Attachment F

Remote Network Access Request Form

Use this form to submit a request to State of Alaska (SOA) for remote access to SOA Network.
(This form can be filled out online and printed for signatures or printed blank and manually completed.)

Read and follow instructions included in this form.

For further information contact your departmental IT staff.

Account Type Requested (check ONLY ONE)

VPN

☐ **Password Authentication**

2-Factor (2FA) VPN

☐ **Hardware token** ☐ **Android App** ☐ **iOS/Apple App** ☐ **Other**

Account Modification Requested (check ONLY ONE)

☐ **New Account** ☐ **Change Existing Account** ☐ **Delete Existing Account**

Information Required for All Fields

State of Alaska User (email) ID: _____

- For Contractors, an ID must be created by your sponsoring department before you can proceed.
- Departmental Technical contact URL: http://oit.alaska.gov/passwordrecovery
- For Health and Social Services, please use your internal process

Account Requestor Information Required:

Name and Title: _____

Telephone Number: _____

Email Address: _____

Fax Number: _____

Sponsoring Department: _____

Sponsoring Division: _____

Company Name (if a contractor): _____

Submit completed form with signatures to departmental IT staff (continued below).

SOA Internal

VPN Installation and Configuration:

You and your supervisor, or Contracting Officer for non-state employees; must review the process and follow instructions provided. Read and commit to the "Customer Acknowledgement" and sign your names. You should also contact your Department Information Security Officer (ISO) for additional requirements or instructions from your department regarding remote access or use. State of Alaska Security Policy ISP-172 Business Use/Acceptable Use and ISP-173 Network Security apply to all users.

To use State of Alaska VPN your computer needs VPN client software. By installing and operating this VPN software, you commit you have already verified your computer is free of malicious software (examples include but are not limited to virus/worms/Trojans) and spyware, and you agree you will continue to keep your computer free of such software. This includes your requirement to keep your computer OS (operating system) patches and anti-virus signatures up-to-date. If your operating system is not patched to current security levels, you must update it before installing VPN software. All SOA PCs are required to have Cybereason installed in "protect" mode**.**
If you do not have up-to-date anti-virus software installed and running on your computer – DO NOT use this computer to connect to the SOA network until you do so!

If you need assistance choosing, downloading, or installing remote access software, contact your department's computer support staff. Contractors and other non-state users are supported by their sponsoring department. No client software, other than the SOA versions available for download, is currently supported.

User/Customer Acknowledgement

Ethical Standard: I acknowledge that reasonable use and common sense must prevail in the workplace use of Office Technologies and that I must understand and comply with applicable Alaska statute, policies, and administrative code.

The Executive Branch Ethics Act states a public employee may not "use state time, property, equipment, or other facilities to benefit personal or financial interests" (AS 39.52.120(b)(3)).

"AS 11.46.740. Criminal Use of a Computer (a) A person commits the offense of criminal use of a computer if, having no right to do so or any reasonable ground to believe the person has such a right, the person knowingly access or causes to be accessed a computer, computer system, computer program, computer network, or any part of a computer system or network, as a result of that access, (1) obtains information concerning a person; or (2) introduces false information into a computer, computer system, computer program, or computer network with the intent to damage or enhance the data record or the financial reputation of a person; (3) introduces false information into a computer, computer system, computer program, or computer network and, with criminal negligence, damages or enhances the data record or the financial reputation of a person; (4) obtains proprietary information of another person; (5) obtains information that is only available to the public for a fee; (6) introduces instructions, a computer program, or other information that tampers with, disrupts, disables, or destroys a computer, computer system, computer program, computer network, or any part of a computer system or network; or (7) encrypts or decrypts data. (b) In this section, "proprietary information" means scientific, technical, or commercial information, including a design, process, procedure, customer list, supplier list, or customer records that the holder of the information has not made available to the public. (b) Criminal use of a computer is a Class C felony."

SOA Internal

Criminal Activity: I acknowledge that misuse of computing resources is a criminal activity under Alaska Statute (including those as follows): "(AS 11.46.484) Criminal Mischief in the Fourth Degree (a) A person commits the crime of criminal mischief in the fourth degree if, having no right to do so or any reasonable ground to believe the person has such a right (1) with intent to damage property of another, the person damages property of another in an amount of $50 or more but less than $500; (2) the person tampers with a fire protection device in a building that is a public place; (3) the person knowingly accesses a computer, computer system, computer program, computer network, or part of a computer system or network; (4) the person uses a device to descramble an electronic signal that has been scrambled to prevent unauthorized receipt or viewing of the signal unless the device is used only to descramble signals received directly from a satellite or unless the person owned the device before September 18, 1984; or (5) the person knowingly removes, relocates, defaces, alters, obscures, shoots at, destroys, or otherwise tampers with an official traffic control device or damages the work upon a highway under construction. (b) Criminal mischief in the fourth degree is a class A misdemeanor. (c) *[Repealed, Sec. 11 ch 71 SLA 1996]."*

Password Confidentiality: I acknowledge that this account shall be used solely in the performance of my authorized job functions. I also acknowledge that I will take the necessary precautions to maintain the confidentiality of my ID password; and that I will immediately report its disclosure or use by anyone other than myself, to my supervisor, or my Contracting Officer and to the State of Alaska Service Center (1-888565-8680 Statewide or 868-7174 in Anchorage).

Security Policy Compliance: I acknowledge that this account shall be used solely in the performance of my authorized job functions. I also acknowledge that it is my sole responsibility to ensure any use or access is compliant with the state security policies and will take all the necessary steps to ensure compliance. Security Policies are located at the following URL: (state email authentication is required) https://oit.alaska.gov/policy

Compromise Remediation /Security Violations: Should security monitoring determine your authenticated VPN-connected host is compromised with malicious software, running a prohibited file-sharing program, or otherwise in violation of security policy, your VPN ID may be immediately deactivated. Reinstatement of the ID will take place only after remediation/investigation has taken place per state policy/operating procedure. Permanent account revocation could be applied depending on the severity of the offense.

Split Tunneling: Split tunneling, or access to local resources (primarily a network attached printer) will be disabled during the connection to the SOA network via VPN.

When the VPN software is active all computer traffic is being diverted through the SOA network, including Internet/Web traffic; this activity may be logged and monitored. **This computer when connected must not be left unattended if no automated screenlock mechanism is being used.**

Please add a brief description of Business Requirement and list all Applications that will require remote access with a brief description of what SOA systems you need access to.

SOA Internal

Once OIT Operations receives the signed and approved Remote Access Request Form, OIT will complete the account authorization process.

***Only Supervisor, ISO, Alternate or Designee signatures are required for deleting an account.

Signed Acknowledgement and SOA Authorization

By signing below, I certify that I meet all access and security measures, requirements, and procedures required in the performance of my authorized job function and I have read and understand my ethical, legal, and password security responsibilities as described above.

Requesting Person

Requester (Print Name) | Telephone Number

- Required for Contractors - Social Security Number or Passport (please include copy of passport) or Copy of Birth Certificate or valid US Drivers License (please include copy of license).
- If State Employee, please use AKPAY Identification Number

Requester (Signature) | Date

Approving Supervisor

Approving Supervisor (Print Name) | Telephone Number

Department (Print) | Division (Print)

Approving Supervisor (Signature) | Date

SOA Internal

Division Director

Division Director (Print Name) | Telephone Number

Department (Print) | Division (Print)

Division Director (Signature) | Date

Department Information Security Representative, Alternate or Designee

Department Information Security Representative, Alternate, or Designee (Print Name) | Telephone Number

Department (Print) | Division (Print)

Department Information Security Representative, Alternate, or Designee (Signature) | Date

SOA Internal