

## **CHAPTER 7**

## **NETWORKS**

Article.

1. State Network.
  2. Network Nebraska.
- RD. Resource Documents.

**ARTICLE 1**  
**STATE NETWORK**

Section.

- 7-101. State communications system; acceptable use policy.
- 7-102. DNS forwarding standard.
- 7-103. SMTP routing standard.
- 7-104. Web domain name standard.
- 7-105. Wireless local area network standard.
- 7-106. Internet of Things (IoT) standard.

**7-101. State communications system; acceptable use policy.**

(1) Purpose. This policy applies to all users of the state communications system. It is intended to provide minimum standards for acceptable use of the system; agencies may adopt policies or standards more stringent than those contained herein. All use of the system is subject to applicable state and federal laws. Users should not have any expectation of privacy regarding personal business conducted on the system unless otherwise protected by state or federal law.

(2) Acceptable Use. The state communications system may be used for the following:

(a) The conduct of state business;

(b) State government sponsored activities;

(c) By state employees and officials for emails, text messaging, local calls, and long-distance calls to children at home, teachers, doctors, daycare centers, baby-sitters, family members, or others to inform them of unexpected schedule changes, and for other essential personal business. Any such use for essential personal business shall be kept to a minimum and shall not interfere with the conduct of state business. A state employee or official shall be responsible for payment or reimbursement of charges, if any, that directly result from any such communication. [Neb. Rev. Stat. § 81-1120.27(1)] Essential personal business shall not include use of the state communications system for personal financial gain or campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question; these uses are prohibited. [Neb. Rev. Stat. § 49-14,101.01(2) and § 49-14,101.02(2)]; and

(d) Such other uses allowed by law.

(3) Remedial Action. Each agency is responsible for taking immediate remedial action to address any violation of this policy within the agency.

(4) Exception. This section does not apply to wireless access points available for general use by the public.

--

**History:** Adopted on March 9, 2004. Amended on November 30, 2009, and July 12, 2018.

**URL:** <https://nitc.nebraska.gov/standards/7-101.pdf>

**7-102. DNS forwarding standard.**

All outbound internet DNS traffic must be forwarded through the state's internal DNS servers.

--

**History:** Adopted on June 27, 2007. Amended on March 4, 2008, and July 12, 2018.

**URL:** <https://nitc.nebraska.gov/standards/7-102.pdf>

**7-103. SMTP routing standard.**

All inbound and outbound SMTP traffic must be routed through the anti-spam and anti-virus appliance managed by the Office of the CIO.

--

**History:** Adopted on June 27, 2007. Amended on March 4, 2008, and July 12, 2018.

**URL:** <https://nitc.nebraska.gov/standards/7-103.pdf>

**7-104. Web domain name standard.**

(1) The approved domain names for Nebraska state government websites are “nebraska.gov” and “ne.gov.” The Chief Information Officer may approve other domain names using the .gov top level domain.

(2) The domain “state.ne.us” is a supported legacy domain that may serve content but should not be publicly promoted.

(3) Domain names using top level domains other than those listed in subsections (1) and (2) may be registered and serve content but must not be publicly promoted.

(4) All state government websites using the .gov domain must comply with federal .gov domain requirements (<https://home.dotgov.gov/registration/requirements/>).

(5) All domain name registrations, purchases, and renewals must be made by the Office of the CIO.

--

**History:** Adopted on April 19, 2013. Amended on October 28, 2014; July 12, 2018; and March 10, 2022.

**URL:** <https://nitc.nebraska.gov/standards/7-104.pdf>

### **7-105. Wireless local area network standard.**

(1) Purpose. The purpose of this standard is to ensure that only properly secured and managed wireless local area networks are deployed by state agencies.

(2) Registration Requirement. All wireless local area networks that connect to the state network must be registered with the Office of the CIO.

(3) Registration Process. The registration process will identify: contact information; device information, including the manufacturer, model, and physical location; the security/firewall technologies being deployed; where logging information is to be stored; and, if the use of the wireless access is only for internet, a description showing how traffic will be separated. Registration information must be submitted to the Office of the CIO Service Desk. Registration must occur prior to deployment. The Office of the CIO will contact the registering agency after reviewing the registration information. Final device names are assigned by the Office of the CIO during the registration process to avoid conflicts and confusion, and to aid in incident response and in identifying and locating wireless devices. If technology allows for the broadcast of a device name, standardized names should appear in the broadcast description, along with any unique identifiers assigned to the unit.

(4) Unregistered and Unsecured Devices. Only approved wireless local area networks and access points will be deployed within state agencies. Unregistered devices will be removed from service. Network managers for the Office of the CIO will incorporate procedures for scanning for unregistered wireless devices and access points. The Office of the CIO may disable network access for a device, server or network if inadequate security is found or improper procedures are discovered.

(5) Management and Security of Access Points.

(a) Physical Security. Access points must be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices must not be placed in easily accessible public locations.

(b) Configuration Management. All wireless access points must be secured using a strong password. Passwords must be changed at least every six months. Administrators must ensure all vendor default user names and passwords are removed from the device.

(6) Security of the Wireless Network.

(a) Logging. All access to the wireless network must be logged with records kept for a minimum of one year. Records must include the time of access, the IP and MAC addresses of the device, and the username.

(b) Access to the State Network. Accessing the state network requires a username and password combination that is unique to each user. The SSID must use a minimum of WPA2 with the use of a FIPS 140-2 validated AES encryption module.

(c) Wireless Intrusion Detection Systems. All wireless networks must use a wireless intrusion detection systems (WIDS) capable of location detection of both authorized and unauthorized wireless devices. All systems must provide continuous scanning and monitoring. WIDS logs and documented actions must be maintained for a minimum of one year

(7) Management of Airspace. All conflicts regarding wireless connectivity are resolved by the Office of the CIO.

--

**History:** Adopted on September 30, 2013. Renumbered on July 12, 2018 (previously was § 7-301). Amended on August 4, 2006; April 11, 2012; and July 12, 2018.

**URL:** <https://nitc.nebraska.gov/standards/7-105.pdf>



### **7-106. Internet of Things (IoT) standard.**

This policy provides standards for Internet of Things (IoT) devices within the state network. IoT devices include but are not limited to door controls, cameras, and wireless sensors. While the benefits of IoT devices are numerous and compelling, it is important to remember that these devices have the potential to introduce significant threats and risks to the state network. IoT devices do not follow an international compatibility standard leaving them more exposed to vulnerabilities. The State of Nebraska must properly govern and manage deployment IoT devices.

The following are the minimum standards for IoT devices on the state network:

- (1) IoT devices must be approved by the Office of the CIO prior to being put on the state network;
- (2) IoT devices must be isolated from business operations on the state network;
- (3) IoT devices must support either username/password or certificate-based authentication;
- (4) IoT devices must support a minimum of TLS 1.2;
- (5) IoT devices must have the ability to be managed at the enterprise level;
- (6) IoT devices must allow for NTP and DNS to be set by administrators;
- (7) IoT device access must be limited to only what is necessary;
- (8) Network traffic for IoT devices should not be prioritized over normal business operations unless the IoT device impacts emergency services or public safety; and
- (9) Wired connections for IoT devices are preferred over wireless connections when possible.

--

**History:** Adopted on March 10, 2022.

**URL:** <https://nitc.nebraska.gov/standards/7-106.pdf>

**ARTICLE 2**  
**NETWORK NEBRASKA**

Section.

- 7-201. Network Nebraska; network edge device standard.
- 7-202. Contracting guideline for upgrade of distance learning services.
- 7-203. IP communication protocol standard for synchronous distance learning and videoconferencing over Network Nebraska.
- 7-204. Video and audio compression standard for synchronous distance learning and videoconferencing.
- 7-205. Scheduling standard for synchronous distance learning and videoconferencing.

## **7-201. Network Nebraska; network edge device standard.**

(1) Purpose. The purpose of this standard is to set minimum standards and specifications for network edge devices that would perform the routing and switching functions of voice, video, and data across the network and assure that packets would get to their correct destination while maintaining the appropriate quality of service (QoS).

(2) Technical Standards. Agencies and other entities electing to connect to Network Nebraska for purposes of transmitting data across the state shall comply with this standard.

(a) Network edge device specifications for new purchases: (1) QoS capabilities; (2) sufficient ports for desired network design; (3) security and/or firewall features; (4) routing and/or routing protocol; (5) traffic shaping and rate limiting; (6) VLAN (802.1q) support; (7) secure remote management (SSH); (8) hardware based encryption acceleration; (9) performance to meet anticipated usage demand; (10) compatibility with central site router features; and (11) IPv6 capable. Option include: a Layer 3 router for basic site deployment; an enhanced Layer 3 router for larger site deployment or higher performance; or a Layer 3 switch/firewall combination.

(b) Network edge device specifications for existing equipment: (1) QoS capabilities; (2) sufficient ports for desired network design; (3) security and/or firewall features; (4) routing and/or routing protocol; (5) traffic shaping and rate limiting; (6) VLAN (802.1q) support; (7) secure remote management (SSH); (8) hardware based encryption acceleration; (9) performance to meet anticipated usage demand; (10) compatibility with central site router features; and (11) IPv6 capable.

### **(3) Responsibilities.**

(a) Network Nebraska Operational Entities. The Collaborative Aggregation Partnership, composed of the University of Nebraska Computer Services Network, the Office of the CIO, and Nebraska Educational Telecommunications, will be responsible for sharing the responsibilities of the network operations portion of Network Nebraska. The responsibility for identification and mitigation of non-compliant entities with respect to this standard resides with the Collaborative Aggregation Partnership.

(b) Education-Related Political Subdivisions. An education-related political subdivision shall provide notice in writing, as required by guidelines established by the University of Nebraska and the Chief Information Officer for participation in Network Nebraska, to the distance education director of the Educational Service Unit Coordinating Council, the University of Nebraska, and the Chief Information Officer prior to the use of any new or additional equipment

that will impact the use of Network Nebraska by such education-related political subdivision or other education-related political subdivisions. [Neb. Rev. Stat. § 86-520.01]

--

**History:** Adopted on July 12, 2006. Amended on March 4, 2008; November 15, 2011; and July 12, 2018.

**URL:** <https://nirc.nebraska.gov/standards/7-201.pdf>

## **7-202. Contracting guideline for upgrade of distance learning services.**

(1) Purpose. The purpose of this guideline is to make the contracted services portion of distance learning contracts more flexible for the end-user and the provider and better able to accommodate future technology applications.

(2) Objective. The objective of this guideline is to permit users to access all the bandwidth on the negotiated circuit. It will allow providers to continue service and to expand networks as required by updating the systems they use to NEBS (Network Equipment Building System) standard compatible equipment. It will allow interoperability between users among multiple consortia. It will permit new telecommunications services on the DS-3 connections in use and permit increased speeds on current services such as access to the internet.

(3) Guidelines. Entities that receive state funding for telecommunications and public entities that are approaching contract expiration for existing distance learning services are advised to make every attempt to take advantage of the efforts to aggregate services and contracts. As new contracts are contemplated for distance learning, it is recommended that discussions minimally include consideration of the following:

(a) Contracting Options. (1) Negotiate one contract for connective terminal hardware and transport as long as the end-user has full access to and flexible use of all bandwidth on the network and has the ability to upgrade video encoding equipment as desired, or (2) negotiate two contracts at the local level; one contract for procurement (including maintenance) of connective terminal hardware (CODEC) and a second contract for transport (preferably the use of Network Nebraska).

(b) Contract Expiration Dates. To the extent possible, the local entity should make transport contract expiration dates co-terminus with the Network Nebraska core transport contracts (contact the Office of the CIO for more information).

--

**History:** Adopted on November 13, 2003. Amended on July 12, 2018.

**URL:** <https://nitc.nebraska.gov/standards/7-202.pdf>

**7-203. IP communication protocol standard for synchronous distance learning and videoconferencing over Network Nebraska.**

(1) Purpose. The purpose of this standard is to implement a consistent communication protocol to be used by all entities wishing to pass synchronous, interactive teleconference video over Network Nebraska.

(2) Standard. All state agencies, entities that receive state funding for telecommunications, and entities that wish to pass synchronous video over Network Nebraska must use IP as their communication protocol for synchronous video.

--

**History:** Adopted on November 13, 2003. Renumbered on July 12, 2018 (previously was § 7-401). Amended on July 12, 2018.

**URL:** <https://nitc.nebraska.gov/standards/7-203.pdf>

**7-204. Video and audio compression standard for synchronous distance learning and videoconferencing.**

(1) Purpose. The purpose of this section is to establish video and audio protocol standards that will enable all existing and future synchronous distance learning and videoconferencing facilities in Nebraska to achieve interoperability and maintain an acceptable quality of service.

(2) Standards.

(a) Video protocol standards for synchronous distance learning and videoconferencing: (i) for data rates above 384 Kbps, H.263; and (ii) for data rates at or below 384 Kbps, H.264 (MPEG-4 Part 10). The CODECs selected for purchase or use should be capable of accommodating both standards and be capable of manual rate selection and/or automatic rate selection. The interconnecting CODECs should be allowed to automatically negotiate the best data rate.

(b) Audio protocol standards for synchronous distance learning and videoconferencing: (i) for data rates above 128 Kbps, G.722; and (ii) for data rates at or below 128 Kbps, G.722 or G.722.1 or G.728. The CODECs selected for purchase or use should have the ability to use G.722 at all speeds and one or both of the other two standards listed for lower speeds. If any two CODECs do not have a common protocol at or below 128Kbps then they should continue to use G.722. The CODECs selected for purchase or use should be capable of accommodating audio standard G.722 and be capable of manual rate selection and/or automatic rate selection. The interconnecting CODECs should be allowed to automatically negotiate the best data rate.

(3) Applicability. This section applies to synchronous distance learning and videoconferencing facilities as follows:

(a) If utilizing state-owned or state-leased communications networks: (i) any synchronous distance learning facility or videoconferencing application which utilizes state-owned or state-leased communications networks must comply with the compression standards listed in this section; or (ii) the entity must provide, or arrange for, the necessary gateway technology to transcode to the adopted standards.

(b) If using state funding: (i) all new facilities or applications receiving state funding must comply with the compression standards listed in this section; and (ii) all existing facilities or applications receiving state funding for ongoing operations must convert to the standards listed in this section as soon as fiscally prudent or upon renewal of any existing communications service contract, whichever comes first.

--

**History:** Adopted on September 9, 2004. Renumbered on July 12, 2018 (previously was § 7-402). Amended on July 12, 2018.

URL: <https://nitc.nebraska.gov/standards/7-204.pdf>



### **7-205. Scheduling standard for synchronous distance learning and videoconferencing.**

(1) Purpose. The purpose of this standard is to establish and define the needs for scheduling to be addressed when purchasing and maintaining scheduling coordination systems. The objective of this standard is to enable all existing and future synchronous distance learning and videoconferencing facilities in Nebraska to achieve interoperability and maintain an acceptable scheduling of services through recurring and ad hoc event coordination.

(2) Standards. This subsection consists of a list of five components and accompanying features that must be available in any software system that is developed for use in scheduling of synchronous events using videoconferencing technology. It is the intent that any and all such scheduling systems defined by the specifications below be accessible either through the internet or within a defined intranet as decided upon by the system administrators. The following sections describe the various levels and types of scheduling or coordination that must be accommodated.

(a) Hardware Control Component. When attempting to link two or more sites electronically, a system must have the capability to coordinate the connectivity between/among the sites. This includes controlling the network and endpoint hardware and bandwidth necessary to cause a successful connection. A hardware control system must be able to control hardware in a network and be capable of linking into other systems listed in this standard to enable the following: (i) browser-based access; (ii) locate devices by IP address [both static and DHCP]; (iii) locate devices by MAC address; (iv) facilitate far-end control in endpoint devices with the capability; (v) display a call list that is understood by non-technical staff using plain English site descriptions; (vi) hardware and software systems must work such that the scheduling system is available for use at least 99.9% of the time; (vii) automatically accumulate log data that may be searched by system administrators using multiple search variables; (viii) maintain security in ways that can be defined by system administrators including providing an identity management system that allows for multiple levels of user access as defined by system administrators; and (ix) facilitate various types of events, such as broadcast to all, broadcast to some, 2-way point-to-point, and 2-way multipoint.

(b) Event Logging Component. A system coordinator must have the ability to track information about events. This may include knowing the number of people at a site, the minutes an event runs at any given site, or the number of events a specific organization schedules. An event logging system must be able to automatically store data and permit reporting and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) store data in an ODBC compliant relational database; (iii) provide fields for logging various pieces of information; (iv) permit system administrator defined fields [no fewer than 64]; and (v) local contact and facility arrangement information.

(c) Facilities Coordination Component. If an event will include locations for which more than one person/organization has responsibility, then some mechanism must exist for coordinating use of facilities. There may be technical or administrative limits as to the number or types of sites that can participate in any given event. This could be as simple as users coordinating times over the telephone or through email, but for some applications there may be a greater need for pre-scheduling and coordination among multiple administrators. A facilities coordination system shall enable access to facilities based on defined permissions, resolve conflicts based on pre-determined policies and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) system editable user access, including: (A) building level admin such that the facilities at a specific location can set policies for that site and permit use by others; (B) regional admin such that a group of facilities can set policies for all related sites and permit use by others; (C) sector admin such that groups of groups of facilities can set policies for all related sites and permit use by others; and (D) user account directory service with definable permissions for each account; (iii) facilities information to be posted, including: (A) identify technology available by site; (B) physical site location; and (C) local contact and facility arrangement information; and (iv) permit system administrator defined fields [no less than 64] that would provide for event information to be posted.

(d) People Coordination Component. If a specific location is to be used, this implies that operational support will be available to support the success of events. Since there will be a variety of site designs and equipment configurations, then there may be a variety of demands on staff time. Finally, there may be limitations as to the total number of participants allowed. A people coordination system must enable interaction of people based on policies set by system administrators and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) allow for multiple permission levels including: (A) view schedules, (B) request systems/facilities, and (C) approve systems/facilities use; (iii) provide information about instructor/facilitator and their availability; (iv) allow for predetermined maximum number of attendees; (v) track and display count of committed and remaining attendees; (vi) allow for predetermined maximum number of sites; and (vii) track and display count of committed and remaining sites.

(e) Event Clearinghouse Component. As system users see a need for pre-scheduled events coordinated among a large number of facilities and administrators, the concept of a virtual location for brokering of events becomes attractive. Such a clearinghouse should serve as a way that event coordinators might let others know the specifics of events they are planning [e.g., a certain class with a specific sort of content will be offered on a certain schedule for a certain period of time or a specific event will happen one time on a specific day at a specific time]. Such an event clearinghouse should also serve as a way for interested parties to find events that meet their specific needs [e.g., a school administrator has a certain number of students who need a specific class that is not offered locally]. Availability might also include information about participant or site number limitations [e.g., the total seats/sites in the class/event, the number

requested/registered so far and the number remaining of the total]. An event clearinghouse system must enable online interaction for publishing of event information and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) posting of one-time single events; (iii) posting of sequenced or cyclical events; (iv) posting of costs to participate in an event; (v) permit system administrator defined fields [no less than 256]; (vi) provide for automated multiple time zone accommodation; (vii) use an ODBC compliant relational database; (viii) user defined search/reporting capability; and (ix) provide for automated email notification of site requests/confirmations.

(3) Applicability. This section applies to the purchase and maintenance of synchronous distance learning and videoconferencing software systems used by educational institutions. The governing board or chief administrative officer of each organization is responsible for selecting and using a synchronous distance learning and videoconferencing software system that is in compliance with these standards. It is the intent of the Technical Panel and Commission that the guidelines and policies for usage of such scheduling and clearinghouse systems be determined by the administrative entities that oversee such distance learning and videoconferencing.

--

**History:** Adopted on September 9, 2004. Renumbered on July 12, 2018 (previously was § 7-403). Amended on July 12, 2018.

**URL:** <https://nitc.nebraska.gov/standards/7-205.pdf>

## **RESOURCE DOCUMENTS**

Section.

7-RD-01. Telecommunications facilities and services.

## **7-RD-01. Telecommunications facilities and services.**

(1) Purpose. This resource document is intended to provide guidance to agencies on telecommunications facilities and services needed in an ordinary office setting and to provide a suggested allocation of responsibilities between a lessor, lessee, and tenant agency. Any such work in a state owned building should meet these minimum requirements.

### **(2) Responsibilities.**

(a) Tenant Agency. The tenant agency will obtain all telecommunication services except local cable-television or satellite-television services from the Office of the CIO. The tenant agency will pay the monthly charges for said telecommunication services. The tenant agency will pay any charges for local cable-television or satellite-television services. This includes costs to install satellite-television receiving equipment and cabling. The tenant agency will contact the Office of the CIO should any of the items in this document not meet the needs of the agency.

(b) Lessor. The lessor should ensure adequate entrance facilities are provided for the telecommunication services required by the tenant agency. This includes all necessary tie cables between the service provider's terminal and/or demarc blocks and all remote wiring-closets/consolidation-points used to attach services to the station cabling serving the telecommunication information outlets. Costs associated with the installation and/or upgrading of existing entrance facilities and/or tie cables should be incurred by the lessor. The lessor should provide, at a minimum, a telecommunications information outlet at each desk and/or workstation. Each telecommunications information outlet should consist of two modular jack connectors: one telephone (voice) jack and one computer (data) jack.

### **(3) Telecommunications Facilities and Services; Recommended Requirements.**

#### **(a) Telecommunications Information Outlet Cabling Requirements.**

(i) Each telephone cable shall be a solid copper, 24 AWG, 100  $\Omega$  balanced twisted-pair (UTP), at a minimum Category 3 cable with four individually twisted-pairs, which meet or exceed the mechanical and transmission performance specifications as outlined in the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as of the signing date of the lease agreement.

(ii) Each data cable shall be a solid copper, 23 or 24 AWG, 100  $\Omega$  balanced twisted-pair (UTP), at a minimum Category 6 cable with four individually twisted-pairs, which meet or exceed the mechanical and transmission performance specifications as outlined in the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as of the signing date of the lease agreement.

(b) Telecommunications Information Outlet Connector Requirements.

(i) Each voice outlet shall be an 8-pin modular, at a minimum Category 3, unkeyed jack, using the USOC pin/pair assignment.

(ii) Each data outlet shall be an 8-pin modular, at a minimum Category 6, unkeyed jack, using the T568B pin/pair assignment.

(c) Telecommunications Cabling Installation Requirements.

(i) The lessor shall provide a complete and working telecommunication distribution system. This system shall include, but is not limited to: all station, riser, aerial, and intra-campus cables as required; conduits, raceways, and all associated cable support hardware; telephone and data outlet connectors, face plates, and identification labels; termination blocks and brackets, patch panels and mounting brackets, distribution rings; all cable terminations and testing; and all associated appurtenances as required by the distribution system.

(ii) Each telephone and computer jack shall be terminated on separate cables, which shall be terminated on separate connecting blocks/panels at a common central location.

(iii) Installation, termination, and testing of telecommunications information outlet components shall be performed by qualified personnel, employed by a company whose primary business is providing telecommunication services. This does not include work normally performed by an electrical contractor.

(iv) All work shall be performed in accordance with the equipment manufacturer's requirements.

(v) All cable terminations shall be performed at the respective terminal boards, equipment cabinets, and station outlets.

(vi) All station cabling shall be "home run" to appropriate distribution frame, block, or equipment cabinet. No splices will be allowed in these lines.

(vii) Distribution panels are not to be located in a plenum area or above accessible ceilings.

(viii) All cables installed above accessible ceilings shall be neatly bundled utilizing commercially available products and attached to appropriate supports. Cables installed randomly and disorderly will not be allowed.

(ix) All cables shall be installed in a fashion not to interfere with the general maintenance of other electrical/mechanical devices, as well as in a manner that other electrical/mechanical devices will not interfere with the operation of the cables intended application.

(x) All installations shall conform to the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as well as any associated technical systems bulletin, as of the signing date of the lease agreement.

(d) Telecommunications Information Outlet Testing Requirements.

(i) Each Voice and data cable link shall be tested and conform to the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as of the signing date of the lease agreement. Testing shall be accomplished using level III or higher field testers.

(e) Telecommunications Information Outlet Documentation Requirements.

(i) Each information outlet faceplate and closet termination point shall be labeled.

(ii) The lessor shall provide a floor plan (paper copy and editable electronic copy) of the occupied space to the tenant agency. This floor plan shall indicate the following: outlet locations and labeling scheme; wiring closets and/or station-cabling concentration points; telephone rooms; data server rooms; and, if more than one wiring closet serves the occupied space(s), a visual representation shall indicate the floor area(s) being served by each closet.

(iii) The tenant agency shall maintain a current copy of the lessor-provided floor plan, indicating any moves, adds, or changes to the information outlets which occurred during the period of the lease. At the end of the lease term, the tenant agency shall provide the lessor a copy of this updated and current floor plan.

(f) Regulatory and Other Requirements.

(i) Wiring methods, conductor applications, and insulation materials shall meet all applicable provisions of the National Electrical Code and Federal Communications Commission Rules and Regulations as well as applicable State and Local Codes.

(ii) All new cables and wires installed shall be listed by Underwriters Laboratories, Inc.

(iii) All cables installed shall meet appropriate fire ratings.

(4) Definitions.

Demarc, or demarcation point, means the physical point at which separation is made between the telecommunications service provider's cable facilities and those owned by the end user/building owner. The point in which the provider's service is handed off to the user's cable facilities and/or equipment. Multiple demarc locations in one physical structure are common. Tie cables which provide connectivity between entrance facilities and demarc locations are owned by the local service provider.

Entrance facilities means an entrance to a building for both public and private network service cables (including antennas) including the entrance point at the building wall and continuing to the entrance room or space. Entrance facilities are often used to house electrical protection equipment and connecting hardware for the transition between outdoor and indoor cable. The entrance facility includes overvoltage protection (often referred to as a terminal) and connecting hardware for the transition between outdoor and indoor cable.

Home run means an individual cable run installed from a central distribution point to termination point. Each cable run is a continuous length without a splice or intermediate point. Each cable run is a continuous length without a splice or intermediate termination point. Typically referred to as a "star" topology.

Telecommunications information outlet means a user connection facility provided in a work area as part of a structured cabling system.

Tie cable means cabling facilities used to connect two physical points together. (Example: multi-conductor cable used to extend services from an entrance room or space to a remote wiring closet or station-cabling cross-connect field.) Riser cables, used to extend services between floors of a structure, are also considered tie cables. Tie cables can be copper or optical fiber in construction.

--

**History:** Approved by the Technical Panel on December 11, 2012.

**URL:** <https://nitc.nebraska.gov/standards/7-RD-01.pdf>