

BIG BEND TELEPHONE COMPANY, INC.

ACCEPTABLE USE POLICY

Effective Date: [DATE]

BBT (“we,” “us,” or “our”) has adopted this Acceptable Use Policy (“AUP”) to promote the lawful, secure, and responsible use of BBT's Internet services and to protect BBT's network, systems, customers, employees, and other users.

This AUP applies to customers and other users of BBT's Internet services (“Service”). It is incorporated into and forms part of the terms governing the applicable Service. Customers are responsible for ensuring that anyone who uses the Service through their account complies with this AUP.

This AUP should be read together with BBT's applicable Terms and Conditions, Network Management Policy, Privacy Policy, and Digital Millennium Copyright Act (“DMCA”) Policy, as applicable.

1. LAWFUL AND RESPONSIBLE USE

The Service may be used only for lawful purposes and in a manner that does not harm BBT's network, systems, equipment, customers, employees, or other persons.

You may not use, or permit others to use, the Service to:

- Violate any applicable federal, state, local, or other law or regulation;
- Engage in or facilitate fraud, phishing, impersonation, deceptive practices, or other unlawful activity;
- Threaten, stalk, harass, intimidate, or unlawfully invade the privacy of another person;
- Transmit, distribute, publish, store, or otherwise make available material that violates applicable law or infringes the legal rights of another person;
- Collect or attempt to collect another person's personal information without authorization or otherwise in violation of applicable law;
- Impersonate another person or entity, falsify sender or identifying information, forge digital or electronic signatures, or otherwise conceal or misrepresent the source of a communication for a fraudulent or unlawful purpose; or
- Use the Service in violation of the applicable rules, policies, or terms governing a network, system, website, application, or service accessed through the Service.

2. ABUSIVE OR DISRUPTIVE CONDUCT

Customers and users must interact with BBT employees, representatives, contractors, and other customers in a manner that does not threaten their safety or materially interfere with BBT's ability to conduct its normal business operations or provide service to its customers.

Prohibited conduct includes:

- Threatening, intimidating, harassing, or verbally abusing BBT employees, representatives, contractors, or other customers;
- Directing obscene, discriminatory, threatening, or abusive language or communications toward BBT personnel or other customers;
- Making repeated, excessive, or intentionally disruptive telephone calls, emails, messages, service requests, or other communications that materially interfere with BBT's normal business operations or the ability of BBT personnel to assist other customers;
- Continuing a pattern of abusive, threatening, or harassing communications after being asked to stop the conduct;
- Engaging in conduct intended to disrupt, obstruct, or interfere with BBT's customer service, technical support, employees, facilities, or normal course of business;
- Engaging in conduct at BBT facilities or service locations that threatens the safety of BBT personnel, contractors, customers, or other persons; or
- Using the Service or BBT's customer-service channels to threaten, harass, intimidate, or abuse another person.

Nothing in this section prohibits a customer from making a good-faith complaint, disputing a charge, requesting technical support, reporting a service issue, or otherwise communicating with BBT regarding the customer's account or Service. The frequency of legitimate communications, standing alone, will not constitute a violation of this AUP.

3. NETWORK AND SECURITY

You may not use the Service in a manner that disrupts, damages, compromises, or interferes with BBT's network or systems or another person's use of a network or service.

Prohibited activities include:

- Interfering with, restricting, inhibiting, or degrading another user's ability to access or use the Service;
- Interfering with or disrupting BBT's network, systems, servers, equipment, or facilities;
- Conducting or facilitating denial-of-service attacks, network flooding, service overloading, or similar attacks or disruptions;
- Introducing, transmitting, or distributing viruses, worms, Trojan horses, spyware, malicious code, or other harmful software or components;
- Accessing or attempting to access another person's computer, account, system, network, software, or data without authorization;
- Circumventing or attempting to circumvent authentication, security controls, access restrictions, or other protective measures;
- Conducting unauthorized probing, scanning, penetration testing, or other attempts to identify or exploit vulnerabilities;
- Using or distributing tools primarily for unauthorized access to or compromise of networks, systems, accounts, or data;
- Altering, modifying, tampering with, damaging, or interfering with BBT-owned equipment or network facilities without BBT's authorization; or

- Using an IP address, network configuration, or protocol in a manner not authorized for the Customer's Service plan, including configuring a static IP address unless permitted by BBT.

Nothing in this AUP prohibits legitimate security measures used to protect a customer's own network or devices, such as firewalls, parental controls, antivirus software, or other reasonable cybersecurity tools.

4. EMAIL, MESSAGING, AND SPAM

You may not use the Service to transmit or facilitate unsolicited bulk communications, spam, or other communications that interfere with or adversely affect BBT's network or other users.

Prohibited activities include:

- Sending unsolicited bulk or commercial email or messages in violation of applicable law;
- Sending excessive volumes of substantially similar, empty, or disruptive messages;
- Using automated systems to harvest email addresses, account names, screen names, or other identifiers without authorization;
- Collecting responses to unsolicited bulk communications;
- Falsifying, altering, or removing message headers or other identifying information;
- Using BBT's name, network, addresses, or other identifiers in a false, misleading, or unauthorized manner; or
- Using BBT's Service or network to facilitate spam, phishing, fraudulent communications, or similar abusive activity.

BBT may use reasonable measures to identify, filter, block, or otherwise address spam, malicious communications, and other network-security threats consistent with BBT's Network Management Policy.

5. INTELLECTUAL PROPERTY

You may not use the Service to infringe copyrights, trademarks, patents, trade secrets, or other intellectual property or proprietary rights.

BBT's procedures for notices of alleged copyright infringement, including notices submitted under the Digital Millennium Copyright Act, are addressed in BBT's separate DMCA Policy, available on BBT's website.

BBT may take action regarding alleged or repeated infringement as provided in its DMCA Policy, applicable Terms and Conditions, and applicable law.

6. RESALE AND UNAUTHORIZED USE OF SERVICE

You may not resell, redistribute, or commercially provide the Service to third parties unless expressly authorized by BBT or permitted under the applicable Service plan or agreement.

Customers may not make the Service available outside the premises or service location in a manner that constitutes unauthorized resale or redistribution of the Service.

Use of the Service must comply with the applicable Service plan and any service-specific restrictions or requirements.

7. CUSTOMER RESPONSIBILITIES

Customers are responsible for use of the Service through their accounts, including use by household members, employees, guests, or other persons to whom they provide access, subject to applicable law.

Customers are responsible for taking reasonable measures to:

- Protect account usernames, passwords, and other credentials from unauthorized access;
- Secure Customer-owned equipment and devices connected to the Service;
- Maintain appropriate security protections, such as current operating-system and software updates, firewalls, and anti-malware protections, as appropriate;
- Prevent unauthorized persons from accessing or using the Service through the Customer's account or network; and
- Promptly address compromised devices or accounts that may adversely affect BBT's network, systems, Service, or other users.

Customers should promptly notify BBT if they become aware of unauthorized use of their BBT account or other circumstances that may compromise the security of the Service.

8. NETWORK USAGE AND MANAGEMENT

Customers may not use the Service in a manner that materially interferes with BBT's ability to provide reliable service to other customers or that causes material harm to BBT's network or systems.

BBT's practices concerning network management, congestion management, network security, performance characteristics, and other network-management matters are described in BBT's Network Management Policy.

Nothing in this AUP is intended to establish a particular data allowance, usage limit, performance level, or network-management practice. Any applicable Service characteristics or limitations are governed by the customer's Service plan and BBT's Network Management Policy.

9. ENFORCEMENT

BBT may investigate suspected violations of this AUP and take reasonable action to protect its network, systems, employees, contractors, customers, and other users.

Depending on the nature, circumstances, and severity of a violation, BBT may take appropriate action consistent with the applicable Terms and Conditions and applicable law, including:

- Providing notice of the suspected violation and requesting corrective action;
- Requiring a customer to cease abusive, threatening, harassing, or disruptive conduct;
- Requiring communications with BBT to occur through a designated method or point of contact when reasonably necessary to address a pattern of abusive or disruptive communications;
- Blocking or restricting harmful, malicious, or abusive network traffic;
- Temporarily suspending affected Service;
- Removing or disabling access to material hosted on systems controlled by BBT, where appropriate; or
- Suspending or terminating Service where warranted.

BBT may take immediate action without prior notice when reasonably necessary to protect the safety of its employees, contractors, customers, or others; protect the security or integrity of its network, systems, or facilities; prevent material disruption to its operations or services; respond to unlawful activity; or comply with applicable law or legal process.

BBT is not obligated to monitor all customer activity or communications for violations of this AUP.

BBT may cooperate with law enforcement or other governmental authorities and respond to valid legal process as required or permitted by applicable law. BBT's collection, use, and disclosure of customer information are further addressed in BBT's Privacy Policy.

10. REPORTING VIOLATIONS

Customers and other persons may report suspected violations of this AUP to BBT using the contact information provided on BBT's website.

Copyright infringement notices should be submitted in accordance with BBT's DMCA Policy.

11. CHANGES TO THIS ACCEPTABLE USE POLICY

BBT may update this AUP from time to time to reflect changes in its services, network, practices, technology, security risks, or applicable legal or regulatory requirements.

BBT will post the current version of this AUP on its website. BBT will provide any additional notice of material changes required by applicable law or the applicable Terms and Conditions.

The Effective Date identified at the beginning of this AUP indicates when the current version became effective.

12. CONTACT US

If you have questions regarding this Acceptable Use Policy or wish to report a suspected violation, please contact BBT using the current contact information available on BBT's website.

Notices of alleged copyright infringement should be submitted in accordance with BBT's DMCA Policy, available on the Legal page of BBT's website.