

**Accompanying Statement
to Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

The policy of Vocatech, Inc. (hereinafter “Company” or “the Company”) is to protect the confidentiality of CPNI, as required by section 222 of the Telecommunications Act of 1996, and the FCC’s rules promulgated thereunder. The key provisions of the Company’s operating procedures and practices with respect to CPNI are set forth below.

I. Use of CPNI:

- A. The company has established operating procedures to ensure compliance with the Commission’s rules governing the protection of CPNI.
- B. The Company does not use, disclose, or permit access to CPNI without customer consent, except as permitted by 47 U.S.C. § 222 and 47 C.F.R. § 64.2005.
- C. The Company does not use, disclose, or permit access to CPNI for marketing purposes.
- D. The Company does not disclose or permit access to CPNI to third-parties.

II. Management Safeguards:

- A. The Company has designated a corporate officer, who is responsible for actively monitoring, managing, and training all employees with access to CPNI.
- B. The company has established a program to inform and train all personnel on the proper use and disclosure of CPNI.
- C. The Company has established disciplinary procedures for any employee that wrongfully accesses, uses, or discloses CPNI. Any improper use of CPNI is treated as a serious offense, and will result in appropriate disciplinary action.
- D. The Company reviews its CPNI procedures on an ongoing basis to ensure compliance with all FCC regulations, and will revise its procedures as needed to reflect any subsequent revisions to the applicable rules and regulations.

III. Authentication:

- A. The Company uses the procedures specified in 47 C.F.R. § 64.2010 to authenticate a customer’s identity before sharing CPNI with that customer.
- B. The Company will disclose CPNI to a customer during an in-person visit only after the customer presents a Valid Photo ID matching the Customer’s Account Information.

- C. The Company will only disclose CPNI over the telephone, based on customer-initiated contact, if the customer first provides the Company with a password that is not prompted by the Company asking for Readily Available Biographical Information or Account Information.
- D. The Company will permit online access to CPNI through a password that is not prompted by the Company asking Readily Available Biographical Information or Account Information.
- E. All physical facilities containing CPNI are secure, with restricted physical access.

IV. Management of Potential CPNI Security Breaches

- A. Consistent with 47 C.F.R. § 64.2011, the Company has adopted procedures for notifying law enforcement of a breach of its customers' CPNI.
- B. The Company maintains records of any and all potential CPNI breaches.
- C. The Company validates the authenticity of all requests from law enforcement, and ensures that such requests are lawful before releasing CPNI.