E911 Notice

This notice is required by the rules of the Federal Communications Commission. Twin City VoIP dba Minnesota VoIP may have the E911 limitations listed below.

1) MnVoip must have accurate address information for Emergency services to be directed to customer site. MnVoIP must be notified if any equipment is moved to a new address otherwise Emergency services may be dispatched to the wrong address.
2) MnVoIP uses electrical power to power equipment necessary to place E911 calls. Any electrical power outages will interfere with your ability to place E911 calls from MnVoIP supported equipment. Battery Back-up is available for purchase but will only last for a limited amount of time depending on equipment capability.
3) Calls, including calls to 911, may not be completed if there is a problem with network facilities including network congestion, network equipment, power failure, or other technical problems.

Prior to changing my address or if I have any 911 related questions I will call Twin City VoIP dba Minnesota VoIP at 612-355-7740. It may take several days to update a service address change.

***Use of Minnesota VoIP services after delivery of this document constitutes your acknowledgment of the E911 notice above.**

General Terms and Conditions

I _____ as an authorized representative of _____ company understand by choosing Minnesota VoIP for my telephone and/or Data services I am agreeing to items listed below but not necessarily limited to those items.

1) I am entering into a month to month agreement unless otherwise stated and will provide MnVoIP with 30 day written notice before cancelling all or part of our account. Billing will continue until such notice is received.

2) We will hold MnVoIP harmless for any loss of business or productivity due to any Telephone or Data outages. I understand that without Internet access our phones may not function and E911 services will not work.
3) We understand that MnVoIP cannot be held responsible for Internet outages even if MnVoIP is the supplier of the Internet, or if customer has alternative supplier.
4) We will notify MnVoIP before allowing any changes to security equipment installed by MnVoIP. All security equipment supplied by the customer must be approved by MnVoIP Technical department.
5) WE will be responsible for all calls originating from our location including International if such access has been requested. (Please read attached Toll Fraud prevention sheet)
6) We will protect security by the use of complex passwords on all voicemails boxes and web portals.

---------- ----------

Authorized Signature Date accepted

Toll-Fraud Prevention Tips

1) **Unauthorized Voicemail Access** – This occurs when someone access's your voicemail illegally by guessing your password and placing outbound calls through the system. Do not leave default passwords for these are easily guessed by criminals. Example, 1234, 1212, 0000, 1111, 9999.
2) **Web Portal Breach** – The web portal once breached can allow criminals to forward you calls to outside numbers. Like your voicemail password these should be as complex as possible and kept private.
3) **Social Engineering** - A perpetrator persuades a company employee to provide dial tone access. Criminals may call claiming to represent the telephone company asking for system transfer or access to dial tone. They also may seek sensitive information such as pins and passwords.

Toll Fraud Prevention Techniques

1) Change all system and voicemail passwords frequently. Every 60-120 days
2) Ask MnVoIP to block International calling if not needed.
3) Educate your employees on the possibility of fraudulent activity. Make them aware of the need for password protection and the prevalence of Toll fraud activity.
4) Never allow changes to security equipment without first notifying MnVoIP IT department.
5) Review your bills closely
6) Be sure to change passwords for former employees
7) If you suspect toll fraud contact MnVoIP immediately.
8) Secure all security equipment and passwords.

MnVoIP does not bear any responsibility for Toll-Fraud. Your Company is responsible for securing all phone equipment and for paying for usage charges that may occur through fraudulent activity.