SUPPLEMENTAL SECURITY ADDENDUM FOR THIRD-PARTY REPRESENTATIVES

This Brightspeed Supplemental Security Addendum for Third-Party Representatives ("**Supplemental Rep Addendum**") is incorporated by refence into and forms part of the Brightspeed Security Addendum (accessible at https://www.brightspeed.com/content/dam/brightspeed/ew/documents/ewabout/Security_Addendum_for_Vendors_and_Third_Party_Representatives.pdf) ("**Security Addendum**") to the Master Representative Agreement ("MRA"), Statement of Work ("SOW"), or Service, Product, or Purchase Order ("Order") (together with any appendices, exhibits, annexes, or amendments thereto, the "**Agreement**") executed between Connect Holding II LLC d/b/a Brightspeed or the Brightspeed Affiliate identified in the Agreement ("**Brightspeed**") and the third-party representative ("**Representative**") indicated in the applicable Agreement and is effective as of the effective date of the Security Addendum. Brightspeed enters into this Supplemental Rep Addendum on its own behalf and on behalf of its Affiliates.

Capitalized terms used in this Supplemental Rep Addendum shall have the meanings set forth in this Supplemental Rep Addendum. Capitalized terms used but not otherwise defined herein shall have the meanings given to them in the Security Addendum or the Agreement.

1. Supplemental Security Measures.

In the Provision of the Provided Services, Representative shall implement and maintain (a) a Security Program in accordance with the Security Addendum available at https://www.brightspeed.com/content/dam/brightspeed/ew/documents/ewabout/Security_Addendum_for_Vendors_and_Third_Party_Representatives.pdf and (b) the supplemental security provisions indicated in Section 2 (Security Program Requirements) of this Supplemental Rep Addendum. "**Provided Services**" means any and all products or services provided by Representative to Brightspeed pursuant to the Agreement.

2. Security Program Requirements.

2.1 **Domain Names.** If the engagement requires using a domain name to provide the required service, the following requirements apply:

2.1.1 All Domain Names (DNS) required as part this engagement must be owned and registered by Brightspeed.
2.1.2 Representative can request a new Domain name through their designated Brightspeed contact.

2.2 **Email Services.** Email domains used in the provision of the Provided Services or otherwise to represent Brightspeed shall meet the following minimum requirements:

2.2.1 Adhere to industry email best practices to prevent spam, phishing and spoofing by utilizing SFP, DMARC, and DKIM records.
2.2.2 Use appropriate security tools to mitigate outbound and inbound phishing schemes and spam.
2.2.3 Meet the requirements of the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), if applicable.
2.2.4 Use a designated domain and do not spoof any of the Brightspeed corporate domains.

2.3 **Websites.** Websites deployed as part of the engagement shall meet the following minimum requirements:

2.3.1 Use Web Application Firewalls (WAFs) to prevent common web application exploits.
2.3.2 Block access to websites that do not meet HTTPS (Encrypted) standards.

2.4 **Social Media.** Representative shall notify Brightspeed of any social media accounts used by Representative in the provision of the Provided Services or otherwise to represent Brightspeed at least three (3) days in advance of such use.

2.5 **Payment Card Industry.**

2.5.1 Representative and any Representative Personnel that accepts, stores, or processes payment card information in the provision of the Provided Services shall, at all times, meet all requirements of the latest version of the Payment Card Industry Data Security Standards ("**PCI-DSS**").

2.5.2 If PCI-DSS is applicable to the provision of the Provided Services, Representative shall deliver to Brightspeed (a) a copy of its annual Attestation of Compliance ("**AOC**") with PCI-DSS and (b) a high-level cardholder data environment (CDE) flow diagram that demonstrates that the AOC is sufficiently scoped.

2.5.3 If requested by Brightspeed, Representative shall permit Brightspeed to perform integrity scans on public interfaces to the cardholder data flow to verify Representative's encryption and other PCI-DSS compliance efforts.

2.6 **Security Assessments.**

2.6.1 Representative shall permit Brightspeed, or a third-party auditor designated by Brightspeed, to audit Representatives compliance with this Supplemental Rep Addendum.

2.6.2 Representative shall permit Brightspeed to perform penetration testing and vulnerability scanning on any publicly accessible resources used in the provision of the Provided Services.

2.7 **Vulnerabilities.**

2.7.1 Vulnerabilities identified or reasonably suspected by Representative or by Brightspeed or its third-party auditor must be remediated at the sole cost of Representative without undue delay, and in any event within the timelines listed in *Table 2: Remediation Timelines* below.

2.7.2 If Representative discovers or reasonably suspects a vulnerability that has, will, or is likely to impact the Provided Services, Brightspeed, Brightspeed Data, Brightspeed's network or systems, Brightspeed customers, or consumers, Representative shall notify Brightspeed at vulnerabilitymanagement@brightspeed.com and cybersecurity@brightspeed.com within the timelines indicated in *Table 3: Notification Timelines*, defined based on severity of the vulnerability.

2.7.3 Representative shall perform automated continuous testing against all assets used in the provision of the Provided Services or to access Brightspeed Data or Brightspeed's systems or networks, including servers, computers, and websites. Such testing should use technology that uses current vulnerability signatures to detect new threats.

Table 1: Remediation Timelines

Severity	Description	Remediation Timeline (Calendar Days)	
		External Facing, PCI, CPNI, US Records, or Customer Service Impacting	Internal Facing
Zero-Day/Emergency	The vulnerability is very likely to be exploited and result in compromise of the confidentiality, integrity, and availability of Brightspeed assets or Brightspeed customer assets.	2 Days	5 Days
Critical	Threat actor may gain control of a system/asset, potential leakage of confidential information, lead to further compromise of Brightspeed assets/resources including lateral	15 Days	30 Days

	movement.		
High	Threat actor may gain access to sensitive information, including security settings resulting in potential misuse.	30 Days	60 Days
Medium	Threat actor may be able to collect sensitive information, such as the precise version of software installed.	60 Days	120 Days
Low	Limited risk to host.	90 Days	180 Days

Table 2: Notification Timelines

Severity	**Notification Requirement**
Zero Day	Immediately upon discovery
Critical	24 hours
High	28 hours
Medium	72 hours
Low	Monthly

3. Notifications.

3.1. Notifications of a Security Incident should be sent to cirt@brightspeed.com using the subject line: Security Breach.
3.2. Notifications of a vulnerability should be sent to vulnerabilitymanagement@brightspeed.com and cybersecurity@brightspeed.com using the subject line: Brightspeed Security Vulnerability.

4. Relationship to the Agreement.

4.1. The parties agree that this Supplemental Rep Addendum replaces and supersedes any existing or prior Supplemental Security Addendum to which the Representative may have been subject.
4.2. The parties agree that the Supplemental Rep Addendum is intended to complement and enhance the Security Addendum and its terms shall be constructed to this effect.
4.3. Except as expressly modified herein, the terms of the Security Addendum and the Agreement shall remain in full force and effect.
4.4. To the extent of any conflict or inconsistency between this Supplemental Rep Addendum and the Security Addendum, the provision offering the greater protection to Brightspeed, Brightspeed Data, or Brightspeed networks and systems shall prevail.
4.5. To the extent of any conflict or inconsistency between the Security Addendum, any other document comprised within the Agreement, and the Brightspeed Supplier Portal[1], the order of precedence shall be,

[1] The Supplier Portal can be accessed at https://www.brightspeed.com/ew/about/doing-business-with-brightspeed/.

each when applicable, in descending order: 1) this Security Addendum, 2) the Data Privacy Addendum, 3) the FCC Addendum, 4) the amended master agreement, 5) the Supplier Portal, and 6) any Order or SOW.

4.6. Under no circumstances shall an Order or SOW modify the Security Addendum or this Supplemental Rep Addendum, unless such modification specifically references the term it is overriding and the document containing such modification is signed by both parties.

4.7. This Supplemental Rep Addendum will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Security Addendum or the Agreement.

5. Term. The term of this Supplemental Rep Addendum shall run concurrent with the term of the Security Addendum.

6. General Provisions. Should any provision of this Supplemental Rep Addendum be invalid or unenforceable, then the remainder of this Supplemental Rep Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible; or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. Unless otherwise expressly stated herein, the parties will provide notices under this Supplemental Rep Addendum in accordance with the Security Addendum.