# UEN GUIDELINES: NETWORK SERVICES
# VOICE OVER INTERNET PROTOCOL

## Purpose

This document outlines UEN's guidelines for implementing a VoIP communication link through its network. The implementation process is defined separately by UEN Technical Services and will be modified as needed. UEN was established to provide Utah students and educators with electronic access to educational services that improve student achievement through high-quality, cost-effective networking through existing public telecommunication services.

## Definitions

**Voice Over Internet Protocol (VoIP):** a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet rather than the public switched telephone system (PSTN).

**VoIP Network:** a Public Telecommunication Network over which VoIP Services are provided.

**VoIP Service(s):** all of the services and technologies that allow the transmitting, receiving, delivering and routing of voice telecommunications by means of internet protocol (IP); i.e., commercial VoIP, PBX VoIP, hosted PBX or any like service regardless of branded terminologies.

**Public Switched Telephone Network (PSTM):** also referred to as the Plain Old Telephone Service (POTS), is the network of the world's public circuit-switched telephone networks.

**Internet Service Provider (ISP):** a company that offers its customers access to the Internet. The ISP connects to its customers using a data transmission technology appropriate for delivering IP such as dial-up, DSL, cable modem, wireless or dedicated high-speed interconnects.

**Firewall:** a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.

**Enhanced 911, E-911 or E911:** a North American telecommunications-based system that automatically associates a physical address with the calling party's telephone number and routes the call to the most appropriate Public Safety Answering Point (PSAP) for that address. The caller's address and information is displayed to the call

taker immediately upon call arrival. This provides emergency responders with the location of the emergency without the person calling for help having to provide it.

**Assisted Global Positioning System (GPS):** a system which can improve the startup performance of a GPS satellite-based positioning system. It is used extensively with GPS-capable cellular phones, making the location of a cell phone available to emergency call dispatchers.

**Border Gateway Protocol (BGP):** the protocol that backs the core routing decisions on the Internet. It maintains a table of IP networks, or prefixes, which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule sets. For this reason, it is more appropriately termed a reachability protocol rather than routing protocol.

**Abstract Syntax Notification (ASN):** a standard and flexible notation that describes data structures for representing, encoding, transmitting and decoding data. It provides a set of formal rules for describing the structure of objects that are independent of machine-specific encoding techniques and is a precise, formal notation that removes ambiguities.

**Synchronous Optical Networking (SONET) Protocols:** standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or light-emitting diodes (LEDs).

**Time-Division Multiplexing (TDM):** a type of digital or (rarely) analog multiplexing in which two or more signals or bit streams are transferred apparently simultaneously as sub-channels in one communication channels, but are physically taking turns on the channel.

## Guidelines

1. In a continuing effort to support schools, school districts, and the public and higher education systems and deliver cost-effective services through an open and competitive bidding process, UEN makes its network available to VoIP services for public and higher education institutions according to identified UEN standards from licensed VoIP vendors.

2. UEN will not solicit VoIP services on behalf of stakeholders.

3. UEN will assist stakeholders in implementing VoIP services at their request.

4. UEN provides VoIP network services as a “best effort” strategy and does not provide guaranteed quality of service (QoS) or level of performance.

5. UEN will not enter into contracts with vendors to guarantee them service beyond contracts with UEN stakeholders.

6. VoIP services will be offered to UEN stakeholders on the condition that the services will not degrade network performance or impose additional operating costs on UEN.

7. If VoIP services are provided, UEN will determine the best interface to link with UEN's network; i.e., location, equipment, protocols, etc.

8. Clients/vendors are responsible to implement and operate VoIP services according to established state and federal rules and regulations.

9. Any licensee offering or marketing VoIP Service shall inform users and potential users of VoIP services of any differences between the VoIP service and traditional telecommunication services.

10. UEN is not responsible for the quality of service (QoS) associated with any particular VoIP vendor. Therefore, the stakeholder exploring VoIP services should consider the issues and potential limitation of VoIP telephone service including but not limited to service quality, latency, availability (i.e., telephone services that are entirely reliant on Internet infrastructure can disrupt all communication, including Enhanced 911 and other equivalent services in case of a single-point failure), voice quality, nature of operation, ease of use, pricing.

11. UEN does not guarantee network security for VoIP services transported over the UEN network infrastructure.

12. UEN will not bear any expenses incurred by stakeholders associated with new connections required to provide commercial VoIP services. Stakeholders exploring VoIP services should consider potential network security responsibilities and issues including but not limited to protecting VoIP networks from unauthorized or unlawful access.

13. UEN may either conduct or authorize a third party to conduct security audits on a licensee's VoIP network and associated facilities, to ensure the security and integrity of that VoIP network. Licensees shall provide access to UEN or any third party appointed by UEN to conduct these security audits.

14. In respect of any VoIP services and VoIP networks over which those VoIP services are provided, licensees shall comply with all requirements of the state (or agencies of the state) regarding national security requirements.

15. UEN reserves the right to shut off excessive or bad traffic and will give fair warning to the institution prior to turning down a circuit or blocking any traffic.

16. Meeting legal requirements of content (CALEA, copyright, etc.) is the responsibility of vendors and all UEN stakeholders.

17. Security breaches that affect UEN must be reported to UEN (vendors are responsible for monitoring and reporting all security breaches).

18. UEN will not be responsible for the loss of telephones service during a power failure. Therefore, the stakeholder exploring implementation of VoIP services should consider service risk issues, such as electrical power failures.

19. UEN will not provide redundant VoIP circuits over the network infrastructure. Therefore, the stakeholder exploring implementation of VoIP services should consider redundancy related issues so that emergency communications are reliably supported.

20. UEN will not be responsible for maintaining a VoIP E911 emergency calling system. Therefore, the stakeholder exploring implementation of VoIP services should consider VoIP E011 issues including but not limited to—

- The nature of IP makes it difficult to locate network users geographically. Emergency calls, therefore, cannot easily be routed to a nearby call center. Since IP allows a great deal of mobility, mobile users could be anywhere that there is network coverage. The VoIP E911 emergency-calling system associates a physical address with the calling party's telephone number. In the United States, the Wireless Communications and Public Safety Act of 1999 leaves the burden of responsibility upon the subscribers and not the service providers to keep their emergency information up to date.
- It will be the responsibility of the VoIP provider to assure that E911 information is up-to-date in conformance with the Wireless Communications and Public Safety Act.

21. UEN will not be responsible for monitoring or enforcing State and Federal telecommunication regulations. Therefore, the stakeholder exploring implementation of

VoIP services should consider regulatory issues including making service accessible to people with disabilities and paying regulatory fees, universal service contributions and other mandated payments.

22. Any VoIP providers connecting to UEN must physically connect and peer to a UEN backbone hub location. Backbone hub locations are USU, WSU, DATC, EBC, SLCC, UVU, SNOW-Ephraim, SNOW-Richfield, SUU, DSC, CEU and UVW. Connections into these locations must be approved by UEN Technical Services staff. 10/100/1000 Ethernet Circuits will be preferred. No Synchronous Optical Networking (SONET) or Time-division multiplexing (TDM) connections are supported.

23. Routing information between UEN and VoIP providers are exchanged only with Border Gateway Protocol (BGP).

24. VoIP provider should preferably use public Abstract Syntax Notation (ASN) for peering but a private ASN will be supported.

25. Any UEN routes sent to VoIP provider should be marked with NO_EXPORT BGP community or something similar which disallows UEN routes from being leaked to any other ASN.

26. Any VoIP provider routes sent to UEN will also be marked with NO_EXPORT BGP community and will not be sent to any neighboring ASN.

27. Any UEN routes leaked outside of the VoIP providers ASN will be reason for termination of connection and BGP peer.

28. VoIP provider cannot use UEN network for transiting any traffic.

29. UEN does not provide any end-to-end service guarantees.

30. UEN will ensure proper routing only on the UEN network.

31. UEN cannot provide any Quality of Service (QoS) guarantees on the UEN network.

32. UEN cannot assist in troubleshooting any layer 4+ issues.

Revision Notes:

Ver. 1 – approved by the UEN Steering Committee on October 22, 2010

Ver. 2 –