

## **ACCEPTABLE USE POLICY**

Santel Communications Cooperative Inc., its affiliates and wholly owned subsidiaries (collectively "Santel") have established an Acceptable Use and Network Management Policy ("AUP") for the protection of Santel and its customers for the use of its products and services. Santel can be contacted at (605) 796-4411 regarding any questions you have about this AUP, Santel, or its products and services. By using services provided by Santel, you agree to be bound by the terms of this AUP.

**Internet Service.** This AUP applies to customer use of any Santel Internet service regardless of technology or the Internet-based application utilized. It is not acceptable to use the Santel network for any fraudulent purpose or other purpose that violates local, state or federal laws or to transmit communications that might be highly offensive or damaging to any recipients or to use the service in a manner that is unintended. This includes, but is not limited to, copyrighted material, material legally judged to be threatening or obscene, or material protected by trade secrets. It is not acceptable to interfere with, violate, circumvent, misuse, distribute or disrupt network users, equipment or services. A customer may not:

1. Use any Internet service or permit, whether intentionally or unintentionally, through act or omission, the use of Internet service for unlawful purposes or purposes that Santel believes to be unacceptable.
2. Use any Internet service to transmit, post or receive material that is threatening, abusive, libelous, defamatory, obscene, pornographic, or otherwise in violation of any local, state, federal or international law or regulation.
3. Transmit, whether intentionally or unintentionally, any information or software that contains a virus, worm, Trojan Horse, or other harmful component.
4. Transmit or download any information, software or other material that is protected by copyright or other proprietary right without the permission of the person owning that protected right.
5. Transmit SPAM or other bulk email.
6. Add, remove, or modify identifying network heading information (aka "spoofing") in an effort to deceive or mislead; or any impersonation of another person using forged headers or other improper identifying information.
7. Engage in any activity which would compromise customer privacy or system security or gain access to any system or data without required permission (e.g. "hacking") of the owner.
8. Engage in any activity which would result in third-party charges to Santel.
9. Resell or otherwise share Santel' Internet service, account information or passwords.

10. Attempt to obtain unauthorized access to any network or account. This includes accessing data not intended for end user customers, logging into a server or account without being expressly authorized to access or probing the security of other networks.
11. Attempt to interfere with the service of others including users, hosts and networks. This includes “denial of service” attacks, “flooding” of networks, deliberate attempts to overload a service and attempts to “crash” any host.
12. Distribute Santel Internet services beyond the scope of your end-user account.
13. Attach equipment, accessory, apparatus, circuit or devices that are harmful to the network and are attached to or connected with Santel facilities.
14. Use Santel’s Internet service for web or email hosting without making special written subscription arrangements with Santel.

Santel does not screen in advance any specific content accessible using its Internet service. Santel reserves the right but does not assume the responsibility, to block or limit access to content that violates this AUP. Santel shall not unjustly or unreasonably block access to lawful content, applications, services or non-harmful devices, subject to reasonable network management. Santel disclaims any liability for any act or omission with regard to Internet content the customer finds objectionable or unsuitable. Use of information accessed by the Internet is at customer’s own risk.

Santel disclaims any responsibility for the accuracy, privacy or quality of the information. By using the Internet service, the customer agrees to hold Santel harmless for content accessed using the Internet service.

A customer may not use Santel’s Internet service for web or email hosting without making special written subscription arrangements with Santel.

Santel reserves the right to disconnect or limit any account access to the Internet that in the opinion of its system administrator is a threat to the security or lawful operation of the Internet service or the service’s software and/or hardware or that repeatedly violates the terms of this AUP.

The customer agrees to indemnify and hold Santel harmless for any and all claims, damages, losses, expenses (including attorneys’ fees and other legal expenses) resulting from the customer’s use of Santel’ Internet service whether or not such use is found to be in violation of any statute, regulation or rule.

### **Inappropriate Usage**

Santel or other relevant authorities may determine inappropriate usage of this account and the privilege may be revoked at Santel’s discretion. Should this occur, Customer will be notified in writing of this action.

## **Change of Status**

Santel will occasionally require new registration and account information by Customer to continue this service. In addition, Customer shall promptly notify Santel in writing of any changes in the account information.

## **SPAM Policy**

Santel has zero tolerance for Unsolicited Broadcast Email and Unsolicited Commercial Email (“UBE/UCE”, commonly known as “Spam”) whether originating from customers, from customers’ customers, or from customers who provide services which are used to support spam.

*Definition of Spam.* Santel defines spam as unsolicited broadcast or commercial email that is sent to addresses that do not affirmatively and verifiably request such material from that specific sender, including but not limited to advertising, surveys, information pieces, third party spamming, website addresses, sales, and auctions.

*Our Policy.* Santel customers and customers of Santel’s customers are prohibited from sending and shall not allow their connection to Santel Internet to be used for sending spam. Mail senders are required to maintain records that verify, on a case-by-case basis, that explicit affirmative permission was obtained from recipients before mailing. Lack of such records can be considered, at Santel’s sole discretion, proof that permission was not obtained.

Santel customers are responsible for ensuring that they, their customers, and their respective agents and contractors abide by this policy. Santel customers will be held responsible for all traffic sent through their connection to Santel Internet. Customers are also responsible for ensuring that they do not advertise or promote themselves through spam.

If Santel receives a complaint, it will be forwarded to the customer for a response and complete resolution. If it is determined that the customer has used a Santel Internet connection to support spam, their account is subject to immediate suspension and/or termination.

*Why this policy?* Unlike senders of traditional junk mail who are required to pay for envelopes, materials and postage, senders of spam can, given the nature of the Internet, impose undue financial burdens on the recipients of their messages at little or no cost to themselves. These include things such as the cost imposed on the recipients in bandwidth to deliver the spam, and time and money wasted in filtering out and deleting spam and changing email addresses. Santel believes that users of the Internet should not be forced to incur such expenses without their consent. As a result, Santel believes that the elimination of spam will result in a better and less expensive Internet experience for all Internet users and will allow Santel to provide better and more efficient service to its customers.

*Reporting Spam.* If you have been spammed by one of our customers, please notify us by sending a copy of the message you received to [info@santel.coop](mailto:info@santel.coop). Immediate attention will be given to the matter. Please be aware that it is not uncommon for spammers to hide behind someone else's email account, as well as use mail servers that they do not own. By sending us a copy of the message you received, we will be able to determine enough information to accurately handle the situation. By examining the full message headers of the offending message, useful information can be obtained about the actual sender.

Spam filtering is FREE for each Santel email account. Spam Filtering detects and stops any incoming email that it thinks is junk/spam email. Email messages that are caught by Spam Filtering are available for a customer to view and are stored for 2 weeks before they are automatically deleted.

## **NETWORK MANAGEMENT POLICY**

Santel commits to the open and non-discriminatory use of the Internet by its customers and commits to use reasonable network management practices to ensure an open Internet. Santel will manage its network and provide access in accordance with the Federal Communications Commission's (FCC's) Rules and in compliance with any future rules adopted by the FCC.

**Transparency.** Santel shall make available public information on its website <https://Santel.coop/terms> regarding its network management practices, performance and commercial terms of its service sufficient for consumers to make an informed choice regarding their use of such services.

Santel will not unjustly or unreasonably prevent or interfere with competition among content, applications, service, or device providers.

**Network Security and Congestion Management.** Santel uses generally accepted technical measures to provide acceptable service levels to all customers, such as application-neutral bandwidth allocation, as well as measures to address service attacks, illegal content and other harmful activities to protect network integrity and reliability. During periods of congestion, Santel may engage in blocking, throttling, and/or prioritizing traffic based on category. If traffic cannot be properly categorized, its priority will be affected. Santel manages the bandwidth of the uplinks to prevent experiencing network congestion.

Santel reserves the right to prioritize traffic based on real time and non-real time applications during heavy congestion periods based on generally accepted technical measures. Santel reserves the right to set speed thresholds on the amount of data you as a customer can upload and download within stated time periods. If you exceed these thresholds, Santel may temporarily limit the speed at which you can send and receive data over the Santel access network. Santel may use other traffic management and prioritization tools to help ensure equitable access to the Santel network for all customers. Excessive bandwidth or hardware usage that adversely affects Santel's

ability to provide its Internet or any other service may result in additional account management and fees.

Santel reserves the right to monitor customer usage and evaluate on an individual account basis bandwidth or hardware utilization to efficiently manage the performance of the network to ensure a sustainable quality broadband service is provided. Peak network usage is between 4 pm and 11 pm Monday – Friday and 10 am – 11 pm Saturday and Sunday. During peak usage times, priority is given to applications such as browsing, email, streaming, instant messaging, gaming and VoIP. The customer further agrees that Santel has the right to disclose any information it deems necessary to satisfy any legal or operational requirements.

Any IP address assigned to a customer on either a dynamic or static basis remains the property of Santel and may not be appropriated for any use other than as intended by Santel or transferred to any other party.

Devices connecting to Company's network must conform to general public standards and be non-harmful to the network.

Santel provides its own methods to secure and protect its Internet service. Such action is not a substitute for the customer providing his/her own security or protection. Santel specifically disclaims any liability for any breach of security or any harm to customer's computing system while connected to Santel' Internet service.

Congestion due to malfunctioning hardware and/or software will be remedied as quickly as network engineers can diagnose and identify the offending hardware / software.

Congestion due to malice will be remedied using any technique available, including protocol-aware filtering and rate-limiting, to control and limit the offending source. Santel may seek criminal charges against those who inflict network malice. Santel may also attempt to recover costs incurred from network malice.

**Performance Characteristics.** The advertised speed of Santel’s Internet service is the maximum bandwidth throughput that is available and achievable with the technology utilized by Santel. Our customer serving networks are comprised of various access platform technologies that deliver Internet service. Some characteristics of generally available Internet access by type:

- **FTTP** (Fiber-to-the-premise) supports best effort up to 1000 Mbps, less than 50ms latency, depending on service level subscribed. Any access platform technology used or supported to provide Internet service may change at any time at the sole discretion of the Company.

Product	Expected & Advertised <sup>1</sup>	Actual Sustained (Download / Upload)	
Starter	25/3	23.6 – 24.5 Mbps	2.6 – 2.9 Mbps
250	250/250	235.2 – 245.7 Mbps	243.2 – 243.7 Mbps
500	500/500	472 – 490.2 Mbps	472.2 – 486.5 Mbps
750	750/750	708.8 – 735.8 Mbps	708.1 – 729.75 Mbps
1000 (Gig)	1000/1000	881.1 – 940.0 Mbps	870.4 – 938.8 Mbps

Typical latency	2-50 milliseconds
Typical Jitter	0-4
Typical Packet Loss	0

Several factors may affect the actual bandwidth throughput of Santel’s Internet service offerings. This includes but is not limited to the distance between service point and Santel’s central office as well as the customer’s computer, modem or router used. Internet traffic and activity during peak usage periods may also impact the available bit rate. We have provided a link to a locally hosted speedtest, to compare your sample results. <http://santel.speedtest.net>

**Electronic Communications Privacy Act (ECPA) Notice.** Customers are hereby notified that Santel does NOT offer the same degree of privacy for email or files that the customer expects from regular paper mail.

**Digital Millennium Copyright Act (DMCA) Policy.** When Santel receives a notice from a copyright holder or its authorized representative regarding an alleged violation of law by someone using an IP address identified as belonging to Santel, the following actions will be initiated:

---

<sup>1</sup> Symmetric performance, unless noted otherwise. Speed tier performance represented in downstream / upstream bandwidth, in Megabits per Second.

1. Santel personnel will review the address to determine whether the address is in use by Santel or by one of its owners or affiliates. If the address has been assigned to an entity other than Santel, the DMCA notice will be forwarded to that entity for review and any action or response.
2. If the address is assigned and used by Santel or one of its customers, Santel personnel will attempt to identify the user. If the offender cannot be identified, the Santel Agent listed on Santel's Internet site, currently Pam Kopfmann, will be notified so she can respond accordingly to the copyright holder or its agent. If the offender is identified, Santel will take the following actions:

a. If the offender is an employee, the responsible supervisor will be notified and appropriate disciplinary action may be warranted. A copy of the violation will be filed by HR in the employee's personnel file.

b. If the offender is a customer, the customer will be notified by telephone or email of the offense. If it is a first-time offense, the customer will be notified and advised that an alleged violation of copyright law has been received and that any further violations could affect the customer's access to the Internet. Notification of a second offense will result in the same action. A third offense will result in notice that Internet service will be restricted for ninety (90) days to limit the ability to violate the law. A fourth offense will result in the termination of Internet service.

**Notice of Copyright Infringement:** If you are a copyright owner (or an agent of a copyright owner) and believe any user material posted on our sites infringes upon your copyrights, you may submit a Notification of Claimed Infringement under the Digital Millennium Copyright Act ("DMCA") by sending the following information to our Designated Copyright Agent:

1. Clear identification of the copyrighted work;
2. Identification of the material allegedly copying the original work, and information reasonably sufficient to allow us to locate the material;
3. Accurate contact information of the person submitting the claim;
4. Statement that the claim is being made with the good faith belief that the alleged use is not authorized by the copyright owner;
5. A statement that the claim is accurate, and under penalty of perjury, the complaining party is authorized to act on behalf of the copyright owner;
6. Signature of the person submitting the claim.

You can submit your Notification to us using the following contact information and Designated Agent:

Company legal name  
Designated Agent  
Mailing address of agent  
Telephone

Santel Communications Cooperative, Inc.  
Attn: Pam Kopfmann  
PO Box 67, Woonsocket, SD 57385  
605-796-4411

Fax  
Email

605-796-4419  
[notices@Santel.coop](mailto:notices@Santel.coop)

The Designated Copyright Agent should be contacted **only** for notices regarding alleged copyright concerns. All other feedback, comments, questions, and other communications should be directed to us through the General Contact Information below.

Santel provides Spam filtering with each customer's email address. Details of this service are listed on Santel's website. Santel will not ask you for your password in an unsolicited telephone call or email. If you believe your password has been compromised, you should immediately change your password to prevent the unauthorized use of it.

**Discrimination.** Santel shall not unreasonably discriminate in transmitting lawful network traffic over a consumer's broadband Internet access service, subject to reasonable network management practices.

**Commercial Pricing.** Please click on the following website link for pricing information including monthly prices, usage-based fees, and fees for early termination or additional network services: <https://santel.coop/services/internet/>

**Privacy Policy.** Please click on the following website link to view Santel's complete privacy policy: <https://santel.coop/terms-conditions/>. Santel does not generally inspect network traffic. Certain traffic information is retained and stored for specific periods of time as required by state or federal law. This includes information stored and provided to law enforcement as it relates to information requested by law enforcement pursuant to national security and/or criminal statutes and Acts. Santel does not otherwise store, use, or provide traffic information for non-network management purposes.

**Impact of Non-Broadband Internet Access Service Data Services.** The Company does not currently offer any non-Broadband Internet Access Service (non-BIAS) Data Services. Accordingly, customers' broadband experiences will not be impacted.

**Contact Information.** If you have any questions regarding this policy, please contact Santel customer service at: (605) 796-4411.

Last modified 12/1/2022