ALFRED One, ALFRED One Data

Acceptable Use Policy (AUP)

1. Purpose

This Acceptable Use Policy ("Policy") defines acceptable and prohibited uses of the services provided, including cloud virtual machines, web hosting, and internet access (collectively "Services"). The purpose of this Policy is to protect the integrity, security, and availability of the Services, and to ensure all users operate in a responsible and lawful manner.

2. Scope

This Policy applies to all individuals, organizations, and entities ("Users") who access or use the Services.

3. Acceptable Use

Users must use the Services in a manner that is:

- Lawful: Compliant with all applicable laws, regulations, and industry standards.
- Responsible: Respectful of the rights of others, including intellectual property, privacy, and confidentiality.
- Secure: Protecting the confidentiality, integrity, and availability of data and systems.

4. Prohibited Uses

Users are strictly prohibited from engaging in the following activities:

4.1 Illegal Activities

- Using the Services to conduct or promote unlawful acts, including fraud, money laundering, identity theft, or distribution of counterfeit goods.
- Hosting or distributing pirated software, copyrighted materials, or any content that infringes upon intellectual property rights.

4.2 Security Violations

- Attempting to gain unauthorized access to any system, network, or account.
- Engaging in denial-of-service (DoS), distributed denial-of-service (DDoS), or other network attacks.

- Deploying malware, viruses, ransomware, or any malicious code.

4.3 Network & Service Abuse

- Excessive use of bandwidth or resources that disrupts the performance or availability of the Services.
- Running open mail relays, spam servers, or engaging in unsolicited bulk email ("spam").
- Operating cryptocurrency mining, botnets, or automated exploitation tools without prior written authorization.

4.4 Inappropriate or Harmful Content

- Hosting or transmitting content that is obscene, abusive, harassing, defamatory, or discriminatory.
- Hosting or promoting hate speech, terrorism, violence, or content intended to incite harm.
- Hosting or distributing child sexual abuse material (CSAM) or any form of exploitation.

5. Internet Access Rules

- Users must not bypass security controls such as firewalls, content filters, or monitoring systems.
- Users may not use internet access for illegal file sharing, torrenting, or accessing prohibited content.
- Users must not interfere with other Users' access to the internet or Services.

6. User Responsibilities

- Users are responsible for maintaining the security of their accounts, credentials, and hosted applications.
- Users must promptly report any suspected security incidents, breaches, or misuse.
- Users must maintain updated patches, security software, and configurations on their virtual machines and hosted applications.

7. Enforcement

- Violations of this Policy may result in warnings, suspension, or termination of Services without notice.
- The provider reserves the right to investigate suspected violations and cooperate with law enforcement agencies where required.

- Users are responsible for any damages, liabilities, or costs resulting from a violation of this Policy.

8. Modifications

This Policy may be updated or revised at any time. Continued use of the Services constitutes acceptance of the most recent version of this Policy.