Teleworking Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☒ Adopted
Document Owner: Information Security Committee
Last Review Date: March 2025

Teleworking Policy

Purpose

The purpose of this policy is to establish the rules and conditions under which short and long-term telecommuting may occur in order to maintain acceptable practices regarding the use and protection of Nebraska Indian Community College (NICC) **Information Resources**.

Audience

The NICC Teleworking Policy applies to any individual connecting remotely to NICC information resources.

Contents

Policy

General Requirements

- Personnel must be approved by their manager and IT prior to remote access or teleworking. Under no circumstance is a person permitted to work remotely without prior permission.
- Personnel are responsible for complying with NICC policies when working using NICC **Information Resources** and/or on NICC time. If requirements or responsibilities are unclear, please seek assistance from the Chief Information Officer (CIO).
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on NICC time and/or using NICC **Information Resources** are the property of NICC.
- The teleworker is responsible to ensure that non-employees do not access NICC data, including in print or electronic forms.
- The team member will be required to maintain a regular schedule. All hours of work must be recorded according to regular NICC policies. Overtime and time off must have advance approval according to the regular policies of NICC.
- Equipment and information must be protected according to their classification and in alignment with the Information Classification and Management policy. Teleworkers are responsible for protecting NICC equipment and information from theft, damage, or other loss while in transit or at the remote work location. At no time should documents or company equipment be left unattended in a public area.

- Personnel are expected to follow NICC's Incidental Use policy when using NICC devices remotely.

Internet Connection

- Personnel must not connect to an unsecured Wi-Fi network with NICC equipment or to perform NICC work.
- Wi-Fi connections must be secured with strong encryption (WPA2). The use of WPA or WAP is not allowed.
- When connecting to a Wi-Fi network, personnel must use only the pre-approved VPN solution.
- Users must not connect to another wireless network and the NICC wireless network simultaneously.
- The use of split-tunnel VPN is prohibited.
- For long-term or home office networks:
    - A high-speed Internet connection is required. Personnel will provide the Internet service at their own expense. The internet connection must be of sufficient bandwidth to allow the team member to efficiently perform their regular job functions.
    - Teleworkers will comply with [Teleworking Procedures] for implementing wireless networks securely.
    - Recommended that wireless networks be secured with a strong password, consisting of 16 or more characters.
    - When possible, the home network used with NICC Information Resources should be isolated from other devices and computers in the home.

Equipment

- NICC provided computing devices are highly recommended to be used for working remotely (laptops and desktops).
- Computing devices must be secured with NICC provided or approved:
    - Active and up-to-date antivirus software
    - Active local firewall
    - Full-disk encryption
    - Automatic screen lock
- Personnel are responsible for regularly rebooting their device in order to allow software patches and updates to be installed.
- Personally owned devices, including but not limited to USB memory, portable hard drives, mobile phones, MP3 players, iPods/iPads, and smart gadgets, are not allowed to be connected to NICC equipment, including wireless connections.
- Maintenance of NICC provided equipment must be provided or preapproved by IT.

Printing

- The printing of any non-public NICC information must be preapproved by the Information Owner.
- The printing of any non-public NICC information to a public printer is prohibited.
- Personnel must be preapproved by IT and their manager for printing at a remote location. Personnel approved to print must have (or be supplied with) a shredder.
    - IT will determine if the person's network is secure.
    - The device used to print must be directly connected to the printer used. Wireless printing must be pre-approved by Information Technology and requires the use of strong encryption.
- All non-public NICC information must be secured when not in use and shredded when no longer needed in accordance with NICC's Information Classification and Management policy.
- The printing of Confidential information at a remote location is not permitted.

Telephone

- When possible remote personnel will use NICC provided phone, phone app, or headset for all NICC related calls.
- When other people are present in the remote work location, a headset must be used to safeguard the conversation.

Office Requirements

- Workspaces must be secured to protect all NICC equipment and maintain the confidentiality of all information related to the organization and/or its customers.
- Personnel must allow IT to inspect and/or retrieve the equipment provided to them at any time.
- NICC may inspect and/or retrieve any NICC information maintained at home by personnel.
- The use of personal video surveillance on home entrances and exits is encouraged.

Definitions

See Appendix A: Definitions

Waivers

Waivers from certain policy provisions may be sought following the NICC Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	November 2023			Document Origination
		5-30-2024	IT Committee	
		10-25-2024	Academic Committee	Review and Approved.
		12-18-2024	Administrative Committee	Review and Approved.
		01-22-2025	Executive Committee	Review and Approved.
		03-29-2025	Board of Directors	Review and Approved.