SECTION 710
COMPUTER AND ELECTRONIC COMMUNICATIONS FACILITIES

SOURCE: NDSU President

1. Section 158 and NDUS Policy 1202.1 govern acceptable use of electronic communications devices and provide definitions used in this section.

2. If someone suspects that another individual has access to their credentials (i.e., UserID and/or password) or has evidence of any other security breach, it should be immediately reported to the NDSU Information Technology Security Officer and supervisor.

3. Batch and interactive access to the administrative computer systems (e.g. ConnectND) must be authorized by a designated access control officer. To locate the appropriate access control officer for a system, contact the Office of Accounting, Human Resources/Payroll, or Registration and Records (student systems), respectively. Supervisors of users with access to the administrative computer systems are responsible for notifying the appropriate access control officer(s) when the user changes jobs or terminates employment with the University.

4. In order to protect the campus data networks, the NDSU Vice President for Information Technology (VPIT) reserves the right to establish requirements and procedures for network access, including forms of registration and/or authorization before devices are able to access the network. In the event of imminent threats or network disruption, it may also be necessary to temporarily block specific types of network traffic or to isolate portions of the network. Any device may be removed from the network or have its network access blocked without notice if its connection to the network poses a threat to the network, to the device itself, or to the user(s) of the device. Examples of reasons why a device might be removed from the network, or blocked include, but are not limited to, the following:

    4.1. A device does not meet current device requirements.

    4.2. A device is used for unauthorized uses or by unauthorized users (see Policy Section 158).

    4.3. Network addresses are unauthorized, misappropriated or have been modified to avoid restrictions

    4.4. A device's connection to the network poses a threat to network or data security as a result of improper configuration or other reasons.

5. Requests for data and networking services must be made to Enterprise Computing and Infrastructure (ECI). The following procedures apply:

    5.1. Work requests: must be submitted on the Request for Data/Networking Services available on the Web. If you have questions, please contact the IT Help Desk (phone 231-8685 option 1). There is a charge for materials and labor. ECI personnel will provide an estimated cost of the project prior to installation, if requested.

5.2. All wiring for data circuits, for example Local Area Networks (LAN), in campus buildings must be installed and tested by ECI personnel or with their approval before it can be connected to the campus communications backbone.

5.3. Departmental (or Building) LANs connected to the Campus Communication backbone must be linked through equipment authorized by ECI.

5.4. Wireless access points and other radio communications devices, modems, or other remote access devices connected to the campus network must be authorized by ECI.

5.5. Unauthorized mechanical or electrical alteration of any part of the network infrastructure (e.g., wall jacks, wire closets, building wiring or circuits) is prohibited. Employees and VPIT approved third party contractors are responsible for promoting the physical security of electronic computing devices and network infrastructure at all times. Access to wiring closets and other locations with computer or electronics communications equipment shall be limited and strictly controlled.

5.6. Assignment of network addresses (e.g., Internet Protocol addresses, domain names) is coordinated by ECI. Contact the Help Desk (231-8685 option 1) for more information.

6. The Vice President for Information Technology (VPIT) reserves the right to establish requirements and procedures for connecting servers to the NDSU networks. Servers are integral to many computer systems and networks. They provide, by their nature, special challenges to ensure the confidentiality, integrity, and availability of computer and network resources.

6.1 A "server" is defined as any device that provides computing service to multiple computers or individuals. See NDUS Policy 1202.1 Section 3.

6.2 All servers on the NDSU networks or operated by NDSU entities must be registered with the Vice President for Information Technology (VPIT).

6.3 All servers are subject to established NDUS and NDSU policies, procedures, and standards. See NDUS Policy 1202.1 ,

6.4 Servers holding private and/or confidential data, defined in the "NDUS Data Classification and Information Technology Security Standards", are especially critical and must be individually evaluated by the VPIT or designee. The factors to be evaluated include, but are not limited to, the following:

6.4.1 The physical, logical and environmental security of the server.

6.4.2 The professional training of the server administrator.

6.4.3 The configuration of the server with regard to security.

6.4.4 The provision for the regular audit and review of the server.

HISTORY:

New July 1990

Amended	February 1993
Amended	June 1996
Amended	March 1998
Amended	October 2004
Amended	October 2007
Amended	June 2008
Housekeeping	March 2010
Housekeeping	April 1, 2011
Housekeeping	June 15, 2018