ACCEPTABLE USE POLICY

SwiftConnect - Acceptable Use Policy (AUP)

1. **Purpose Statement**
   This Acceptable Use Policy (AUP) defines the rules and guidelines for the proper use of SwiftConnect’s digital services and information systems infrastructure. It aims to protect the availability, integrity, and confidentiality of our systems, customers, and data. As a vital part of our overall Information Security Policy, this AUP ensures ethical behaviour, regulatory compliance (particularly with the Lesotho Communications Authority), and responsible digital citizenship. It sets the expectations for all users to safeguard company assets and avoid misuse of services that could disrupt network operations or compromise customer trust.

2. **Scope**

This policy applies to all users who access SwiftConnect's infrastructure and services, including:

- Employees, interns, and contractors using internal systems or remote access
- Residential and business subscribers using ISP services and value-added products
- Third-party vendors and partners integrated through APIs or enterprise portals
- Visitors using guest Wi-Fi or public network interfaces

Systems covered include (but are not limited to): broadband internet, VoIP systems, DNS, DHCP servers, routers/modems, cloud services, CRM platforms, mobile apps, portals, user devices, and all data hosted within our ecosystem.

3. **Acceptable Use**

The following uses are encouraged and required:

- Accessing SwiftConnect systems only with authorized credentials and devices
- Using strong passwords, encryption, and multi-factor authentication
- Communicating respectfully with customers and partners via digital platforms
- Reporting security incidents or vulnerabilities to IT within 1 hour of detection
- Protecting confidential information and customer records as per LCA standards □ Using SwiftConnect services for lawful, approved, and work-related activities only
- Regularly updating devices and software to reduce risk of exploits
- Respecting copyright, licensing, and intellectual property agreements
- SwiftConnect Solutions - Acceptable Use Policy (AUP)
- Following SOPs for all service configurations, escalations, and digital transactions
- Participating in periodic cybersecurity and compliance training

4. **Unacceptable Use**

The following actions are strictly prohibited:

- Accessing or attempting to access systems or data not assigned to you
- Distributing or viewing illegal, pornographic, hateful, or violent material
- Using SwiftConnect services for fraudulent or criminal activities
- Circumventing firewalls, content filters, or traffic-shaping tools
- Launching attacks such as phishing, spoofing, or man-in-the-middle operations
- Tampering with, bypassing, or disabling security features
- Hosting proxy servers or VPNs designed to avoid legal restrictions
- Using peer-to-peer (P2P) file sharing tools that strain network resources
- Spamming, bulk-messaging, or auto-dialing using SwiftConnect's platforms
- Leaking internal business strategies, customer information, or partner contracts

5. Security Measures

To safeguard systems and data, SwiftConnect implements:

- Next-gen firewalls with anomaly detection and geofencing
- Continuous log monitoring and behavior-based alerting
- End-to-end encryption for sensitive data in transit and at rest
- Periodic vulnerability scanning and penetration testing
- Multi-factor authentication (MFA) across all admin-level accounts
- Role-based access control (RBAC) and time-based session expiration
- Automatic patch deployment across endpoints and servers
- Endpoint Detection & Response (EDR) software on all devices
- Regular backups stored across redundant, secured cloud zones
- Access to systems only from secure, verified devices and IPs

6. Monitoring & Privacy

SwiftConnect reserves the right to monitor and audit user activity for compliance, security, and performance reasons. Monitoring may include:

- Traffic logs and bandwidth consumption trends
- Login/logout activity, access logs, and session data
- Alerts for suspicious or unauthorized login attempts
- Packet inspection to detect malware or unauthorized apps
- System health reports including latency, packet loss, and uptime
- Monitoring emails and VoIP logs for abuse prevention (where lawful)
- Detecting unpatched systems or out-of-date software versions
- While user privacy is respected under data protection laws, there is no expectation of absolute privacy when using company systems for activities that may breach this policy or LCA regulations.

7. Consequences of Violations

Violations of this AUP may result in:

1. Formal warning issued by system administrators or supervisors
2. Suspension of access to systems and services
3. Termination of employment or service agreement for repeat offenses
4. Reporting to Lesotho Communications Authority for regulatory breaches
5. Involvement of law enforcement for cybercrime or fraud cases
6. Financial liability for damages or resource misuse caused
7. Legal proceedings if breach results in harm to customers or reputation

8. Acknowledgement

By using SwiftConnect Solutions' systems, all users:

- Acknowledge that they have read, understood, and agreed to this AUP
- Accept responsibility for their actions and digital footprint
- Understand the monitoring policies and consequences of violations
- Commit to using systems ethically and in compliance with applicable regulations

SwiftConnect Solutions - Acceptable Use Policy (AUP)

This policy is reviewed bi-annually and updated as needed. Notifications will be issued to all users when changes occur. Non-compliance will not be excused by ignorance.