Uniti Group Inc.

Data Protection Policy

(Effective October 1, 2019)

Purpose. Uniti Group Inc. (the "Company") obtains and retains certain data and information as part of its normal business operations, which may include without limitation offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, financial data, etc. (collectively, "Information"). This Data Protection Policy (the "Policy") outlines measures taken by the Company's management and employees to treat such Information of its employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. Additional information about how the Company collects, shares and uses Information in certain contexts and related privacy rights is included in the Company's Privacy Policy available here: https://uniti.com/legal/policies/privacy-policy.

Commitments. The Company strives to closely monitor its security and data protection protocol in order to ensure continual and constant evolution of security measures, including fine tuning security configurations and monitoring industry tools and trends. Once Information is made available to the Company, the Company undertakes the following commitments in relation to such Information:

- Ensure Information is accurate and updated periodically as required;
- Use Information for lawful purposes only and processes it in a way as to protect the Information against unauthorized or illegal access by internal or external parties;
- Restrict and monitor access to any Information that may contain sensitive data and train employees in online privacy and security measures;
- Safeguard against losses of such Information, including corrupted or compromised data; and
- Maintain strict data protection practices and procedures as well as to establish clear procedures for reporting privacy breaches or data misuse as identified by the Company or its agents.

Practices. The Company has implemented certain practices that are regularly reviewed to ensure the Company's actions are compatible with the objectives stated in this Policy. These practices currently include:

- *IT Infrastructure*. The Company's IT infrastructure is comprised of on-premise applications, cloud hosted applications and an internal corporate network. Data centers have redundant network connections, power backup and physical access controls. All applications are backed up nightly with weekly backups stored off site. Critical applications have redundant instances for the purpose of failover at secondary data center locations. Cloud hosted applications are vetted based on their criticality to the business and the sensitivity of information they manage. The Company also requires that business critical cloud applications have SOC certifications. In addition, all cloud vendors must meet a minimum-security profile. Backups are also maintained for critical cloud applications. The internal corporate network provides access and connectivity for employees, vendors, contractors to business and operational support systems and resources. Core network elements are designed in redundant configurations. Remote access is configured through a VPN with multiple interconnect points.
- *Prevention and Security*. The Company's comprehensive approach to security demonstrates the Company's commitment to securing applicable data and information. The Company leverages firewalls

for all internet access points and such firewalls are updated in near-real time by the vendor to protect against threats. All major corporate internet access points are secured and monitored 24x7x365. The Company is notified if any new or potential threats are found.

- *Employee Training and Awareness.* The Company requires all employees to undergo cyber security training created by a leading cyber security training and awareness platform. Internal phishing campaigns are conducted throughout the year to measure employee awareness. Cyber security emails are sent to all employees periodically to keep cyber security top of mind.
- *Security Audits*. The Company employs third party security experts to annually conduct security audits. The audits include external penetration tests, internal vulnerability assessments and wireless testing. Audit recommendations are tracked and addressed by the IT team.
- *Security Council*. The Company has formed an internal security council to track security initiatives. In addition to tracking initiatives, the purpose is to create an open forum to identify new security concerns that may otherwise go unaddressed. The security council is chaired by the CIO with cross functional members from our Engineering, Operations and IT departments.

Summary. At every stage, the Company will seek to advise and cooperate with customers, vendors, industry experts and employees to address any issue or concern that may arise which could impact the Company's security and data protection protocol of sensitive Information. The Company also encourages its customers, sub-contractors and suppliers to adopt similar policies and objectives.