NORTHWEST INDIAN COLLEGE
Xwlemi Elh>Tal>Nexw Squl

NWIC Remote Access Form

The purpose of this policy is to provide a process by which employees of the Northwest Indian College, through the Northwest Indian College (NWIC) and other non- NWIC entities or individuals, may be authorized and permitted to remotely access the NWIC's computer information system in an appropriate and secure manner for authorized business purposes.

Policy:

This policy governs the remote access by authorized entities and individuals to information on the NWIC computer networks whether on-site or off-site. There are six elements of this policy as described below:

1. **Access Software System**

    a. The VPN (Virtual Private Network) appliance system provides for security, functionality and flexibility in accessing information contained on NWIC's computer systems via a secure remote access connection.

    b. Access to the NWIC's computer network systems will be provided via Barracuda SSL (Secure Socket Layer) VPN tunneling appliance.

2. **Internet Service Provider (ISP)**

    a. The NWIC will provide its users with Internet access at its discretion.

    b. Non- NWIC users will be responsible for providing the Internet access services necessary to facilitate connectivity to the NWIC SSL VPN at their expense outside of the NWIC computer network.

3. **Client Software for NWIC Applications**

    a. All SSL VPN appliances will be licensed and provided by the NWIC IS Department.

    b. The IS Department shall establish and enforce minimum standards for equipment, operating system, and application software necessary for network connectivity via the Barracuda SSL VPN tunneling appliance.

    c. Barracuda SSL VPN tunneling appliance will not be made available until minimum specifications of equipment have been verified and any applicable waivers have been signed.

4. **Access Requirements for NWIC and Non-NWIC Entities/Users**

a. Remote access approval is required at both the NWIC Department Director and President levels.

b. The standards contained in the NWIC IS User Manual shall be followed.

c. All users must comply with all NWIC policies relating to privacy, confidentiality and appropriate use.

d. Background checks may be required of any user at the discretion of the President, upon the recommendation of the IS Director and shall be conducted at the expense of the requesting entity, including non- NWIC entities. Background checks shall be conducted by the NWIC Human Resources Department.

e. The appropriate NWIC Division Director must confirm, by signature, both the need for remote access by a specific entity or individual and approval of the Department Director for the NWIC IS Department to enable such access. Authorizing signatures shall be required on the following forms prior to activating remote access connectivity:

   i. Network Access request form
   ii. Internet/intranet acceptable use policy
   iii. Jenzabar access request form

5. Support Services

a. The NWIC IS Department, at its discretion, will assist in enabling SSL VPN connectivity through reasonable mitigation of technical issues with the use of this technology associated with Internet Service Provider's (ISP) or connectivity providers. Expenses for mitigating such issues shall be at the expense of the requesting non- NWIC entity.

b. Support is not provided for non- NWIC equipment. Referrals to qualified third party vendors of support services will be made available.

c. Support for NWIC assets will be provided by the IS Department.

d. NWIC IS support will not be provided at any non- NWIC remote location.

6. Authorization of use of technology

a. Approval for all non- NWIC personnel to use remote access via SSL VPN must provide written and signed authorization and a description of need from a senior level official of the non- NWIC organization.
b. Criminal background expenses shall be completed at the requesting entity's expense.

Procedure:

a. The NWIC IS Director shall be responsible for the oversight and implementation of the SSL VPN Remote Connectivity process.

b. The NWIC IS Department shall coordinate the set up process.
   i. Criminal background checks where required shall be conducted by the Human Resources Department.
   ii. Signature on required forms.
   iii. Client Software loaded.

iv. Completion of training session

c. Violations of this policy or inappropriate use by any user shall be grounds for termination of remote access privileges at the discretion of the IS Department Director.

d. Any formal appeals of actions taken or not taken pursuant to this policy shall be made in writing to the IS Department Director.

i. The IS Director shall make every reasonable attempt to resolve remote access issues.
ii. Any issue related to this policy that is not considered to be satisfactorily resolved by the IS Director may be appealed to the NWIC's Office of the President for a final review and decision.

Approval:

Employee Name (please print) _____

Employee Signature _____Date___/___/____

Administrative Authorization:

Name (please print) _____

Signature _____Date___/___/____

IS Director Name (please print) _____

IS Director Signature _____Date___/___/____

President (please print) _____

President Signature _____Date___/___/____

For Internal I.S. Department Processing Only

__ Group Membership(s) *I.S. initial* _____ *Date* _____

NORTHWEST INDIAN COLLEGE

Xwlemi Elh>Tal>Nexw Squl