Radius Global Infrastructure, Inc.

Data Protection, Privacy and Cybersecurity Policy

(Approved February 25, 2022)

Radius Global Infrastructure, Inc. and its subsidiaries (collectively, the "Company") sets forth the following Data Protection, Privacy and Cybersecurity Policy (the "Policy"). This Policy outlines measures taken by the Company's management and employees to treat data and information of its employees, tenants, customers, partners and other interested parties (the "Information") 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 Online Privacy Policy available here: https://www.radiusglobal.com/static-files/dedcfca9-93aa-4d9e-810b-ddca7a23a9e2.

1. The Company strives to closely monitor its security and data protection protocols in order to ensure continual and constant evolution of security measures, including fine tuning security configurations and monitoring industry tools and trends.

2. The Audit Committee of the Company's Board of Directors oversees the Company's policies and procedures with respect to risk assessment and risk management, including with respect to information technology, cybersecurity, and data privacy with the Audit Committee providing periodic reports to the full Board of Directors.

3. An employee-led team is charged with tracking IT, data protection, privacy and cybersecurity initiatives and to create an open forum to identify new security concerns that may otherwise go unaddressed, to the Company's executive management to consider and implement and discuss, when appropriate, with the Audit Committee.

4. Once Information is made available to the Company, the Company undertakes the following commitments in relation to such Information:

   - Use Information for lawful purposes only and process it in such ways so 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 privacy and security measures; 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.

5. 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:

   - Requiring all employees to undergo annual 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;
   - Leveraging layered email filtering capabilities to ensure malicious emails are blocked. In addition, the Company utilizes SPF, DKIM & DMARC for email security;
   - Internal network traffic is encrypted using a Virtual Private Network (VPN); leveraging firewalls for all internet access points and such firewalls are updated in near-real to protect against threats. All major corporate internet access points are secured and monitored 24x7x365. In addition, the Company maintains a Security Operations Center (SOC) Team to monitor network traffic 24x7. The Company is notified if any new or potential threats are found;

- Engaging 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;
- Using an IT infrastructure comprised of on-premise applications, cloud hosted applications and an internal corporate network and using data centers that have redundant network connections, power backup and physical access controls;
- Backing up all applications (including critical cloud applications) nightly with weekly backups stored off site, ensuring critical applications have redundant instances for the purpose of failover at secondary data center locations, and vetting applications based on their criticality to the business and the sensitivity of information they manage;
- Requiring that business critical cloud applications have SOC certifications and that cloud vendors meet a minimum-security profile; and
- Providing internal network access and connectivity for employees, vendors, contractors with core network elements designed in redundant configurations. Additionally, providing remote access that is configured through a VPN with multiple interconnect points.