PO Box 968, 281 E 200 N, Roosevelt, UT 84066 • 435.725.0100 • spectra-it.com

# Acceptable Use Policy (AUP)

**1. Purpose**

This Acceptable Use Policy ("AUP") outlines acceptable use of IT systems, services, and resources managed by SPECTRA ("Service Provider"). This policy is designed to protect the integrity, security, and performance of the Service Provider's systems and the data of its clients.

**2. Scope**

This policy applies to all users of the services provided by the Service Provider, including but not limited to client employees, contractors, and third parties who access systems under management or monitoring by the Service Provider.

**3. Acceptable Use**

Clients and their users must:

- Use IT resources only for lawful business purposes.
- Maintain the confidentiality, integrity, and availability of systems and data.
- Follow best practices for cybersecurity, including but not limited to:
    - Using strong, unique passwords and changing them regularly
    - Enabling multi-factor authentication wherever supported
    - Keeping software, operating systems and antivirus programs up to date
    - Reporting suspicious emails, links or attachments as soon as possible
    - Avoiding use of unsecured or public Wi-Fi for accessing sensitive systems
    - Locking devices when unattended or logging off when not in use
    - Restricting data sharing to only authorized and secure channels
- Access only the systems and data to which they have been authorized.

**4. Prohibited Use**

Clients and their users may not:

- Use IT systems for any illegal, fraudulent, or malicious activities.
- Introduce or distribute viruses, malware, or other harmful code.
- Attempt to gain unauthorized access to any system or data.
- Interfere with or disrupt network services or security controls.
- Use IT resources to harass, discriminate, or transmit offensive content.
- Store or transmit sensitive personal or financial data unless encryption and appropriate safeguards are in place.
- Share login credentials or allow unauthorized users to access systems.

- Bypassing or disabling security controls.

**5. Monitoring and Enforcement**

The Service Provider reserves the right to monitor network traffic and access logs to ensure compliance with this policy. Violations may result in:

- Suspension or termination of access to IT services.
- Notification to client management.
- Legal action if required.

**6. Client Responsibilities**

Clients must:

- Ensure their users are aware of and comply with this AUP.
- Promptly notify the Service Provider of any security incidents or suspected misuse.
- Cooperate with the Service Provider during investigations into breaches or violations.

**7. Policy Review and Amendments**

This AUP may be updated periodically. Clients will be notified of material changes. Continued use of services after changes constitutes acceptance of the updated policy.

**Acknowledgment**

By using the services provided by SPECTRA you acknowledge that you have read, understood, and agree to comply with this Acceptable Use Policy.