

Annexure A - Definitions

For the purposes of this Agreement, the following terms shall have the meanings set forth below:

1. **Acceptable Use Policy (AUP):** Refers to PICO's policy outlining the permissible use of its Public Cloud Services by the CLIENT and CLIENT'S Authorized Users. The AUP sets out the rules of conduct and restrictions designed to protect the integrity, security, and lawful use of the Cloud Services.
2. **Access Control:** Refers to the security measures and policies implemented by PICO to regulate and restrict who or what (users, processes, devices) can view, use, or modify resources within the Public Cloud Services.
3. **Affiliate:** Means, with respect to any Party, any entity that directly or indirectly controls, is controlled by, or is under common control with that Party. For the purpose of this definition, "control" means the direct or indirect ownership of more than fifty percent (50%) of the voting shares or similar right of ownership in an entity, or the legal power to direct or cause the direction of the general management and policies of an entity, whether through the ownership of voting shares, by contract, or otherwise.
4. **Agreement:** Means this Master Services Agreement, including all its Annexures (Annexure A, B, C, D, E, F, G), any Proposal, and any Purchase Order or Work Order accepted by PROVIDER, all as may be amended from time to time in accordance with the terms hereof.
5. **Authentication:** Refers to the process of verifying the identity of a user, device, or process attempting to access Public Cloud Services, typically involving credentials like passwords, multi-factor authentication, or digital certificates.
6. **Authorization:** Refers to the process of determining what specific resources or actions an authenticated user, device, or process is permitted to access or perform within the Public Cloud Services.
7. **Authorized User:** Means any individual or entity, including employees, agents, contractors, or customers of the CLIENT, who is authorized by the CLIENT to access and use the Public Cloud Services under the terms of this Agreement.
8. **Bare Metal Server (BMS):** Refers to a physical server provided by PICO without virtualization, offering dedicated hardware resources for high-performance workloads that require direct access to underlying infrastructure.
9. **BDT:** Refers to Bangladesh Taka, the lawful currency of the People's Republic of Bangladesh, which shall be used as the standard unit for all payments, fees, and charges specified under this Agreement unless otherwise stated.
10. **BEFTN:** Stands for Bangladesh Electronic Funds Transfer Network. It's a system that allows electronic fund transfers between banks in Bangladesh.
11. **Block Storage:** Refers to a data storage method offered by PICO that divides data into fixed-sized blocks, each assigned a unique identifier, offering high performance and low latency for use cases like databases and virtual machines.
12. **Business Day:** Means a day (other than a Friday or Saturday) on which banks are generally open in Bangladesh for the transaction of normal banking business.
13. **Client:** Means the customer entity that is the signatory to this Agreement. With respect to each purchase order executed under this Agreement, "Client" also means an Affiliate which executes such purchase order.
14. **Client Data:** Means all data, information, files, content, and materials (including text, audio, video, images, graphics, animations, illustrations, and personal or business data) submitted, stored, or otherwise processed by the CLIENT or its Authorized Users within the Public Cloud Services.
15. **Cloud Server Backup Service:** Refers to the managed backup solution provided by PICO for cloud servers, ensuring data recoverability.
16. **Cloud Server Disaster Recovery (DRaaS):** Means a comprehensive Public Cloud Service provided by PICO that ensures business continuity by replicating and restoring cloud environments to a secondary site in case of a primary site failure, offering robust Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
17. **Cloud Service Provider (CSP):** means a company, such as PICO, that delivers cloud computing services, including IaaS, PaaS, and SaaS, to individuals or businesses.

18. **Client Self-Service Portal:** Refers to PICO's proprietary web-based interface that provides CLIENTs with a unified platform for provisioning, managing, monitoring, and accessing billing information for their Public Cloud Services.
19. **Compliance:** Refers to adherence to applicable laws, regulations, industry standards, and internal policies governing data protection, privacy, and security in the context of Public Cloud Services.
20. **Confidential Information:** Means any non-public information disclosed by one Party (the "Disclosing Party") to the other Party (the "Receiving Party"), whether in written, oral, electronic, or other form, that is designated as confidential or that, by its nature or the circumstances of its disclosure, should reasonably be understood to be confidential. Confidential Information includes, but is not limited to, trade secrets, business plans, financial data, technical data, product designs, Client Data, pricing information, and marketing strategies.
21. **Container:** Is a lightweight virtualization method enabling multiple isolated applications to run on a shared operating system within the Public Cloud Services.
22. **Container Engine:** Is a cloud-based service provided by PICO for deploying and managing containerized applications.
23. **Cybersecurity:** Refers to the practices, technologies, and processes designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access within the Public Cloud environment.
24. **Data Breach:** Refers to a security incident where Client Data or other sensitive information is accessed, disclosed, acquired, or used without authorization, or is lost or stolen.
25. **Data Encryption:** Refers to the process of transforming Client Data into an unreadable format to prevent unauthorized access, both in transit (during transmission) and at rest (when stored), using cryptographic keys.
26. **Data Residency:** Refers to the physical location where Client Data is stored and processed, ensuring compliance with local laws and regulations concerning data sovereignty.
27. **DDoS-P (Distributed Denial of Service Protection):** Protects Public Cloud Services and Client resources from DDoS attacks by mitigating malicious traffic aimed at disrupting service availability.
28. **Disclosing Party:** Shall mean any Party disclosing Confidential Information to the other Party.
29. **DNS (Domain Name Service):** Is a cloud-based domain resolution service provided by PICO for fast and reliable name resolution for Public Cloud Services.
30. **DNS-GSLB (DNSsec and Global Server Load Balancing):** Enhances DNS security and distributes traffic across global server locations to optimize performance and availability for Public Cloud Services.
31. **Documentation:** Means any and all additional documents, policies, procedures, programs, requirements, criteria and/or information relating to the usage of the Cloud Services, including but not limited to the Acceptable Use Policy (AUP), Data Retention Policy, and/or Service Level Agreements ("SLAs"). PICO may update or modify the Documentation from time to time, provided that changes to the Documentation will not result in a material reduction in the level of performance or availability of the applicable Cloud Services provided to the User(s) for the duration of Term of such usage.
32. **Downtime:** Refers to the period during which the Public Cloud Services are unavailable or do not meet the specified Service Levels, excluding scheduled maintenance or events caused by factors outside of PICO's reasonable control.
33. **Due Date:** means the payment or renewal date of the customer's active subscription plan.
34. **Effective Date:** Means the date on which this Agreement becomes effective and binding on the Parties, as specified on the first page of this Agreement.
35. **EIP (Elastic IP):** Is a dedicated public IP address that can be dynamically associated with Public Cloud instances (ECS or BMS).
36. **ELB (Elastic Load Balancer):** Is a service provided by PICO that distributes incoming network traffic across multiple servers to ensure high availability and efficient resource utilization for Public Cloud applications.
37. **Endpoint Detection and Response (EDR):** Refers to security solutions provided by PICO that protect cloud instances and other endpoints from malware, advanced persistent threats, and other security threats.

- 38. **EVS (Elastic Volume Service):** Is a scalable block storage service provided by PICO for ECS and BMS instances.
- 39. **Firewall as a Service (NGF / AIF / HMF):** Provides cloud-based firewall solutions (including Next-Generation Firewalls, Advanced Internal Firewalls, and Hybrid-Mesh Firewalls) for network security within the Public Cloud Services, enforcing traffic rules and threat prevention.
- 40. **Force Majeure:** Has the meaning ascribed to it in Clause 8 of the Master Services Agreement (Main body).
- 41. **IAM (Identity Access Management):** Manages user permissions and access to Public Cloud resources provided by PICO, ensuring that only authenticated and authorized users can access specific services and data.
- 42. **IaaS (Infrastructure as a Service):** Is a cloud computing model in which virtualized computing resources, such as servers, storage, and networking, are provided by PICO to users over the internet, forming the foundational layer of Public Cloud Services.
- 43. **Image Management Service (IMS):** Is a service provided by PICO for creating, storing, and managing system images for ECS instances.
- 44. **Incident:** Means any event or condition that causes or may cause an interruption or reduction in the quality or availability of a Public Cloud Service or component thereof.
- 45. **Incident Response:** Refers to the structured process followed by PICO to identify, contain, eradicate, recover from, and learn from security incidents or data breaches.
- 46. **Intellectual Property (IP) / Intellectual Property Rights (IPR):** Means all proprietary information, patents, patent applications, trademarks, trade names, service marks, certification marks, collective marks, designs, processes, inventions, licenses, copyrights, and trade secrets of either Party, including, but not limited to, such rights relating to the origin, design, manufacture, programming, operations, function, configuration, or service of the licensed product.
- 47. **Key Management Service (KMS):** Is a cloud-based encryption key management solution provided by PICO, enabling secure creation, storage, and management of cryptographic keys.
- 48. **Lock-in Period:** Is a fixed duration, as specified in this Agreement or any specific Purchase Order, during which withdrawals, exits, or terminations are restricted or subject to penalties to ensure commitment and protect interests.
- 49. **Malware:** Refers to malicious software (e.g., viruses, worms, ransomware, spyware) designed to disrupt computer operations, gather sensitive information, or gain unauthorized access to computer systems, which PICO actively defends against.
- 50. **Marketplace Offering / Listing:** Any Public Cloud Service or third-party solution made available for purchase or subscription via the Marketplace.
- 51. **Marketplace Provider:** A third-party vendor offering their solutions through the Marketplace.
- 52. **MFS (Mobile Financial Services):** Is the use of a mobile phone to access financial services and conduct financial transactions within Bangladesh.
- 53. **Monthly Recurring Charge (MRC):** Refers to the fixed, recurring fee payable by the CLIENT on a monthly basis for the ongoing provision of services or products under this Agreement.
- 54. **Multifactor Authentication (MFA):** Is a security mechanism required by PICO that requires users to provide two or more forms of authentication to verify their identity for accessing Public Cloud Services, significantly enhancing security.
- 55. **Multi-availability Zone:** Means the deployment of PICO's infrastructure across multiple distinct and physically separated locations within a geographical region of Bangladesh, designed to be isolated from failures in other zones, providing high availability and fault tolerance for Public Cloud Services.
- 56. **NAT Gateway (NAT):** Enables private Public Cloud instances to securely access the internet while maintaining network isolation.
- 57. **Network ACL:** Is a security layer provided by PICO that controls traffic flow at the subnet level within a VPC.
- 58. **Next-Generation Firewall (NGF):** Is an advanced firewall solution provided by PICO with deep packet inspection, intrusion prevention, and application control capabilities.
- 59. **Network Operations Center as a Service (NOCaaS):** A specialized service to handle the comprehensive, 24/7/365 monitoring, management, and support of IT infrastructure, including cloud resources and connectivity. The service acts as a dedicated command center that proactively

- monitors the network and systems, rapidly detects and triages incidents, performs troubleshooting and root cause analysis, and ensures high availability, security, and optimal performance.
60. **NPSB:** Refers to the National Payment Switch Bangladesh, a centralized platform operated by Bangladesh Bank that facilitates the interconnectivity and interoperability of electronic payment systems.
 61. **Object Storage:** Is a data storage architecture offered by PICO where data is stored as discrete units, or objects, along with metadata and a unique identifier, optimized for scalability and unstructured data.
 62. **OBS (Object Storage Service):** Is a cloud-based storage solution provided by PICO for storing unstructured data as objects.
 63. **OpenStack:** Refers to the open-source cloud operating system used by PICO as its foundational Infrastructure-as-a-Service (IaaS) platform for managing computing, storage, and networking resources.
 64. **PaaS (Platform as a Service):** Is a cloud computing model where PICO offers a platform with hardware and software tools to develop, deploy, and manage applications over the internet.
 65. **Party / Parties:** Refers to PICO or the CLIENT individually, and "Parties" refers to PICO and the CLIENT collectively.
 66. **Personal Data:** Means any information related to any identified or identifiable person and any other additional data deemed as personal data under the applicable personal data protection laws.
 67. **Person:** Shall mean any individual, corporation, company, voluntary association, partnership, joint venture, limited liability company, trust, unincorporated association or government (or any agency, instrumentality or political subdivision thereof).
 68. **PICO Marketplace (or "Marketplace"):** An online platform operated by PICO for the offering and procurement of Public Cloud Services and third-party solutions.
 69. **Prepaid Basis:** Refers to a payment structure where the CLIENT is required to make payment in advance for the services to be provided under this Agreement.
 70. **Price:** Means the fees and charges payable for Public Cloud Services as specified in Annexure D (Product and Payment Schedule) and/or any relevant Purchase Order.
 71. **Primary Tenure:** Means the initial fixed term of the Agreement, as specified in the Product and Payment Schedule (Annexure D) or a specific Purchase Order, during which the Agreement is binding and subject to specific termination conditions.
 72. **Privileged Access Management (PAM):** Refers to security solutions and practices employed by PICO to secure, monitor, and control highly sensitive access to critical cloud infrastructure and systems.
 73. **Prohibited Use:** Means any use of the Public Cloud Services or resources provided under this Agreement that is unlawful, unauthorized, under restriction, or otherwise inconsistent with the terms and conditions of this Agreement, including the Acceptable Use Policy.
 74. **Proposal:** Means the proposal document provided by PICO to the CLIENT outlining the scope, nature, and commercial terms of the Services, which forms part of this Agreement.
 75. **Public Cloud Services/Cloud Services:** Means the cloud computing services provided by PICO to the CLIENT, including but not limited to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Container services, storage, networking, security, and other related services as described in the Proposal, provided via PICO's shared cloud infrastructure.
 76. **Purchase Order (PO):** Means a document issued by the CLIENT and accepted by PICO for the purchase and delivery of Public Cloud Services under the terms of this Agreement.
 77. **Receiving Party:** Shall mean the Party receiving Confidential Information from the Disclosing Party.
 78. **Recovery Point Objective (RPO):** Refers to the maximum acceptable amount of data loss measured in time, defining how much data can be lost during a disaster before significant harm occurs to a business process.
 79. **Recovery Time Objective (RTO):** Refers to the maximum acceptable length of time that a system or application can be down after a failure or disaster before it significantly impacts business operations.
 80. **Resolution Time:** Refers to the total amount of time it takes to fully resolve a technical issue for Public Cloud Services, starting from the moment it is reported until the problem is completely fixed, including diagnosis, troubleshooting, and implementation of the solution.

81. **Response Time:** Refers to the amount of time it takes for a Public Cloud Service to respond to an Authorized User's request.
82. **Risk Management (Cybersecurity):** Refers to the ongoing process of identifying, assessing, and treating cybersecurity risks to protect the confidentiality, integrity, and availability of information and systems within the Public Cloud Services.
83. **RTGS:** Stands for Real Time Gross Settlement, which is an electronic system for transferring funds between bank accounts in Bangladesh.
84. **SaaS (Software as a Service):** Is a cloud computing model where software applications are hosted by PICO and made available to Authorized Users over the internet, typically through a subscription model.
85. **Scalability:** Is the ability of a Public Cloud Service or system to handle an increasing workload efficiently by adjusting its resources accordingly.
86. **Scalable File Service (SFS):** Is a managed, scalable file storage service provided by PICO for shared access across cloud instances.
87. **Security Group (SG):** Is a firewall-like feature provided by PICO that controls inbound and outbound traffic for cloud resources.
88. **Security Incident:** Means any event or condition that causes or may cause an interruption or reduction in the quality or availability of a Public Cloud Service or component thereof, or any unauthorized access, use, disclosure, modification, or destruction of Client Data, or interference with the operation of the Public Cloud Services.
89. **Security Information and Event Management (SIEM):** Refers to a security service provided by PICO that collects, analyzes, and correlates security event logs from various sources for real-time threat detection and security incident analysis across the Public Cloud environment.
90. **Security Orchestration, Automation and Response (SOAR):** Refers to security solutions provided by PICO that automate the response to security alerts and streamline security operations workflows.
91. **Service Level:** Means the specific performance standards and metrics for the Public Cloud Services as detailed in the Service Level Agreement (Annexure C).
92. **Shared Responsibility Model:** Refers to the cloud security framework outlining the division of security responsibilities between PICO (the Cloud Service Provider) and the CLIENT (the Cloud Customer), where PICO is responsible for the "security of the cloud," and the CLIENT is responsible for "security in the cloud."
93. **Single Sign-On (SSO):** Is an authentication process provided by PICO that allows Authorized Users to access multiple Public Cloud applications or services with a single set of login credentials.
94. **SLA:** Refers to the Service Level Agreement that outlines the commitments PICO makes regarding delivery and/or performance of the Services.
95. **Security Operations Center as a Service (SOCaaS):** Refers to a fully managed, 24/7/365 manned, security operations center service provided by PICO for real-time threat detection, incident response, and detailed reporting on the security posture of the Public Cloud services.
96. **Software:** Means any program, tool, and other operating information used by a physical computer or cloud platform, including any third-party software, provided by a software licensor/provider under the Agreement for the usage of PROVIDER or CLIENT or both.
97. **TrustNet:** A dedicated, private networking service that establishes a high-throughput, low-latency, end to end network security, software based network automation, and reporting between an on-premises data center and/or network endpoint of any type (e.g. node, browser, machine, human identity login) and/or a cloud provider's Virtual Private Cloud (VPC).
98. **Work Order (WO):** Is an Agreement between a CLIENT and the PROVIDER to deliver goods or services on a recurring basis over a set period.
99. **Technical Information:** Means any information generated by or for the PROVIDER concerning CLIENT's identification by reference to an identification number (or to one or more factors), activity log, billing, usage volume, statistics or other specific information associated with the CLIENT's use/utilization of the Services offered by the PROVIDER.
100. **Tenant:** Refers to an individual or organization that subscribes to and uses services provided by PICO, essentially acting as a CLIENT who accesses and utilizes shared infrastructure while maintaining data isolation and separate access controls within that shared environment, typically within a multi-tenant architecture.

- 101. **Term:** Means the duration of this Agreement, commencing on the Effective Date and continuing until terminated in accordance with Clause 9 of the Master Services Agreement (Main body).
- 102. **Third Party:** Means any person, entity, or organization that is not a signatory to this Agreement and is not an Affiliate of a Party, including but not limited to agents, contractors, sub-contractors, customers, consultants, or other individuals or entities acting on behalf of or in connection with the Parties but who are not themselves bound by this Agreement.
- 103. **Threat Intelligence:** Refers to evidence-based knowledge about existing or emerging threats, including context, mechanisms, indicators, implications, and actionable advice, used by PICO to inform its security defenses.
- 104. **Threat Intelligence and Flow Analytics:** Refers to services provided by PICO that monitor and analyze network traffic for potential threats and anomalies within the Public Cloud environment.
- 105. **Uptime:** Refers to the percentage of time that the Public Cloud Services are operational and accessible, as defined and measured in the Service Level Agreement (Annexure C).
- 106. **Virtual Machine (VM):** Is a software-based emulation of a physical computer that runs an operating system and applications just like a traditional machine, provisioned as an ECS instance within PICO.
- 107. **Virtual Private Cloud (VPC):** Is a private, isolated cloud network provided by PICO for secure resource deployment for a CLIENT, allowing them to define their own network topology.
- 108. **Virtual Private Network (VPN):** Is a secure tunnel for encrypting communication between on-premises networks and PICO environments.
- 109. **Vulnerability:** Means a weakness in the Public Cloud Services, its systems, or processes that could be exploited to compromise the confidentiality, integrity, or availability of Client Data or Public Cloud Services.
- 110. **Vulnerability Assessment and Penetration Testing (VAPT):** Refers to security services offered by PICO to evaluate cloud security by identifying and analyzing vulnerabilities (Vulnerability Assessment) and actively attempting to exploit them to test the effectiveness of security controls (Penetration Testing).
- 111. **WAAPaaS (Web Application and API Protection as a Service):** Is a security service provided by PICO that protects web applications and APIs from attacks, including Web Application Firewalls (WAF), bot protection, and API security.

Service Requests Management

The following classifications shall apply to Service Requests:

- A. **High:** Means any service requests that concern the critical part of YOUR service usage and could potentially cause significant damage or service outage. These requests shall be managed urgently due to their high impact.
- B. **Medium:** Means any service request that indicates the necessity of changing service or service details, checking on the service, or asking for helpful advice. These requests shall be managed properly within a reasonable timeframe.
- C. **Low:** Means any general service requests or service detail inquiries that do not immediately impact critical service functionality. These requests shall be managed at regular intervals.
- D. **Planned:** Means any service requests that cannot be completed within a short time and require a specific plan for implementation. The duration for completion will vary according to the nature of the request and the agreed-upon plan.