Acceptable Use Policy

Document: Acceptable Use Policy	Effective Date: 10/1/2022
Document ID: IS.002	Last Revised Date: 05/20/2024

1. Purpose

The purpose of this Acceptable Use Policy is to outline the acceptable uses of Brightspeed's information assets. These rules are intended to protect Brightspeed assets, resources, networks, and employees from cybersecurity and other risks, including exposure to malware, compromised systems and services, and legal liability.

2. Scope

This document applies to information, information systems, electronic and computing devices, applications, and network resources ("Information Assets") used to conduct business on behalf of Brightspeed. All Brightspeed employees, contractors, must comply with this document. For the purposes of this Policy, the term "Brightspeed" shall include all operating companies owned or controlled by Connect Holding LLC, including without limitation all incumbent local exchange carrier and non-regulated services provider entities.

3. Policy

3.1 General Use of Corporate Networks and IT Resources

Users of Brightspeed's network and IT resources shall:

- Comply with all applicable U.S. and international laws, rules, and regulations.
- Comply with contractually agreed upon security obligations and requirements.
- Comply with all Brightspeed information security policies, standards, guidelines, regulations, procedures, and rules.
- Respect and protect the intellectual property rights of Brightspeed, its customers, and other users within Brightspeed, and include all laws regarding the distribution, use, and acquisition of copyrighted content.
- Avoid sharing passwords or accounts with anyone, including trusted friends or family members. Note that the Authorized User is responsible for any actions performed using their account.
- Be respectful and professional in all online communications using Brightspeed's network and IT resources.
- Only access information assets that they are authorized to access and that are necessary to do their job.
- Use corporate email accounts, internet IDs, and web pages only for corporate communications.
- Follow all corporate cybersecurity guidelines and protect against the propagation of viruses and other malware. Users should exercise extreme caution when opening email attachments received from outside or unknown senders.
- Only use Brightspeed-approved technologies when working in Brightspeed's environment.

3.2 Privacy

- The use of Brightspeed's information assets such as its network is monitored by Brightspeed's IT and Security teams and there should be no expectation of privacy by users.
- The data and work product created on or using Brightspeed corporate systems, applications, and platforms are the property of Brightspeed.

3.3 Prohibited Usage of Brightspeed's IT Resources

The following uses of Brightspeed's resources are prohibited. Violation of this policy may lead to disciplinary action up to and including termination. Certain prohibited activities may also lead to civil or criminal liability. Under no circumstances is an employee of Brightspeed to:

- Use Brightspeed's network, applications, or systems to engage in any unlawful or impermissible activity.
- Circumvent Brightspeed security measures or those of Brightspeed customers, vendors, or other entities.
- Interfere with the proper operation of Brightspeed's network or introduce any software or malicious code that propagates viruses or malware, or that generates sustained high volume network traffic that hinders network performance.
- Violate the intellectual property rights of any person or entity that are protected by copyright, trade secret, patent or other similar laws or regulations, including without limitation, the use, installation, or distribution of "pirated" or other unlicensed software.
- Disclose Brightspeed's restricted, confidential as defined in the Information Classification Standard, which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, customer lists, technical product information, computer software source codes, computer/network access codes, business relationships, or other information which by its nature or use is reasonably viewed as confidential or sensitive.
- Visit internet sites that contain obscene, hateful or otherwise objectionable material.
- Make or post indecent remarks, proposals or materials on the internet.
- Download any software or electronic files without implementing anti-virus protection measures approved by Brightspeed.
- Intentionally use, distribute or create viruses, worms or other malicious software.
- Access Brightspeed systems or data from a country or region identified on the High Risk Countries List
- Travel to countries/regions identified on the Brightspeed High-Risk Countries List with Brightspeed Data/Devices
- Operate a business, usurp business opportunities, organize political activity or conduct activity for personal gain.

- Imply that the user is representing, giving opinions or otherwise making statements on behalf of Brightspeed without prior authorization or use Brightspeed trade names, logos, or trademarks without prior written authorization
- Use a personally-owned workstation or mobile device for business purposes, or to create or store restricted, confidential, or commercially sensitive information.
- Introduce malware or information leakage or data loss into the Brightspeed network, or use USB (Universal Serial Bus) flash drives or any other portable storage media unless specifically authorized by the Brightspeed IT and Enterprise Cyber Security departments.
- To implement or install, without explicit approval by the authorized parties, software or other technology to prevent opening gaps that put critical systems and cardholder data at risk.
- Use any online storage service (e.g., Dropbox, Google Drive, iCloud etc..) except for the Brightspeed provided Microsoft OneDrive.
- Modify security software, security tools, or configuration on Brightspeed managed devices.
- Users may not use unapproved communication and collaboration tools and/or methods including SMS/MMS.
- Use of QUIC protocol
- Use of any software, IT hardware, or tools not approved by Security Risk Management

3.4 Email and Communications Activities

Users of Brightspeed's email and communication resources may not:

- Send unsolicited email or other types of electronic messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (spam)
- Use unsolicited emails originating from within Brightspeed's networks or from another internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by Brightspeed or connected via Brightspeed's network
- Solicit emails that are unrelated to business activities or for personal gain
- Send unencrypted restricted or confidential emails in violation of the Cryptographic Management Standard
- Use Brightspeed corporate email accounts for non- Brightspeed business.
- Use SMS or MMS for any business related communications

3.5 Blogging and Social Media

Employees may not, in the course of blogging or posting to social media:

- Reveal any Brightspeed restricted, confidential, or proprietary information, trade secrets, or any other confidential information;

- Engage in any blogging or social media posting that could harm or tarnish the image, reputation, or goodwill of Brightspeed or its employees;
- Make discriminatory, disparaging, defamatory, or harassing comments generally about Brightspeed or other Brightspeed employees; or
- Attribute personal statements, opinions, or beliefs to Brightspeed when engaged in blogging or using social media.
- Expressly or implicitly hold themselves out as representing Brightspeed.

3.6 Secure Information Transfer

Confidential or restricted information must be securely transferred only through authorized methods using encryption or secure file transfer. Confidential or Restricted information may not be electronically transferred in an unencrypted or unprotected format.

3.7 Record Retention

Information storage and retention time frames shall be limited to what is required for legal, regulatory, and/or business purposes in accordance with Brightspeed's Records Retention Policy.

3.8 Information Protection

3.8.1 Information Classification

Personnel must adhere to the information classification Policy/Standard and ensure appropriate measures are taken to protect information commensurate with its value to Brightspeed. The information classification system includes the following categories: Restricted, Confidential, Internal Use, and Public.

See the IS.017 - Information Classification in the IS.004 - Asset Management Standard for additional details.

3.8.2 Information Protection Requirements

The confidentiality, security, and integrity of information must be protected while that information is at rest, in use, and in transit.

3.8.3 Information at Rest

Information is “at rest” when data is physically on computer data storage in any digital form. It refers to data not actively moving from device to device or network to network. The following guidelines apply to safeguard restricted and confidential information at rest (i.e., in storage):

- Restricted and Confidential information must only be stored on encrypted storage devices at rest.
- Store all information on access-restricted and/or access-controlled Brightspeed managed OneDrive or Brightspeed managed SharePoint.
- Dispose of restricted or confidential information only after confirming compliance with records retention laws.
- Restricted data should only be stored on assets specifically approved to store restricted data by IT and Enterprise Cyber Security.

3.8.4 Information in Use

Information is “at use” is data that is currently being updated, processed, erased, accessed, or read by a system or user. It is data that is actively being accessed and used. The following are guidelines to safeguard confidential information in use:

- For access to systems that host confidential information, personnel must request access using an approved access request process/tool and be positively authenticated (i.e., have an established user identity in Azure Active Directory or another authentication source).

- Use restricted or confidential information (such as Social Security numbers) to the minimum necessary to support business operations (e.g., last four digits of social security numbers). Information should be stored only in approved information repositories.

  The use of any AI program, tool, library or other information resource must meet the Brightspeed’s Generative AI Policy and must be approved by Brightspeed Security Risk Management (SRM) team prior to use.

3.8.5 Information in Transit

Information in “transit” is data that is actively moving from one location to another. This is typically data moving across a network but could also be data moving between devices, or other media. Brightspeed-issued encryption solutions should be used to protect the integrity of confidential and commercially sensitive information that will be transmitted outside of Brightspeed.

Other rules to follow:

- Use the secure mail feature by selecting Options > Encrypt > Encrypt Only when composing an email to encrypt the email.
- Password-protect files that contain confidential information (See IS.008 Cryptographic Management Standard).

Restricted information should never be transmitted outside Brightspeed unless approved by IT, Legal, and Enterprise Cyber Security.

4. Document Change Control

Version No.	Revised by	Effective date	Description of Changes
	Sharman Sibia		Initial Draft
	Sharman Sibia	07/24/2023	Added restrictions for SMS/MMS
	Sharman Sibia	05/20/2024	Yearly Update

The owners of this document are Brightspeed Enterprise Cyber Security and the Brightspeed CISO. It is the responsibility of the document owners to maintain, update and communicate the content of this document. Questions or suggestions for improvement must be submitted to the document owner.

4.1 Annual Review

This *Acceptable Use Policy* will be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.