# Supplier Acceptable Use Policy

## 1. Scope

This Brightspeed Supplier Acceptable Use Policy ("AUP") applies to all Brightspeed: information systems, electronic and computing devices, applications, and network resources ("Information Assets") used and/or accessed by Supplier Personnel to conduct business for the benefit of Brightspeed and/or on behalf of Brightspeed. All Brightspeed information and data used or accessed by Personnel is the confidential information of Brightspeed. To the extent applicable to a Supplier, Supplier's employees, agents, personnel, contractors, etc. and the employees, agents, personnel, and contractors, etc. of Supplier's subcontractors (collectively, "Personnel") must comply with this AUP at all times while providing products and services to Brightspeed, as applicable. For the purposes of this AUP, the term "Brightspeed" shall include all operating companies owned or controlled by Connect Holding II LLC d/b/a Brightspeed and its parent company Connect Holding LLC, including without limitation all incumbent local exchange carrier and non-regulated services provider entities. Supplier remains at all times responsible for compliance with this AUP by its Personnel.

## 2. Supplier's Use of Brightspeed Corporate Networks and IT Resources

Suppliers must:

- 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, regulations, procedures, and rules as provided or made available to Supplier and Personnel.
- Respect and protect the intellectual property rights of Brightspeed, its customers, and other users within Brightspeed, including without limitation all laws regarding the distribution, use, exportation, and acquisition of copyrighted and licensed content.
- Avoid sharing passwords or accounts with anyone, including trusted friends or family members. Suppliers are responsible for all acts performed under the account(s) of their Personnel.
- 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.

#### 2.1.1 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.

### 2.2 Prohibited Usage of Brightspeed's IT Resources

The following uses of Brightspeed's resources are prohibited. Violation of this AUP is considered a material breach of all agreements between Supplier and Brightspeed, and if no such agreements exist, then Brightspeed reserves all rights under common law. Certain prohibited activities may also lead to civil or criminal liability. Under no circumstances is a Supplier to permit its Personnel 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.
- 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.
- Attempt to reverse engineer, decompress, disassemble, access the source code, or in any way attempt to gain access to Brightspeed intellectual property, proprietary information, and Brightspeed confidential information which Brightspeed has not provided or permitted access to by Supplier Personnel.
- 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 (ie. spam).

## 2.3 Protection of Brightspeed Information.

This section 2.3 applies in the event an agreement between Supplier and Brightspeed does not include a Security Addendum.

### 2.3.1 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.

### 2.3.2 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.

### 2.3.3 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).