THE STATE of ALASKA
GOVERNOR BILL WALKER

Health and Social Services
Division of FMS (IT Security & Technology)

Non-DHSS Employee Access Request Form

Form Instructions for Non-State employee access

The **Sponsoring Agency** will ensure this form is filled out in its entirety, and the applicant information is correct.

Dates for Access: Maximum access is one (1) year for all organizations and/or contractors, at the end of the year all renewals are mandatory and will be resubmitted by the sponsoring agency. All organizations and/or contractors will need an SOA ID to be created by the sponsoring department before they can proceed.

VPN Installation and Configuration:
The Sponsor, or Contracting Officer must review the process with their Non-state employees as well provide all instructions necessary for an setting up an VPN account.
To use State of Alaska VPN your computer needs VPN client software. *Please click here for FAQ's and help.*

(All applicants: Must read and sign page two (2) "On Site and/or Remote Access Agreement" and have a copy of their ID and HIPAA training certificate.

Attach all completed form/s and signed remote access agreement to your DHSS Help desk ticket {DHSS HELP DESK}, or you can Scan and Email them to **hss.helpdesk@alaska.gov**

***Only Supervisor and ISO/Alternate/Designee signatures are required for deleting an account.*

Sponsoring Agency Information:			**Applicant Information:**	
Today's Date:			**State of Alaska User ID:**	
Department/Division:			**DHSS ID:**	
Sponsor name:			**Last Name:**	
Sponsor Email Address:			**First Name & MI:**	
Type of request: VPN No Action needed---- ◉	○ New VPN Account ○ Delete VPN Account** ○ Renew VPN Account ○ Change existing VPN account		**Phone:**	
Type of request: DHSS Account No Action needed---- ◉	○ New DHSS Account ○ Delete DHSS Account** ○ Renew DHSS account ○ Change existing DHSS account		**E-mail Address:**	
Type of request: OpenConnect No Action needed---- ◉	○ New OpenConnect account ○ Delete Open Connect Account ○ Renew Open Connect account ○ Change OpenConnect account		**Driver's License Or State ID#: (Passport #, DLN, or Copy of Birth Cert.)**	ID# / State Identification Type: ○ Driver's License ○ State ID ◉ Passport ○ Birth Certificate
Type of request: SOA Account No Action needed---- ◉	○ New SOA Account ○ Delete SOA Account** ○ Renew SOA Account ○ Change existing SOA			
Dates for Access:	Start Date:	End Date:	**Position Title and/or Duties Performed:**	
Contracting organization or Company, *If applicable*				

Please add a brief description of the business need and list all applications/systems that require remote access.

I certify that the above information is accurate and the requested access is necessary for the conduct of State of Alaska business. I will review this person's access annually and I will notify DHSSIT and the Department Security Office when access requirement changes, such as password resets if they forget their Passphrase, account changes , and deletions when the requester is no longer authorized into the State of Alaska systems.

Sponsor printed Name, and phone number:	**Sponsor Signature & Date:**
Division Director printed Name, and phone number:	**Division Director Signature & Date:**
ISO, Alternate, or Designee printed Name, and phone number:	**ISO, Alternate, or Designee Signature & Date:**
Ticket Number:	

THE STATE of ALASKA
GOVERNOR BILL WALKER

Health and Social Services
Division of FMS (IT Security & Technology)

Non-DHSS Employee Access Request Form

ON SITE and/or REMOTE ACCESSAGREEMENT

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"(AS39.52.120(b)(3)).

"AS11.46.740. Criminal Use of a Computer (a) A person commits the offense of criminal use of 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 an 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."

Criminal Activity: I acknowledge that misuse of computing resources is a criminal activity under Alaska Statute (including the following): "(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."

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. DHSS Security Policies are located at the following URL: http://in.dhss.ak.local/das/pandp/default.htm#700 State of Alaska Security Policy ISP-172 Business Use/Acceptable Use and ISP-173 Network Security apply to all VPN users. SOA Security Policies are located at the following URL: https://intranet.state.ak.us/admin/SecurityPolicies/

Personal Computers: DHSS policies do not allow the processing of HIPAA information, electronic protected health information (ePHI), or other confidential protected information on personal computers or other personal devices (tablets, etc.).

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 (1-888-565-8680 Statewide or 868-7174 in Anchorage).

Compromise Remediation /Security Violations: 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 state owned PCs are required to have HIPS installed in "protect" mode. If you do not have up-to-date anti-virus software installed and running on your computer DO NOT INSTALL and use this VPN software!

Should security monitoring determine your authenticated VPN-connected host is compromised with malicious software, is found 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: I acknowledge that it is my sole responsibility to ensure my computer's VPN client configuration is set to not allow local networking, while connected to any state network or system. When the VPN software is active (yellow padlock in system tray is "locked"): all computer traffic is being diverted through the SOA network, including Internet/Web traffic; this activity may be logged and monitored. **This computer CANNOT be left unattended when the VPN is active**.

Date	*Printed Name (Applicant)*	**Signature*