated JIRA ID. Paysys Labs shall ensure to provide the customer with detailed reports and logs of support tickets raised during the contract period.

30.5.8 Level 3 Critical Problems

The following types of situations will be reported as a Level 3 problem:

- An important function or process has an error, but the system is functioning. There is a high risk of financial loss because of the problem, but the Customer can identify and mitigate the risk through operational means.
- Customer problems cannot be resolved in an acceptable time frame through Level 2 support.
- The scheduled completion date communicated in the Level 2 process has been missed.

30.5.8.1 Corrective Process

The CSR and Customer resources will determine the information required to adequately document the problem. The estimated resolution time will be communicated within 1 hour. CSR will inform the Customer about the root cause of the problem as identified at that moment as well as the next steps towards the resolution. Typical resolution turnaround is targeted to be 1 day or less. The CSR will update the Customer with the status and progress leading to resolution every 12 hours. The CSR will notify the CSM who will review the situation and the plan to determine if additional intervention is required to resolve the problem.

30.5.9 Level 2 Major Problem

The following types of situations will be reported as a Level 2 problem.

- An important function or process has an error, but the system is functioning. There is a small financial risk, but the Customer can identify and mitigate the risk through operational means.
- Customer problems cannot be resolved in an acceptable time frame through Level 1 support.
- The scheduled completion date communicated in the Level 1 process has been missed.

30.5.9.1 Corrective Process

The CSR and Customer resources will determine the information required to adequately document the problem. The estimated resolution time will be communicated within 2 business hours after the required documentation is received from the Customer. CSR will inform the Customer about the root cause of the problem as identified at that moment as well as the next steps towards the resolution. Typical resolution turnaround is targeted to be 3 days or less. The CSR will periodically communicate with the Customer as to status and progress leading to resolution. As appropriate, the CSR will notify the CSM who will review the situation and the plan to determine if additional intervention is required to resolve the problem.

30.5.10 Level 1 Minor Problem

A Level 1 problem is defined as one in which an important function or process has an error, but the system is functioning. The problem exposes the Customer no risk of financial loss. Most of the “Standard Support” types of calls will also be classified with severity Level 1. All minor impact on the system, cosmetics errors or individual cardholder complaints or LOG review request will be classified under this category.

30.5.10.1 *Corrective Process*

The CSR and Customer Resources will determine the information required to adequately document the problem. The estimated resolution period will be communicated within two days after the required documentation is received from the Customer. CSR will inform the Customer about the root cause of the problem as identified at that moment as well as the next steps towards the resolution. Typical resolution turnaround is targeted to be 7 days or less. The CSR will periodically (monthly) communicate with the Customer (only to the designated personnel) as to status and progress leading to resolution.

30.6 Threat and Vulnerability Management

1. Pursuant to Clause 28.3.2.3 (Security Hardening and Compliance) of Annexure A-3, Clause 28.4.3 of Annexure A-4, Clause 28.5.3 of Annexure A-5, and Clause 30.1 of Annexure C, the Service Provider hereby agrees to maintain a risk-based Threat and Vulnerability Management (TVM) program aligned with ISO 27001 standards. The TVM program shall include authenticated scanning, patch and configuration management, a risk-acceptance workflow, and exceptions tracking.
2. The Service Provider shall provide, for all in-scope applications and modules, quarterly vulnerability assessments (VA) and penetration testing (PT) twice a year. Additionally, VA shall be carried out for all newly developed and deployed modules under the Change Request mechanism.
3. Paysys shall share an executive summary and detailed findings relevant to CDNS's in-scope environment via a secure channel, following report validation with CDNS's relevant departments. Paysys shall target to share the report within fifteen (15) business days.
4. Paysys shall classify vulnerabilities by risk category (e.g., Critical, High, Medium, Low) and shall meet the following remediation targets, measured in calendar days, on a risk basis:
 - a) Critical (internet-facing / exploitable): mitigate within ten (10) days; patch to be deployed within fifteen (15) days where available.
 - b) Critical (internal): remediate within fifteen (15) days.
 - c) High: remediate within thirty (30) days.
 - d) Medium: remediate within forty-five (45) days.
 - e) Low: remediate within sixty (60) days.
5. Any patches available from the Software OEMs for Critical vulnerabilities shall be applied within a minimum of twenty-four (24) hours and maximum of seventy-two (72) hours. Where patches are unavailable, Paysys shall implement compensating controls.

6. CDNS shall have the right to allow its third-party vendors to conduct security audits, testing, and VAPT on the in-scope environment, on both a periodic and ad-hoc basis, subject to providing the Service Provider with reasonable prior notice of any such activity.

30.7 Service Level Commitments

Item	Minimum Service Level
Service Uptime	99.5 %
Service Credit Arrangement	Available

30.8 Escalation Matrix

Level 1 Minor:	Customers can report general issues via email: operations@paysyslabs.com
Level 2 Major:	CBA – Hussain Jaffer Ali - hussain.ali@paysyslabs.com Raast - Muhammad Alishan: muhammad.ali@paysyslabs.com
Level 3 Critical:	Head of Operations – Tariq Dedhi: tariqdhedhi@paysyslabs.com
Level 4 Emergency:	Chief Technology Officer – Azeem Yaseen: azeem.yaseen@paysyslabs.com

30.9 SLA Penalty Framework

30.9.1 Penalty Attribution Principle

Penalties shall be applied strictly against the financial component associated with the breached service.

No Duplication of Penalties. Where a single incident, downtime event, or root cause could give rise to a penalty or service credit under more than one SLA head in this Annexure, the penalty shall be assessed once only, against the financial component of the Service Tower to which the root cause of the event is attributed in accordance with Clause 30.9.1. No single event shall attract penalties under more than one SLA head, nor be applied against the financial component of a Service Tower that is not the root cause of the breach.

Service Tower	Reference from Annexure B Commercials and Payment Terms
Application Takeover & Transition-In	Tagged to Table B.2 S# 1
Application AMC	Tagged to Table B.2 S# 3
Enhancements / CR	Tagged to Table B.3
IaaS Provisioning (Hardware and Software)	Tagged to Tables B.4.1 and B.4.2
Infrastructure Managed Services	Tagged to Table B.5

30.9.2 Application Takeover & Transition-In SLAs

(Mapped to Table B.2 S# 1)

SLA Parameter	Target	Frequency	Penalty	Penalty Cap	Chronic Non-Performance
Transition Completion	≤ 6 Months	Weekly	0.5% of Year-1 cost per week of delay	10% of the cost quoted in Table B2 Year 1	Transition delay exceeds 20 weeks

30.9.3 Uptime SLA and Matrix

Mapped to B.2 S# 3 and Table B.4.1 and B.4.2

CDNS and the Service Provider agree to a defined 99.5% Uptime SLA for the CDNS CBA and Infrastructure as a service with defined maintenance exclusions, penalty matrices and capped service credits.

The Service Provider shall be responsible for ensuring a minimum of 99.5% as monthly Application and Infrastructure Uptime.

Tolerance Level [a]	Total Available Hours [b = 24 x 30]	Uptime Hours [c = a x b]	Downtime Hours [d = b - c]
99.5%	720	716	Up to 3.6 hours

Upon failure to meet this obligation, CDNS shall have the right to claim a monthly service credit, on monthly fees and charges received by the Service Provider as per the following table:

Tolerance Level [a]	Total Available Hours [b=24x30]	Uptime Hours [c=axb]	Downtime Hours [d=b-c]	Service Credit
99.5%	720	716.4	up to 3.6 hours	0% of Monthly Fee
95%-99.4%	720	684	up to 36 hours	5% of Monthly Fee
90%-94.99%	720	648	Up to 72 hours	10% of Monthly Fee

85%-89.99%	720	612	up to 108 hours	15% of Monthly Fee
80%-84.55%	720	576	up to 144 hours	20% of Monthly Fee

The penalties described above apply solely to the software application uptime for the Core Business Application (CBA) and the uptime of the provided hardware and software in Infrastructure as a Service where the provided infrastructure as a service causes downtime in the CBA. It is understood that this uptime is not related to factors outside of the selected Service Provider’s scope of work including, but not limited to, network issues, power outages, bandwidth fluctuations, or latency-related issues.

CDNS will be responsible for providing the rack space, internet connectivity, bandwidth, network, and all associated components required to ensure proper operation of the infrastructure in the NTC Data Center. Any downtime caused by network failures, power outages, bandwidth constraints, or external factors beyond the Service Provider’s control will not be considered as part of the uptime calculation for the application, and no penalties will be applied in relation to such outages. The above quoted figures and times are for a month of 30 days, and for clarity purposes only. The actual downtime for months comprising of 28, 29, 30 or 31 days will be calculated monthly as per the formula denoted above. Penalties shall be calculated Month-wise against the financial component of the Service Tower to which the downtime is attributed by root-cause analysis — i.e., the IaaS value (Tables B.4.1/B.4.2) where the downtime originates in the hardware/software infrastructure, or the CBA AMC value (Table B.2 S# 3,) where it originates in the application — and shall not be applied against the financial component of any Service Tower that is not the root cause. Where a single outage has causes spanning more than one tower, the penalty shall be applied only to the tower of primary root cause as jointly determined. The total penalties for any SLA breaches, as outlined, will be capped at 20% of the annual value of the respective tower.

Pre-scheduled downtime for maintenance activities will not be counted towards downtime. To minimize pre-scheduled downtime, traffic will be analyzed, and the activities will be done at low peak time.

Mapped to Table B.3

<i>SLA Parameter</i>	<i>Target</i>	<i>Penalty</i>
<i>CR Delivery Timeline</i>	<i>As per mutually approved project Plan</i>	<i>Penalty applicable only for Service Provider-attributable delays</i>
<i>Up to 10% delay in approved timeline</i>	<i>Allowed</i>	<i>No penalty</i>
<i>Delay between 10 and 30% of Approved Timeline</i>	<i>Not allowed</i>	<i>2.5% of total CR value</i>
<i>Delay beyond 30% and up to 50%</i>	<i>Not preferred</i>	<i>5% of total CR value</i>
<i>Delay beyond 50%</i>	<i>Not acceptable</i>	<i>Additional Penalty of 0.5x rate per MDs per day for exceeding 50% deviation</i>
<i>Documentation & Deliverables</i>	<i>Mandatory</i>	<i>1% of CR value if documentation and deliverables are not present at date of CR-Go live</i>

- *Total penalty for any individual CR shall not exceed 10% of the total approved CR value.*
- *A Man-Day represents one person-day of effort and shall not be construed as a calendar day or working day.*
- *The approved timeline (in calendar days) for any change request / project can differ from the total approved mandays for any project, given as how the Service Provider can align multiple resources to work simultaneously, or break tasks constituting a single manday's efforts over multiple days.*
- *Delays shall be calculated on a per calendar day basis, when the actual project duration exceeds the approved timelines.*
- *In case, during CR execution, it is determined that the originally approved Man-Day estimate is insufficient due to expanded scope, additional regulatory requirements, technical dependencies, or design changes, the Service Provider shall formally submit a Revised Effort & Impact Assessment for approval by CDNS.*
- *Upon approval, the revised Man-Days shall become the new baseline for SLA measurement.*
- *Penalties shall only be applicable for delays attributable to the Service Provider as per the Service Provider's defined responsibilities in the CR's scope work*

Example – CR Delay (between 10% and 30% of Approved Timeline)

Approved Change Request (CR) Details:

- *Approved Effort: 50 Man-Days*
- *Approved Rate: PKR 35,000 per Man-Day*
- *Total CR Value: PKR 1,750,000*

Actual Delivery Delay:

- *Delay: 8 Man-Days*
- *Delay Percentage: 16%*

Assessment:

- *Delay is within 20% of approved timeline*
- *As per SLA, delay up to 20% results in 2.5% of total CR value*

Penalty:

- *Penalty = 2.5% × 1,750,000*
- *Penalty = PKR 43,750*

Example – CR Delay (Penalty @ 5% of CR Value)

Approved Change Request (CR) Details:

- *Approved Effort: 50 Man-Days*
- *Approved Rate: PKR 35,000 per Man-Day*
- *Total CR Value: PKR 1,750,000*

Actual Delivery Delay:

- *Delay: 18 Man-Days*
- *Delay Percentage: 36%*

Assessment:

- *Delay exceeds 20% but is within 50%*
- *Penalty applicable at 5% of total CR value*

Penalty Calculation:

- *Penalty = 5% × 1,750,000*
- *Penalty = PKR 87,500*

Example – CR Delay (Penalty Beyond 50% Deviation)

Approved Change Request (CR) Details:

- *Approved Effort: 50 Man-Days*
- *Approved Rate: PKR 120,000 per Man-Day*
- *Total CR Value: PKR 6,000,000*

Actual Delivery Delay:

- *Delay: 30 Man-Days*
- *Delay Percentage: 60%*

Assessment:

- *Delay exceeds 50% of approved effort*
- *Penalty applicable only for delay exceeding 50%*

Penalty Calculation:

- *Delay beyond 50% = 5 Man-Days*
- *Penalty = $0.1 \times 120,000 \times 5 + 5\% \times 6,000,000$*
- *Penalty = 60,000 + 300,000*
- *Penalty = PKR 360,000*

30.9.5 AMC SLAs for Developed Modules

Mapped to Table B.3 AMC

Upon expiry of the warranty period, each developed module or capability shall transition into AMC, priced as a percentage of its respective development cost, as quoted in B.3

Scope of AMC for Developed Modules

- Availability and performance of developed Modules
 - Incident resolution and defect fixing
 - Compatibility with core CBA changes
 - Security patches and tuning
 - Ongoing documentation updates
- a) **SLA Metrics**
Any new modules developed during the course of the contract shall be subject to the same uptime and SLA metrics as the Core business application of CDNS, i.e., the penalty matrix defined above in section 30.9.3
- b) **Degradation Clause (Critical):**
If a module or enhancement that has been successfully delivered and accepted subsequently exhibits performance degradation, unavailability, or functional failure during AMC, such degradation shall be treated as an AMC SLA breach, not a development defect.
- c) **Penalty Applicability:**
Penalties shall be calculated against the AMC value derived from the percentage quoted in Table B.3, and not against the original development cost.

30.9.6 Managed Services SLA

Mapped to Table B.5

CDNS and Paysys Labs have mutually agreed on severity levels (Emergency, critical, Major, Minor), including clear definitions, response times, target resolution, correction, and intimation processes for each level in [section 30.5.6](#). Failure to meet the described resolution times shall result in the following penalties. Penalties have been mutually discussed and agreed between the Service Provider and CDNS and shall be capped to 10% of the total annual managed services value and applied only if service restoration has not been achieved within an agreed tolerance period.

S#	Severity Level	Resolution TAT	Penalty in case TAT is not met
1	Level 4 Emergency	Under 4 Hours	No Penalty as any emergency issue will result in CBA Downtime which will be penalized under 30.9.3
2	Level 3 Critical	Under 1 Business Day	5% of Annual Managed Services Cost*
3	Level 2 Major	Under 3 Business Day	3% of Annual Managed Services Cost*
4	Level 1 Minor	Under 7 Business Days	No Penalty

***Note:** Where an incident initially classified at severity level 2 is subsequently escalated to a severity level 3, and the resolution timelines for both levels are missed, the penalties applicable to each such level shall both apply cumulatively.

Where the nature of a reported issue, bug, or fault reasonably requires time beyond the agreed TATs in Section 30.5.6 — for example, where resolution depends on development work in the underlying module — Paysys Labs may request an extension of the applicable timeline from CDNS, supported by justifiable evidence. Any such extension shall be subject to CDNS's agreement, and penalties shall be applicable on the extended timeline.

30.9.6.1 Security & Compliance

CDNS and Paysys Labs have mutually agreed upon resolution timelines, in clause 30.6 of this agreement for vulnerability fixes based on severity levels (critical, high, medium, low), with flexibility to review and adjust timelines based on the nature of the vulnerability and dependencies on internal systems, external systems or third parties. The Service Provider shall work collaboratively with CDNS to resolve any audit concerns within a reasonable time frame, factoring in both Service Provider and CDNS responsibilities, and ensuring any audit logs are maintained for accountability and traceability. Both parties have defined the agreed-upon timelines for audit findings and resolution, with a joint escalation matrix in place to manage breaches, ensuring transparency and accountability for both parties.

30.9.6.2 Backup & DR

The Service Provider shall conduct periodic Disaster Recovery (DR) drills as per agreed schedule which would span over the period of at least 1 week twice a year and ensure real-time backup of

all critical systems. In case of failure to meet defined RTO/RPO parameters during DR drills, corrective measures shall be implemented within a mutually agreed remediation timeline.

Repeated failure to meet DR performance benchmarks may attract SLA penalties in accordance with the applicable SLA framework.

The Service Provider should also provide continuous, real-time backup and ensure full visibility of the backup status to CDNS. The Service Provider is required to maintain and demonstrate compliance with this backup protocol throughout the contract duration.

30.9.6.3 Capacity Management

The Service Provider shall remain fully responsible for infrastructure sizing and forecasting.

Any performance degradation caused by incorrect sizing based on the growth projections shared by CDNS shall be rectified at no additional cost to CDNS.

30.9.6.4 Hardware Lifecycle

As part of lifecycle management, the Service Provider shall be responsible for ensuring that all hardware and software components are backed by OEM warranties (if applicable) for up to three years from the date of contract award/provisioning, and that OEM support is available for the entire contract duration. The Service Provider will be responsible for diagnosing and resolving any hardware-related issues that arise, ensuring minimal downtime and business continuity. This includes handling hardware failures, replacing faulty components, and coordinating with hardware vendors for warranty support or component replacement.

In the event of a hardware or software failure, the Service Provider will be responsible for providing a quick resolution, including replacing faulty components and restoring full functionality in a timely manner.

30.9.6.5 Integration Availability

(NADRA, SBP, RAAST, 1Link etc.)

Any Integration failures will be described as an issue with a defined severity level. If the Service Provider is unable to resolve the issue within the defined Severability response time, they shall be held liable against the defined penalty. Severity levels will be agreed mutually with the Service Provider in the service agreement

30.9.7 Penalty Cap and Chronic Non-Performance

1. **Penalty Cap:**

Total penalties in any contract quarter shall not exceed 20% of the total amount payable in the any Quarter, and in any contract, year shall not exceed 20% of the total amount of that contract year, and in the contract, duration shall not exceed 20% of the Total Contract Value.

2. Chronic Non-Performance shall entitle CDNS to invoke PBG, scope reduction, or termination.

30.9.8 Delay Not Attributable to the Service Provider

Any delay in the performance or delivery of obligations by the Service Provider that is caused due to reasons attributable to the CDNS shall not attract any penalty or liquidated damages.

In such cases, the corresponding timelines shall be reasonably extended, subject to mutual agreement between the CDNS and the Service Provider, without any additional financial liability on the CDNS.

30.9.9 Right to Review and Appeal Penalties

Notwithstanding anything to the contrary, the Service Provider shall reserve the right to review and appeal against any penalties imposed by CDNS, and the CDNS shall not withhold, deduct, or set off any payments due to the Service Provider without first providing the Service Provider with written notice and a reasonable opportunity to contest, respond to, and agree upon any such penalty.

31 ANNEXURE D – CHANGE REQUEST FORM

CR Number	Version	Issue Date	BRD Reference Number
-----------	---------	------------	----------------------

Work	xxx	x	xx	Jira Ticket ID
------	-----	---	----	----------------

Request Form

Description

Customer	Central Directorate of National Savings			
Title	Change Request	Request Date	xx	
Originator	CDNS			
Description of Request	xx			
Change details	xx			
Responsibilities of Customer	xx			
Responsibilities of Paysys				
Assumptions	xx			
Delivery	Technical Efforts required for the Activity/Change			
	Description	Man day(s)	Unit Rate (PKR)	Total (PKR)
	Senior Solution Design specialist	x	xxx	xxxx
	Software Developers	x	xxx	xxxx
	Quality assurance	x	xxx	xxxx
	Total Efforts & Cost (excluding tax)	xx		xxxx

Approval

I/we agree to the contents of Work Request & the terms & conditions mentioned above.

Central Directorate of National Savings		Paysys Labs Pvt. Ltd	
Name		Name	
Date		Date	
Signature		Signature	

Payment Terms:

Payment against each approved Change Request shall be made on a milestone basis as follows:

- i. 15% of the CR Value shall be invoiced upon formal approval of the CR at step 1 after submission of the detailed CR form covering Scope of work (including process flows, descriptions, and details of the change and its impact), Estimated Man-days and Cost, Project Plan, Work Breakdown structure, any 3rd Party Dependencies, tools, or services required,

- ii. 70% of the CR value shall be invoiced upon UAT Signoff by CDNS at step 4.
- iii. 15% of the CR Value shall be invoiced upon Go-Live/ Production Deployment at step 5.

All invoices shall be submitted by the Service Provider through the project management tool and email/ courier accompanied by the relevant milestone completion evidence. CDNS shall notify Paysys within Ten (10) Business Days of receiving the invoice of any discrepancy/objection to an invoice, which shall be rectified by Paysys within Ten (10) Business Days whereupon a corrected/amended invoice shall be issued/submitted by Paysys and payment shall be made by CDNS within Forty-Five (45) days of invoice approval.