

Business Internet Acceptable Use Policy

Effective Date: August 1, 2026

This Acceptable Use Policy ("AUP") applies to all Internet access and related services ("Services") provided by Third Generation of Pennsylvania LLC ("Provider") to its business customers ("Customer"). This AUP is incorporated into and forms part of Provider's Business Internet Service Terms and Conditions.

Customer is responsible for ensuring that its employees, contractors, guests, users, and others accessing the Services through Customer comply with this AUP.

1. Lawful Use

Customer may use the Services only for lawful business purposes and may not use the Services to violate any applicable law, regulation, court order, or third-party legal right.

2. Prohibited Activities

Customer may not use, or permit others to use, the Services to:

- transmit, store, publish, or distribute unlawful material;
- infringe copyrights, trademarks, intellectual property, privacy, or other legal rights;
- send unlawful spam, unsolicited bulk communications, or fraudulent messages;
- distribute viruses, malware, ransomware, or other malicious code;
- gain or attempt to gain unauthorized access to any account, computer, system, or network;
- conduct malicious scanning, probing, denial-of-service attacks, or similar activities;
- intentionally interfere with or disrupt the operation or security of any network, system, or service;
- impersonate another person or entity, forge communications, or engage in fraud or deceptive activity;
- use the Services in connection with conduct that creates a material security risk to Provider, an Underlying Provider, or other users; or
- use the Services in a manner that materially interferes with the reasonable use of Provider's or an Underlying Provider's network by others.

3. Network and Security Responsibility

Customer is responsible for maintaining reasonable security for its networks, systems, accounts, equipment, and devices connected to the Services.

Customer must take reasonable steps to prevent unauthorized use of the Services and must reasonably cooperate with Provider in responding to security incidents, abuse complaints, or network threats associated with Customer's connection.

Customer is responsible for traffic originating from its network, except to the extent caused by Provider.

4. Network Management

Provider and its underlying carriers, telecommunications providers, Internet service providers, and other network vendors ("Underlying Providers") may use commercially reasonable network-management and security practices to protect network integrity, mitigate threats, respond to congestion or abuse, and maintain reliable service.

Such measures may include temporarily blocking or limiting traffic that reasonably appears malicious or materially harmful to network operations.

5. Violations and Enforcement

Provider may investigate suspected violations of this AUP and may take reasonable action necessary to protect customers, networks, systems, or third parties.

Depending on the nature and severity of the violation, Provider may:

- notify Customer and request corrective action;
- block or restrict affected traffic;
- temporarily suspend affected Services; or
- terminate Services for material or repeated violations in accordance with the Business Internet Service Terms and Conditions.

When reasonably practicable, Provider will give Customer notice and an opportunity to correct a violation before suspending or terminating Services.

Provider may take immediate action without prior notice when reasonably necessary to address unlawful activity, fraud, an active cybersecurity threat, material network disruption, an emergency, or a requirement imposed by law or an Underlying Provider.

6. Abuse Complaints and Cooperation

Customer agrees to reasonably cooperate with Provider regarding legitimate abuse, security, or legal complaints relating to Customer's use of the Services.

Provider may provide information or take action when required by applicable law, court order, governmental authority, or other lawful process, subject to Provider's applicable privacy obligations.

7. Changes to this AUP

Provider may update this AUP from time to time to address changes in law, technology, security threats, network requirements, or requirements imposed by Underlying Providers.

Provider will provide notice of material changes when required by the Agreement or applicable law.

8. Contact

Questions regarding this AUP or reports of suspected abuse may be directed to:

Third Generation

Abuse/Security: abuse@3genusa.com

Support: support@3genusa.com

Phone: 412-489-1100

This AUP should be read together with Provider's Business Internet Service Terms and Conditions. If there is a conflict between this AUP and those Terms, the order-of-precedence provisions in the Terms will control.