Annexure E

Acceptable Use Policy (AUP)

This Acceptable Use Policy (the "AUP") outlines the prohibited activities and acceptable practices for using the PICO (the "PROVIDER," "We," "Our," or "Us") and its network of online platforms, products, services, and infrastructure (collectively, the "Services").

This AUP applies to all CLIENTS and USERS (collectively, "YOU" or "YOUR") who access or utilize the Services through purchasing, subscribing, or registering accounts. The Services must be used in accordance with their intended purpose and in compliance with the applicable Master Services Agreement, including our Terms of Service ("Terms"), to which this AUP is incorporated by reference.

By using the Services, YOU agree to abide by the latest version of this AUP, which may be modified by Us at any time by posting a revised version. It is YOUR responsibility to regularly review this AUP for updates. YOU also agree to ensure that YOU and YOUR Authorized Users, employees, agents, or any party accessing the Services through YOUR account ("End Users") comply with this AUP. If YOU violate this AUP or assist others in doing so, PICO may take disciplinary action without incurring any liability, including but not limited to, suspension or termination of YOUR use of the Services and deletion of YOUR account, without refund.

1. PROHIBITED CONTENT AND ACTIVITIES

YOU shall not use the Services to engage in, facilitate, encourage, promote, or instruct others to engage in any illegal, harmful, fraudulent, or offensive activities, or to transmit, store, display, distribute, or otherwise make available any information or content (User Content) that falls into these categories. The following activities and content are strictly prohibited:

1.1. Illegal, Unlawful, Harmful, or Fraudulent Activities

1.1.1. Engaging in any activity that violates any applicable local, national, or international law or regulation, including but not limited to laws regarding child exploitation, illegal gambling, fraud, money laundering, terrorism financing, or the sale/distribution of illegal substances.

1.1.2. Offering or distributing fraudulent goods, services, schemes (e.g., "get-rich-quick" schemes, pyramid schemes), or promotions.

1.1.3. Activities that infringe upon the rights of others, including privacy, publicity, or contractual rights.

1.2. Intellectual Property Infringement

1.2.1. Infringing upon or misappropriating the intellectual property rights, proprietary rights, trade secrets, or confidential information of PICO or any third party (including copyrights, trademarks, patents). This includes unauthorized copying, using, or distributing copyrighted or trademarked content without explicit permission or proper attribution.

1.2.2. Unauthorized disclosure of private, proprietary, or confidential data or information belonging to others.

1.2.3. Reselling or sub-licensing PICO's Services or providing access to them without prior written consent, unless expressly permitted under a specific Partner Program Track.

1.3. Offensive or Objectionable Content

1.3.1. Content that is defamatory, libelous, obscene, pornographic (specially child pornography), abusive, harassing, threatening, discriminatory, an invasion of privacy, or that promotes violence, hatred, bigotry, racism, religious intolerance, misogyny, or any form of physical harm against individuals, groups, or animals.

1.3.2. Content that is culturally or socially objectionable under the laws or prevailing moral standards of Bangladesh or the jurisdiction where the Services are accessed or the User Content is consumed.

1.4. Malware and Malicious Code

1.4.1. Transmitting, storing, or otherwise making available any content or computer technology (e.g., viruses, Trojan horses, worms, time bombs, cancelbots, spyware, ransomware) that could cause damage, disrupt, secretly intercept, or take control of any system, program, data, or personal information.

1.4.2. Engaging in activities that involve the creation, distribution, or operation of botnets or similar malicious networks.

1.5. Misrepresentation and Impersonation

1.5.1. Submitting content or information that inaccurately represents, impersonates, or otherwise misleads others about YOUR identity, qualifications, affiliations with individuals or organizations, or assuming someone else's identity.

1.5.2. Forging TCP-IP packet headers, email headers, or any part of a message to mislead about its origin or path.

2. NO SPAM OR UNSOLICITED COMMUNICATIONS

2.1. Strict Prohibition

YOU are strictly prohibited from sending, distributing, or facilitating the sending of unsolicited bulk commercial email, messages, advertisements, or promotions (commonly known as "SPAM") through the Services. This prohibition extends regardless of how recipient email addresses were acquired, generated, or obtained, and includes the use of opt-in, double opt-in, or any other form of email recipient list for bulk unsolicited communications via the Services.

2.2. Prohibited Spamming Activities

2.2.1. Sending unsolicited bulk messages, including instant messenger spam, SMS spam, or unsolicited voice calls.

2.2.2. Spamming internet newsgroups, forums, or online communities.

2.2.3. Posting spam content on classified services (e.g., Craigslist) or social media platforms except in designated, approved areas and in compliance with their terms of service.

2.2.4. Using PICO's communication tools (e.g., forums, messaging features within Services) to promote businesses or opportunities not explicitly approved by PICO.

2.2.5. Collecting responses to messages from other services if they violate this policy.

2.2.6. Modifying email headers or impersonating another person or entity without their explicit permission.

2.3. Indemnification (for Spam Violations)

All CLIENTS, Affiliates, agents, employees, or promoters engaging in any electronic commercial mail promotions in violation of this Policy agree to indemnify and hold PICO harmless from any claims, charges, legal actions, debts, or allegations arising from violations of applicable laws governing commercial email transmission or this AUP. PICO shall provide prompt notice of such claims, but retains the right to select its own legal representation, with all related costs and expenses borne solely by the party responsible.

3. NO SECURITY VIOLATIONS

YOU are prohibited from using the Services to compromise the security or integrity of any network, computer system, software, or device (referred to as a "System"). Forbidden activities include:

3.1. Unauthorized Access: Gaining access to or using any System without explicit permission, including attempting to probe, scan, or test a System's vulnerabilities or bypassing any security or authentication measures.

3.2. Interception: Monitoring data or traffic on a System without authorization.

3.3. Malicious Code Deployment: Deploying or executing malicious code, exploits, or malware on any System.

3.4. Reverse Engineering/Cracking: Attempting to reverse engineer, decompile, or disassemble any PICO Service or related software, or attempting to circumvent any license keys or copy protection mechanisms.

4. NO NETWORK AND SYSTEM ABUSE

YOU are prohibited from connecting to users, hosts, or networks unless YOU have explicit permission to do so. Prohibited activities include:

4.1. Monitoring or Crawling: Monitoring or crawling any System in a way that causes harm, disruption, or excessive load to the System or its resources.

4.2. Denial of Service (DoS): Overloading or attempting to overload a target System with communication requests so it cannot respond to legitimate traffic or respond so slowly it becomes ineffective. This includes initiating or participating in Distributed Denial of Service (DDoS) attacks against any target.

4.3. Intentional Interference: Deliberately disrupting the proper operation of any System, including attempts to overload a System via methods like mail bombing, news bombing, broadcast attacks, or flooding.

4.4. Operation of Certain Network Services: Running network services such as open proxies, open mail relays, or open recursive DNS servers without authorization or proper security configurations that prevent abuse.

4.5. Avoiding System Restrictions: Using manual or automated methods to bypass any access or usage limits placed on a System or Service.

4.6. Excessive Resource Consumption (Fair Use): While PICO provides scalable resources, activities that lead to disproportionate or abusive consumption of shared resources (e.g.,

excessive CPU, network I/O, or database queries) that negatively impact the performance, availability, or stability of the Services for other CLIENTS or PICO's infrastructure are prohibited. In such cases, PICO reserves the right to implement appropriate measures, including limiting resource availability or working with the CLIENT to optimize their usage.

5. NO HIGH-RISK USE

YOU may not use the Services in any application or situation where failure of the Services could lead to death or serious bodily injury to persons, or to severe physical or environmental damage. This includes, but is not limited to, the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support systems, or weapons systems.

6. SHARED RESPONSIBILITY MODEL FOR SECURITY AND COMPLIANCE

6.1. The CLIENT acknowledges and agrees to its responsibilities within the Shared Responsibility Model. While PICO is responsible for the security of the cloud infrastructure (e.g., physical security, network infrastructure, virtualization platform), the CLIENT is solely responsible for security in the cloud. This includes, but is not limited to:

6.1.1. Client Data Security: Protecting the confidentiality, integrity, and availability of Client Data, including any Personal Data, processed, stored, or transmitted through the Services.

6.1.2. Operating System and Application Security: Securing the operating systems, applications, configurations, and network settings within YOUR Public Cloud Service instances. This includes applying necessary patches, updates, and configuring appropriate security controls (e.g., firewalls, access controls, vulnerability management).

6.1.3. Access Management: Managing and securing YOUR user identities, credentials, and access permissions within YOUR account.

6.1.4. Compliance: Ensuring that YOUR use of the Services and any User Content comply with all applicable laws and regulations specific to YOUR industry or jurisdiction.

6.1.5. Backup and Recovery: Implementing and maintaining appropriate backup and disaster recovery procedures for YOUR Client Data and applications, unless explicitly covered by a managed backup service from PICO.

6.2. PICO shall not be responsible or liable for any security breaches, data loss, or system compromise that arises from the CLIENT's misconfiguration, lack of proper security controls, failure to apply patches, or other omissions in its responsibilities under the Shared Responsibility Model. SLA credits (as per Annexure C) do not apply to service disruptions or security breaches solely attributable to CLIENT-side security failures.

7. COMPLIANCE AND ENFORCEMENT

7.1. PICO reserves the right, but does not assume the obligation, to monitor and investigate any violations of this AUP, or any other unauthorized or prohibited use of the Services. In response to a suspected or actual violation, PICO may, at its sole discretion, do the following:

7.1.1. Investigation: Investigate suspected violations of this AUP, including gathering information from the CLIENT and other USERS involved.

7.1.2. Warning: Issue a warning to the CLIENT.

7.1.3. Suspension: Temporarily suspend access to the Services or portions thereof.

7.1.4. Termination: Permanently terminates access to the Services and Master Services Agreement.

7.1.5. Content Removal: Remove or block access to User Content that violates this AUP.

7.1.6. Reporting: Report illegal activities to the appropriate law enforcement authorities or relevant regulatory bodies.

7.1.7. Legal Action: Take legal action to enforce this AUP and seek damages for any harm caused by the violation.

7.2. PICO may share User information in accordance with its Privacy Policy to protect its Services, enforce this AUP, and comply with legal obligations, including responding to valid governmental or court orders.

8. REPORTING VIOLATIONS

If YOU become aware of any violation of this AUP, please report it to us immediately at: info@picopublic.cloud providing detailed information, including specific dates, times, and the nature of the suspected violation, will greatly assist US in investigating and taking appropriate action.

9. **ACKNOWLEDGEMENT:**

By using PICO's Services, YOU explicitly agree to adhere to this AUP. Failure to comply may result in restrictions, suspension, or termination of YOUR access to the Services.