

Facilities Based
Broadband Internet Access Service and VoIP
Systems Security and Integrity Plan
for City of Hudson DBA Velocity Broadband

SYSTEM SECURITY AND INTEGRITY PLAN of City of Hudson DBA Velocity Broadband

The following procedures govern City of Hudson DBA Velocity Broadband's ("Company") compliance with lawful requests for electronic surveillance in conformity with the Communications Assistance for Law Enforcement Act as implemented by Commission's rules.

I. OVERVIEW

Any employee that receives a request from a law enforcement agency or anyone else for any form of electronic surveillance must follow these procedures exactly. Failure to adhere to the procedures set forth herein may result in disciplinary action, including possible termination of employment.

II. ACTIONS AND AUTHORIZATIONS

This VoIP and facilities-based broadband internet access service Systems Security and Integrity Plan ("SSI Plan") establishes the policies and procedures for the supervision and control of the officers, employees' and agents of the Company. It is the policy of the Company to comply with the letter and spirit of all applicable United States electronic surveillance statutes and regulations. Pursuant to 47 C.F.R. § 1.20005 and the Communications Assistance for Law Enforcement Act ("CALEA"), under this SSI Plan, Company will: (a) ensure that any interception of communications or access to call- identifying information effected within its broadband service premises can be activated only in accordance with appropriate legal authorization, appropriate carrier authorization, and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission; and (b) implement the assistance capability requirements of CALEA section 103, 47 U.S.C. § 1002, to ensure law enforcement access to authorized wire and electronic communications or call identifying information. Any questions about how to comply with the policies and procedures in this SSI Plan should be referred to the employee appointed by the Company to oversee the provision of technical assistance and compliance. Contact information for this individual can be found in Appendix A.

Upon receipt of authorization, the Company has established appropriate carrier authorization policies and procedures to supervise and control officers and employees authorized to assist law enforcement agencies in conducting any interception of communications or access to call/ IP address identifying information. Any employee who receives a request for any form of electronic surveillance, whether from a law enforcement official or from any other person, should immediately direct the requesting party to the Company's SSI Representative identified in Appendix A, who has been designated as the authorized person to accept these requests and act on them. The SSI Representative is specifically charged with the responsibility to assist law enforcement in conducting any interception of communications or providing access to call/ IP address identifying information. In addition, the SSI Representative is responsible for ensuring that appropriate legal authorization is provided. Such authority consists of an order signed

by a judge or magistrate authorizing or approving interception of wire or electronic communications, or other authorization pursuant to 18 U.S.C. § 2518(7) or any other relevant federal or state statute. The SSI Representative's name, title, and contact information have been submitted to local law enforcement agencies in advance so that requests of this nature can be submitted directly to the designated contact. This information, along with a description of the duties of the SSI Representative, is included in Appendix A, attached hereto. If the SSI Representative is not available, all requests must be immediately directed to the most senior management employee available.

The SSI Representative designated to act on these types of requests will assume total responsibility for any request from receipt of the request to its final disposition, including the proper certification and storage of all details regarding the request. The specific responsibilities include but are not limited to:

- Serving as the point of contact for law enforcement concerning an ordered surveillance request seven days a week, twenty-four hours a day,
- Ensuring that all requests are made with appropriate legal authorization, such as an order signed and dated by the judge or magistrate authorizing or approving the request, and
- Implementing the request by, among other things, initiating the request for interception or access to call/ IP address identifying information, instructing those performing the various tasks involved, and ensuring compliance with all applicable rules and regulations.

III. RECORDS RETENTION

Information regarding each interception of communications, whether properly authorized or not, will be documented on an approved certification form contemporaneously with, or within a reasonable time after, the initiation of the interception. Such certification will include the following:

- The name of the requesting law enforcement officer, together with his or her agency and department, and a copy of the order or equivalent authorization; or, in the case of an unauthorized interception, all available documentation detailing the request,
- Information regarding the surveillance request, including the date and time it was presented, the date and time of implementation, the type of interception or call/IP address identifying information requested (e.g., pen register, trap and trace, Title III, or PISA), the target's name and telephone number, IP address or circuit identification, and the duration of the interception, and
- The actions taken to obtain this information, and the name, signature, and title of the SSI Representative authorizing and overseeing the action requested in the order or request.

After review of the certification form and associated documents, the SSI Representative will sign and date the record and ensure that it is maintained in the Company's offices at 1140 Terex Road, Hudson, OH 44236 in a secure area, for a period of no less than two (2) years.

IV. UNAUTHORIZED USE OF SURVEILLANCE CAPABILITIES

Any employee who knowingly misuses intercept capabilities intended for lawful surveillance will face disciplinary measures, up to and including dismissal. Information regarding any attempt to interfere with a lawful request for surveillance and any incidents of unauthorized electronic surveillance will be reported to local law enforcement.

These policies and procedures will remain in effect until notice is provided to the Commission regarding a significant change.

Electronically Signed this 1st day of May 2023.

/s/ Will Ersing

Will Ersing
Assistant IT Director
City of Hudson DBA Velocity Broadband
1140 Terex Road
Hudson, OH 44236
Telephone: 330-342-9544
Email: wersing@hudson.oh.us

Appendix A

Description and Contact Information of System Security and Integrity (SSI) Representative and Alternative

Will Ersing
Assistant IT Director
City of Hudson DBA Velocity Broadband
1140 Terex Road, Hudson, OH 44236
330-342-9544
wersing@hudson.oh.us

Job Description: In addition to duties as the SSI Representative described in the attached SSI Plan, Will Ersing serves as the Assistant IT Director for City of Hudson DBA Velocity Broadband. In that capacity, Will is responsible for any open records requests and its responses to lawful requests for records ensuring that disclosed information remains in compliance with the Terms of Use and Privacy Policy, and as permitted by law.

If the above listed SSI Representative cannot be reached:

Maureen Reich
Broadband Business Development Manager
City of Hudson DBA Velocity Broadband
1140 Terex Road, Hudson, OH 44236
330-342-9544
mreich@hudson.oh.us