SCHEDULE 2: ACCEPTABLE USE POLICY (AUP)

Version: October 2024

This Acceptable Use Policy ("AUP") outlines the terms under which 3verest PTY Limited ("3verest") provides Cloud Services to its Clients. This AUP is incorporated into the Master Services Agreement ("MSA") between 3verest and the Client and governs the use of all 3verest Cloud Services. By using 3verest Cloud Services, the Client agrees to comply with this AUP.

1. General Overview of Cloud Services

Cloud Server(s):
Cloud servers provided by 3verest include a combination of hardware and software resources, such as Central Processing Units (CPU), Random Access Memory (RAM), Hard Disk Drives (HDD), Operating Systems (OS), and User Access Licenses. These resources form the foundation for hosting and delivering applications and services.

- **Features and Functionality**: Clients can select compatible operating systems, and 3verest can provide licenses for these as part of the order process. Cloud server resources (CPU, RAM, HDD) are scalable, and additional resources can be purchased as needed.
- **Client Responsibility**: Clients must notify 3verest if they intend to use any operating system or software not listed as supported. Any issues, including performance, compatibility, or security problems arising from the use of unsupported software or operating systems, are the sole responsibility of the Client.

2. Acceptable Use and Restrictions

Prohibited Activities:
The Client agrees not to use the Cloud Services for any of the following activities, which are strictly prohibited:

- **Cryptocurrency Mining**: Using Cloud Servers for the generation or mining of cryptocurrencies (e.g., Bitcoin) is prohibited due to the excessive resource consumption associated with such activities.
- **Malicious Activities**: Hosting, transmitting, or distributing malicious software, including viruses, worms, spyware, or any software intended to harm or disrupt other networks or systems, is strictly prohibited.
- **Network Disruption**: Engaging in activities that disrupt the integrity or performance of the 3verest network, including but not limited to denial-of-service (DoS) attacks, port scanning, or any actions that overload or degrade the Cloud Services.
- **Illegal Content**: Hosting, storing, or transmitting any content that violates applicable laws or regulations, including content that infringes on intellectual property rights or privacy laws.

- **Resale of Services**: Clients may not resell, redistribute, or provide Cloud Services to third parties, including bandwidth or server access, without express written permission from 3verest.

Resource Usage and Scalability:
Clients must not exceed the allocated resources (CPU, RAM, HDD) as outlined in their order form. Any use of resources beyond the purchased capacity without prior approval may result in:

- **Throttling or Suspension**: 3verest reserves the right to temporarily reduce service performance or suspend services until resource usage is aligned with the purchased allocation.
- **Additional Charges**: Excessive use may incur additional charges as specified in the Client's order form.

3. Network and Connectivity

Bandwidth and Internet Usage:
While 3verest provides connectivity to a network and the internet as part of its Cloud Services, the following conditions apply:

- **No Guarantee of Speed**: 3verest does not warrant or guarantee the speed or consistency of internet connections or network links, whether provided directly by 3verest or through third-party providers. Any speeds provided are indicative only and do not constitute a guarantee of performance.
- **Monitoring and Throttling**: 3verest actively monitors bandwidth usage and reserves the right to throttle or restrict bandwidth at its sole discretion, particularly in cases of excessive or abusive use.
- **VPN Usage**: Clients are responsible for managing their own Virtual Private Network (VPN) configurations. Any security vulnerabilities, performance issues, or service disruptions caused by VPNs or similar network configurations are the Client's responsibility.

4. Backup Services and Disaster Recovery

Cloud Backup(s):
Cloud backup services are designed to create copies of Client data and snapshots of Cloud Servers for recovery purposes.

- **Standard Retention**: 3verest maintains a standard backup retention period of 7 days unless otherwise specified in the order form. Data beyond this retention period will not be available for restore unless additional retention is purchased.
- **Quality Disclaimer**: 3verest does not guarantee the completeness, accuracy, or integrity of backup data. It is the Client's responsibility to verify that backups meet their specific recovery needs and to request any additional backup services.

- **Client Responsibility**: Clients must ensure their data is backed up according to their recovery needs. 3verest will not be held responsible for any data loss outside the agreed retention period or resulting from the Client's failure to ensure data integrity.

Disaster Recovery Backup(s):
These backups are designed for off-site storage and restoration of Client data. Clients must manage retention periods and verify data accuracy.

- **Retention Periods**: Customizable at the time of ordering. Clients can extend retention by placing additional orders.
- **Client Responsibility**: 3verest will not be liable for the quality or completeness of disaster recovery backups beyond the specified retention period.

5. Security Responsibilities

3verest Security Measures:
3verest takes security seriously and implements industry-standard technical and organizational measures to safeguard the infrastructure supporting its Cloud Services. These include, but are not limited to:

- **Encryption**: Data at rest and in transit is protected using strong encryption protocols.
- **Firewall Protection**: Cloud Servers are protected by virtual firewalls, which provide basic intrusion prevention and monitoring.
- **Access Control**: 3verest limits administrative access to its infrastructure to authorized personnel only, using multi-factor authentication where applicable.
- **Monitoring and Alerts**: 3verest monitors its network and Cloud Services for unauthorized access attempts, suspicious activities, and security incidents. Clients are notified of any identified security incidents that may affect their data or services.

Client's Role in Security:
While 3verest provides these foundational security layers, the responsibility for securing access to and use of the Cloud Services, as well as safeguarding Client data, rests with the Client. This includes:

- **Access Management**: Clients are responsible for managing user accounts, access credentials, and permissions within their own Cloud Servers and environments. This includes enforcing strong password policies and using multi-factor authentication where possible.
- **Configuration Security**: Clients must ensure that all configurations, including operating systems, applications, and network settings, follow security best practices. Any misconfigurations or vulnerabilities introduced by the Client could compromise the security of the Cloud Services.
- **Data Security**: Clients are responsible for securing the data they store, process, or transmit using 3verest's services. This includes implementing encryption, access controls, and data classification measures tailored to their specific requirements.

- **Regular Updates and Patching**: Clients must ensure that all applications, operating systems, and other software within their control are kept up-to-date with the latest security patches and updates to mitigate vulnerabilities.
- **Security Incident Response**: In the event of a suspected or actual security breach within their own environment, Clients are responsible for promptly responding to the incident, including taking steps to contain, investigate, and remediate any security issues. 3verest will cooperate with Clients in investigating incidents that affect their Cloud Services but is not liable for breaches resulting from Client-side vulnerabilities or configurations.

Responsibility for VPN and Network Configurations:
Clients using Virtual Private Network (VPN) connections or other remote access methods to connect to the Cloud Services must ensure that these configurations are secure and align with best practices. Any vulnerabilities, unauthorized access, or performance issues resulting from misconfigured VPNs or remote access methods are the Client's responsibility.

Disclaimer of Liability for Security Breaches:
3verest provides a secure infrastructure, but it cannot guarantee absolute security. Security is a shared responsibility, and Clients are expected to take proactive steps to secure their data and access. 3verest disclaims any liability for security breaches or data losses resulting from the Client's failure to implement adequate security measures within their control. Clients are encouraged to conduct regular security audits and assessments of their environments to ensure compliance with their internal security policies and industry standards.

6. IP Address Usage

IP Address Allocation:

- **Non-Portability**: IP addresses provided by 3verest are not portable or transferable. Any use of unassigned or unauthorized IP addresses will result in the suspension of network access until the issue is corrected.
- **Misuse of IP Addresses**: Unauthorized use of IP addresses may result in immediate suspension, and any costs associated with the resolution of the issue will be borne by the Client.

7. Email Services and Spam Control

Email Use Policy:

- **Spam Monitoring**: 3verest reserves the right to monitor outgoing email traffic for spam or abusive content. In cases of suspected abuse, 3verest may suspend email services to prevent harm to network integrity or to avoid blacklisting.
- **Blocking Rights**: 3verest may block any email or attachment deemed high-risk or inappropriate, at its sole discretion, to protect the integrity of its services.

8. General Disclaimers and Limitations of Liability

No Warranties for Open Source Software:
3verest provides no warranties for any open-source software used on its servers. All risks associated with such software, including compatibility and security risks, are borne by the Client.

Liability for Client Actions:
Clients are solely responsible for any actions or omissions that violate this AUP or the MSA, including unauthorized use or modification of the Cloud Services. 3verest disclaims all liability for disruptions or damages caused by such actions.

Limitation of Liability:
3verest's liability under this AUP is strictly limited as follows:

- **Service Suspension**: 3verest reserves the right to suspend services if the Client's actions threaten the integrity or security of the 3verest network or services.
- **No Liability for Excluded Activities**: 3verest will not be liable for any damages, including loss of data, revenue, or business opportunities, resulting from activities excluded under this AUP, such as unsupported software or unapproved network configurations.
- **Service Quality Disclaimer**: The services are provided "as-is" and "as available," and 3verest disclaims any warranties not expressly set forth in the MSA, including implied warranties of merchantability or fitness for a particular purpose.

9. Governing Law

This AUP is governed by and construed in accordance with the laws of New South Wales, Australia. Any disputes arising out of or related to this AUP shall be resolved in the courts of Sydney, New South Wales.