



Department of Health and Social Services

DIVISION OF HEALTH CARE SERVICES Background Check Program

4601 Business Park Blvd., Bldg K Anchorage, Alaska 99503-7167 Main: 907.334.4475 Fax: 907.269.3488

Alaska Background Check Application

*Asterisks mark required fields. Applications will not be processed without complete information.

Personal Information

Full Legal Name: Last First M.I. Date of Birth (mm/dd/yyyy)

Permanent/ Physical Address: Physical Street Address Apartment/Unit # City State ZIP Code

Mailing Address (if different than Permanent/ Physical Address): Mailing Address Apartment/Unit # City State ZIP Code

Primary Phone: () Secondary Phone: ()

*Applicant's Email Address:

*SSN (or ITN) : This is an ITN

Demographic Information

*Race: (Asian, Black, White Native American, or Unknown) *Gender: (Male, Female, Unknown, Other) *Eye Color: (Black, Blue, Brown, Hazel, Green, Grey, Unknown) *Hair Color: (Black Blonde, Brown, Grey, Sandy or Light Brown, Red, White, Unknown) *Height: FT IN *Weight: Lbs. *Place of Birth (Country/State): US Citizen(Y/N):

Alias

Aliases/Prior Names (includes all names by which a person is currently known as, or has previously gone by, including nick names): Please attach additional pages as necessary

First Name: Middle Name: SSN/ITN: This is an ITN Date of Birth: (mm/dd/yyyy)

First Name: Middle Name: SSN/ITN: This is an ITN Date of Birth: (mm/dd/yyyy)

Prior Address History

Prior Addresses in the last 10 years: Please list the state(s) in which you have lived outside of Alaska for the last 10 years. This includes those states in which you have lived for schooling or training even if you remained an Alaska resident during that time. If you have lived in Alaska for the entirety of the last 10 years, you do not need to complete this section. Please attach additional pages as needed.

State: _____ Year(s) From: _____ **to** _____
State: _____ Year(s) From: _____ **to** _____
State: _____ Year(s) From: _____ **to** _____

Pre-Employment Information

Pre-Employment Information: Only complete this information if you are applying directly with a licensed and/or certified entity. The entity should provide you this information. If the entity does not provide this information to you, leave this section blank.

Provider Name: _____

State Program under which the individual will work, such as Assisted Living, PCA, Hospital, Hospice, etc.: _____

Position Title: _____

Position Type: _____
(Employee/Independent Contractor/Volunteer/Other)

Instructions

1. You should only submit this form to the Background Check Program (BCP) if you have not already applied on-line or through a licensed and/or certified entity. You may apply on line at: <https://nabcs.dhss.ak.local/bcpapplicant>. Hard copy applications will only be processed in the order in which they are received and will not be processed until a full and complete application is received, including all applicable fees and fingerprint cards.
2. Hard copy applications submitted to the BCP will not be connected to any other application or to any specific provider type within the system and require fingerprint cards and all applicable fees. **Please note fees are non-refundable.**
3. Hard copy applications submitted to the BCP must be complete within 30 days from the date the application was received. All fees and fingerprint cards must be **received by** the BCP within the 30 day timeframe. Applications found incomplete after 30 days are automatically closed. If you still require a background check, you will be required to submit a new application including all fees and fingerprints.
4. Payments may be made by check, credit card or money order. Cash payments may only be made in person at 4601 Business Park Blvd., Bldg. K, Anchorage, AK 99503. All payments must be for the exact amount. If you wish to pay by credit card, you must contact the Background Check Program at (907) 334-4475 to make a payment over the phone. Fees for fingerprint based background checks are \$76.50 and are **not refundable.**
5. Please ensure you provide a valid email address. The email address will be used to communicate with you regarding your application status, including information regarding determinations or needed information.
6. If an eligible determination is made, you must associate with a licensed and/or certified entity within 100 days of the determination. Unassociated applications will be closed after 100 days without further notice and will immediately render a background check invalid. If you continue to need a valid criminal history check, you will be required to submit a new application including all fees and fingerprints.
7. A complete application includes this application form, non-refundable payment in the amount of \$76.50, and one set of fingerprints. Complete applications should be mailed to: State of Alaska, Background Check Program, 4601 Business Park Blvd., Bldg. K, Anchorage, AK 99503.

I, _____, authorize and consent to any person provided a copy or facsimile of this Release of Information Authorization for Background Check by an authorized representative of the Department of Health & Social Services, to disclose any information regarding me in relation to civil court information, criminal justice, juvenile justice, protective service and licensing records. I understand any person providing information or records in accordance with this authorization is released from any and all claims or liability for compliance. I understand that this information may otherwise be confidential and that I am waiving that confidentiality and any claim I may have with regard to release of these records. I understand information obtained through this Release of Information Authorization for Background Check will be held in confidence in accordance with DHSS guidelines.

I, _____, authorize and consent to the department marking my name in the Alaska Public Safety Information Network (APSIN) under 7 AAC 10.915(e).

Applicant Signature

Date



RELEASE OF INFORMATION AUTHORIZATION FOR BACKGROUND CHECK

This form must be signed by the applicant for a background check and must be maintained in the individual's personnel file. If requested by the department, the form must be provided within 24 hours.

I, _____, authorize and consent to any person provided a copy or facsimile of this Release of Information Authorization for Background Check by an authorized representative of the Department of Health & Social Services, to disclose any information regarding me in relation to civil court information, criminal justice, juvenile justice, protective service and licensing records. I understand any person providing information or records in accordance with this authorization is released from any and all claims or liability for compliance. I understand that this information may otherwise be confidential and that I am waiving that confidentiality and any claim I may have with regard to release of these records. I understand information obtained through this Release of Information Authorization for Background Check will be held in confidence in accordance with DHSS guidelines.

I, _____, authorize and consent to the department marking my name in the Alaska Public Safety Information Network (APSIN) under 7 AAC 10.915(e).

I, _____, understand that upon submission of my fingerprints will be used to check the criminal history records of Alaska and of the Federal Bureau of Investigations (FBI).

I, _____, understand that procedures for obtaining a change, correction, or updating of an FBI criminal history record are set forth at Title 28, Code of Federal Regulations (CFR), Section 16.34.

This form must be signed; if the individual is 16-17 years of age, a parent signature must also be included.

Printed Name of Applicant (must be legible)

Date

Signature of Applicant

Applicant's SSN

Parent Printed Name, if applicable (must be legible)

Parent Signature.



Division of FMS

IT Services

Non-Department Employee Access Request Form



Instructions for Non-Department Employee Access Request / Agreement

Sponsor:

Sponsors' need to ensure this request is filled out in its entirety, and all applicant information is correct. By signing this request for waiver confirms you (sponsor) have on file all required training certificates, other end user agreements for the program required and additional documents. (example is ID). This information will need to be readily available if requested and kept on file with the sponsors agency.

Dates for Access:

Maximum access is one (1) year. A renewal waiver request is required from sponsor to extend account. Deleted accounts cannot be extended.

Submit waiver via email to hss.helpdesk@alaska.gov

New account - Completed form (signed second page), HIPAA Certificate and photo identification.

Renew account - Completed first page of form and signed by Sponsor.

Delete account - Email hss.helpdesk@alaska.gov account and date for deletion.

***New applicants: Must read and sign page two (2) "On Site and/or Remote Access Agreement".**

Sponsor Information			Applicant Information:	
Today's Date:			Last Name:	
Division or Sub Division:			First Name & MI:	
Sponsors name:			Phone:	
Sponsors Email Address:			External E-mail Address:	
Type of request: VPN No Action needed-----	New VPN Account Renew VPN Account	Change existing VPN Account	Check box if State of Alaska email address is needed.	
Type of request: Dept Account No Action needed-----	New Dept Account Renew Dept account	Change existing Dept account	E-mail Address:	
Type of request: OpenConnect No Action needed-----	New OpenConnect account Renew Open Connect account	Change OpenConnect account	Driver's License Or State ID:	
Type of request: SOA Account No Action needed-----	New SOA Account Renew SOA Account	Change existing SOA	ID#	State
Dates for Access:	Start Date:	End Date:	Driver's License	State ID
			Passport	Birth Certificate
			Position Title and/or Duties Performed:	
			Have new account resemble (another account security/access rights should match)	

All request for Access must contain a detailed description on 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, notifying both the Dept II via the Internal Departments help desk and the requesting Departments Compliance/Security Office if access needs require change.

Sponsor Printed Name:	Phone Number:	Sponsor Signature:	Date
Division Director Printed Name:	Phone Number:	Division Director Signature: <small>Not required for account renewal / deletion</small>	Date
ISO, Alternate, or Designee Printed Name:	Phone Number:	ISO, Alternate, or Designee Signature:	Date
Web Help Desk (WHD) Ticket Number:	Compliance Security Office Notes:		



Division of FMS

IT Services

Non-Department Employee Access Request Form



AK | DFCS
ALASKA DEPARTMENT OF
FAMILY AND COMMUNITY
SERVICES

ON SITE and/or REMOTE USER ACCESS AGREEMENT

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. Dept Security Policies are located at the following URL: <http://in.FCS.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: FCS 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