



Grant Agreement Number 169196

**AMENDMENT TO  
STATE OF OREGON  
INTERGOVERNMENTAL GRANT AGREEMENT  
FOR THE FINANCING OF  
COMMUNITY DEVELOPMENTAL DISABILITIES PROGRAM SERVICES**

In compliance with the Americans with Disabilities Act, this document is available in alternate formats such as Braille, large print, audio recordings, Web-based communications and other electronic formats. To request an alternate format, please send an e-mail to [dhs-oha.publicationrequest@state.or.us](mailto:dhs-oha.publicationrequest@state.or.us) or call 503-378-3486 (voice) or 503-378-3523 (TTY) to arrange for the alternative format.

This is amendment number **01** to Grant Agreement Number **169196** between the State of Oregon, acting by and through its Oregon Department of Human Services, hereinafter referred to as “**ODHS**” and Tillamook County, hereinafter referred to as “**County**” or “**CDDP**”.

1. This amendment shall become effective on the later of: (I) **July 1, 2022** provided it is (i) approved in writing by the Oregon Department of Justice on or before such date, and (ii) is signed by all parties, regardless of the date of the parties’ signatures; or (II) the date this Contract is approved in writing by the Oregon Department of Justice, and is signed by all parties, regardless of the date of the parties’ signatures.
  
2. The Agreement is hereby amended as follows: Language to be deleted or replaced is ~~struck through~~; new language is **underlined and bold**.
  - a. **Exhibit B, Part 2, “Service Element Standards and Procedures”, Section 9, “Special Projects”** is hereby amended as follows:
    9. **Special Projects**
      - a. Special Projects are a mechanism for special payments as a pass-through payment to the CDDP.
      - b. All requests **for Special Projects funding** must be submitted to [ODDS.FundingReview@dhs.oha.state.or.us](mailto:ODDS.FundingReview@dhs.oha.state.or.us) prior to authorization **by ODDS or submitted through an identified application process prior to authorization by ODDS. If County subcontracts the entire CDDP Program, the County, the County is prohibited from applying or receiving Special**

**Projects funding. An ODDS approved contractor may apply for Special Project funding and, when approved in writing by ODDS, may be allowed to subcontract or partner with a community organization to conduct the Project.**

- c. Performance requirements for Special Projects not otherwise defined in this Agreement are described below:
- (1) A Special Project must be authorized in advance by ODDS, and the Special Project must be performed prior to ODDS releasing funding. ~~Funding for Special Projects will be paid to the CDDP through eXPRS or direct payment.~~ **unless otherwise approved by ODDS in writing.**
  - (2) ~~Terms and conditions of each Special Project will be defined in cooperation with the CDDP.~~ **Funding for Special Projects will be paid to the CDDP through eXPRS.**
  - (3) **Terms and conditions of each Special Project will be defined in cooperation with the CDDP.**
- d. All Special Project funds are subject to Settlement to confirm and reconcile any discrepancies that may have occurred between actual ODHS disbursements of funding, and the amount actually delivered and invoiced at the end of the Agreement period or biennium in which they are authorized, whichever comes first.
- b. **Exhibit B, Part 3, “Financial Terms and Conditions”, Section 2, “Use of Funds”, subsection b.,** is hereby superseded and restated in its entirety as follows:
- b. CDDP may use funds for costs that are incurred for common or joint purposes that benefit more than one cost objective (i.e. for the community developmental disabilities program services provided by this agreement and one or more other programs) and that cannot be readily identified with a particular final cost objective without effort disproportionate to the results achieved. Funds may be used for such costs (commonly referred to as indirect costs or overhead costs) subject to the following requirements:
- (1) ODHS will allow indirect charges at the County’s federally-approved Negotiated Indirect Cost Rate if the County provides proof of such a rate
  - (2) If the County does not have a federally-approved rate, CDDP may provide cost documentation for the community developmental disabilities program services and ODHS will negotiate a cost rate with the CDDP not to exceed the ODHS’ rate provided on the budget models.
  - (3) If CDDP does not have a federally approved Negotiated Indirect Cost Rate and does not choose to negotiate a rate with ODHS,

CDDP may use a 10% de minimis rate for costs as described in this Section 2.b. No documentation is required to justify the 10% de minimis cost rate.

Costs must be consistently charged as either indirect or direct costs, but may not be double charged or inconsistently charged as both.

**c. Exhibit B, Part 3, “Financial Terms and Conditions”, Section 4, “Audit Requirements”, subsection a., is hereby amended as follows:**

- a.** ~~CDDP, or a~~ A CDDP operated by a ~~non-county~~ Subcontractor, is required to submit to ODHS an Audit within 120 calendar days of the end of the previous fiscal or biennial period. Audits must:
- (1) Cover the entire previous fiscal or biennial period and include all federal and state funds provided to CDDP as part of this Agreement.
  - (2) Must be submitted directly to [ODDS.Contracts@dhsosha.state.or.us](mailto:ODDS.Contracts@dhsosha.state.or.us) by the auditing agency or a Certified Public Accountant (CPA).

**d. Exhibit E, “Standard Terms and Conditions”, Section 24, “Notice” is hereby amended as follows:**

- 24. Notice.** Except as otherwise expressly provided in this Agreement, any communications between the parties hereto or notices to be given hereunder shall be given in writing by personal delivery, facsimile, e-mail, or mailing the same, postage prepaid to County or ODHS at the address or number set forth in this Agreement, or to such other addresses or numbers as either party may indicate pursuant to this Section. Any communication or notice so addressed and mailed by regular mail shall be deemed received and effective five days after the date of mailing. Any communication or notice delivered by e-mail shall be deemed received and effective five days after the date of e-mailing. Any communication or notice delivered by facsimile shall be deemed received and effective on the day the transmitting machine generates a receipt of the successful transmission, if transmission was during normal business hours of the County, or on the next business day if transmission was outside normal business hours of the County. Notwithstanding the foregoing, to be effective against the other party, any notice transmitted by facsimile must be confirmed by telephone notice to the other party. Any communication or notice given by personal delivery shall be deemed effective when actually delivered to the addressee.

**ODHS:** Office of Contracts & Procurement  
635 Capitol Street NE, Suite 350  
Salem, OR 97301  
Telephone: 503-945-5818  
Facsimile: 503-378-4324

**County:** Tillamook County  
Attn: Isabel Gilda **or Erin Skaar**  
201 ~~Laureal~~ **Laurel** Avenue  
Tillamook, Oregon 97141  
Telephone: (503) 842-3403  
Email: [igilda@co.tillamook.or.us](mailto:igilda@co.tillamook.or.us); [eskaar@co.tillamook.or.us](mailto:eskaar@co.tillamook.or.us);

This Section shall survive expiration or termination of this Agreement.

- e.** For services provided on and after the effective date of this amendment, **Exhibit H, Part 1 and Exhibit H, Part 2** are hereby superseded and restated in their entirety, as set forth in **Exhibit H, Part 1 and Exhibit H, Part 2**, attached hereto and incorporated herein by this reference.
- 3.** Except as expressly amended above, all other terms and conditions of the original Agreement and any previous amendments are still in full force and effect.

**4. Signatures.**

**Tillamook County**

**By:**

\_\_\_\_\_  
Authorized Signature

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

**State of Oregon acting by and through its Oregon Department of Human Services**

**By:**

\_\_\_\_\_  
Authorized Signature

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

**Approved for Legal Sufficiency:**

Approved via email by Wendy J. Johnson  
Department of Justice

6/14/2022  
Date

**EXHIBIT H, PART 1**  
**Privacy and Security Agreement**

1. **PURPOSE.** County requires the Access described in Exhibit H, Part 2, *Third Party Information System Access Request* (Form MSC 0785), which is hereby incorporated into this Exhibit H, Part 1 by reference, to perform the Work. The terms and conditions of this Privacy and Security Agreement govern:
  - 1.1. County's Use of Data;
  - 1.2. County's Access to ODHS' Information Assets and Systems;
  - 1.3. The periodic exchange of Data between ODHS' and County's systems via electronic means; and
  - 1.4. The interconnection between ODHS' and County's respective networks and information systems.
2. **TERM.** This Privacy and Security Agreement is effective for a period coterminous with the Agreement, subject to review at least annually by ODHS, unless terminated earlier by either party in accordance with the "Suspension or Termination" section of this Privacy and Security Agreement.
3. **DEFINITIONS.** The following definitions apply to this Privacy and Security Agreement:
  - 3.1. "Access" means the ability or the means necessary to read, communicate, or otherwise use ODHS or State Data, Network and Information Systems, and Information Assets
  - 3.2. "Breach" means the acquisition, access, exposure, use, or disclosure of Data or an Information Asset in a manner not in compliance with applicable law, rule, or policy, or Data loss, misuse, or compromise.
  - 3.3. "Client Records" includes any client, applicant, or participant information regardless of the media or source, collected by County in the course of completing the Work, provided through the Network and Information Systems to County, or otherwise exchanged between the parties.
  - 3.4. "Data" means information created, transmitted, or stored through the Network and Information Systems, including metadata, personal information, and Client Records.
  - 3.5. "Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of any Network and Information System or Information Asset. An Incident is an observable, measurable occurrence that is a deviation from expected operations or activities. An Incident may be a Breach, failure to protect a User's identification (ID), or theft of computer equipment that uses or stores any Information Asset.
  - 3.6. "Individual Access Request (IAR)" refers to the ODHS form used to authorize a User, identify the User's job assignment, and the required access to Network and

Information System(s). It generates a unique alpha/numeric code used to access the ODHS Network and Information Systems.

- 3.7. "Information Asset(s)" refers to all information provided through ODHS, regardless of the source, which requires measures for security and privacy. Includes Data.
- 3.8. "Network and Information System(s)" means ODHS' and the State of Oregon's computer infrastructure which provides personal communications; Data such as Client Records; Access to other Information Assets, regional, wide area, and local networks; and the internetworking of various types of networks.
- 3.9. "User" means any individual authorized to access Network and Information Systems and who has an been assigned a unique log-on identifier.

**4. CHANGES TO PRIVACY AND SECURITY AGREEMENT.** Other than as allowed under this section, County shall be requested to submit input to a revised *Third Party Information System Access Request* (Form MSC 0785), to request changes to Exhibit H, Part 2. ODHS will review County's request and, if approved in writing by ODHS, the parties will amend the Agreement in accordance with Exhibit E, Section 27.

- 4.1. **Point of Contact Changes.** Each party will provide notification to the other of any change of its respective point(s) of contact noted in Exhibit H, Part 2, including any technical lead, and name an interim or replacement person in any such notice. Exhibit H, Part 1 will be deemed amended to include the updated information.
- 4.2. **Administrative Changes.** County may request updates to Exhibit H that are administrative in nature and do not modify the mode of Access or type of data by submitting a written request to ODHS. Upon written acceptance by ODHS, Exhibit H will be deemed amended to include the updated information.

## **5. NOTIFICATIONS.**

- 5.1. **Points of Contact.** The parties have designated their respective technical leads in Exhibit H, Part 2. The parties will facilitate direct contacts between technical leads. The parties will provide notification to the other of any changes in technical point of contact information.
- 5.2. **Breach Notification.** In the event the County or its subcontractors or agents discover or are notified of an Incident or a Breach, including a failure to comply with County's confidentiality obligations under the Agreement, County shall immediately notify ODHS' Program Sponsor identified in Section 4 of Exhibit H, Part 2 (or delegate) of the Incident or Breach. If ODHS determines that an Incident or Breach requires notification of ODHS clients, or other notification required by law, ODHS will have sole control over the notification content, timing, and method, subject to County's obligations under applicable law.
- 5.3. **Requests for Data.** In the event of the County receiving a third-party request for Data, including any electronic discovery, litigation hold, or discovery searches, County shall first give ODHS notice and provide such information as may be reasonably necessary to enable ODHS to protect its interests.

- 5.4. **Changes in Law.** Each party will provide notice to the other of any change in law, or any other legal development, which may significantly affect its ability to perform its obligations.
6. **GRANT OF LICENSE.** Subject to the County’s compliance with the Agreement, County is hereby granted a non-exclusive, non-transferable, and revocable authorization to Access and use Information Assets only in accordance with this Agreement and applicable laws, rules, and policies. County and its employees, contractors, and agents shall not manipulate any URL or modify, publish, transmit, reverse engineer, participate in any unauthorized transfer or sale of, create derivative works of, or in any way exploit the content or software comprising this Access, or Information Assets made available through this Access.
7. **DATA PRIVACY.** In addition to the County’s obligations under Exhibit D, “General Terms and Conditions”, Section 9 regarding Confidentiality of Information:
- 7.1. **Generally.** County shall hold all Client Records, and other information as to personal facts and circumstances obtained by the County on ODHS clients, as confidential, using the highest standard of care applicable to the Client Records, and shall not divulge any Client Records without the written consent of the client, the client’s attorney, the responsible parent of a minor child, or the minor child’s guardian except as required by other terms of this Privacy and Security Agreement or applicable law.
- 7.2. **Limited Purposes.** County shall limit the use or disclosure of Data concerning clients to persons directly connected with the administration of this Privacy and Security Agreement or the Agreement. Confidentiality policies apply to all requests from outside sources.
- 7.3. **Privacy Protections.** Data may include information, such as Client Records, subject to specified confidentiality protections under state or federal law. County shall comply with laws, regulations, and policies applicable to the information described in Exhibit H, Part 2, including as specified in this Agreement.
- 7.4. **Training.** County’s employees, subcontractors, and agents who will Access Data have received training on the privacy and security obligations relating to the Data, including Client Records. County shall provide periodic privacy and security training to its employees, subcontractors, and agents.
8. **SECURITY REQUIREMENTS.**
- 8.1. **Compliance with Laws, Regulations, and Policies.** County and its employees, contractors, and agents shall comply with all applicable state and federal laws and regulations, and State of Oregon policies governing use and disclosure of Data (including Client Records) and Access to Information Assets, including as those laws, regulations, and policies may be updated from time to time. Applicable laws, regulations, and policies include but are not limited to:
- 8.1.1. ODHS and OHA Information Security and Privacy Policies:  
<https://www.oregon.gov/oha/FOD/OIS-ISPO/Pages/Policies.aspx>

- 8.1.2. ODHS and OHA Privacy and Confidentiality administrative rules, OAR Chapter 407, Division 14, and OAR Chapter 943, Division 14.
- 8.1.3. The Health Insurance Portability and Accountability Act (HIPAA), including as amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 (“ARRA”), and its implementing Privacy Rule and Security Rule, 45 CFR Parts 160 and 164. County shall comply with HIPAA Compliance included in the Agreement in Exhibit D “General Terms and Conditions”, Section 12 in connection with County’s Access.
- 8.1.4. The Oregon Consumer Identity Theft Protection Act, ORS 646A.600 through 646A.628, to the extent applicable.
- 8.1.5. Oregon’s Statewide Information Security Standards:  
<https://www.oregon.gov/das/OSCIO/Documents/2019StatewideInformationAndCyberSecurityStandardsV1.0.pdf>
- 8.2. **Responsible for Compliance.** County is responsible for the compliance of its employees, agents, and subcontractors with this Agreement and with any third-party licenses to which Access is subject.
- 8.3. **Privacy and Security Measures.** County represents and warrants it has established and will maintain privacy and security measures that meet or exceed the standards set in laws, rules, and regulations applicable to the safeguarding, security and privacy of Data, including Client Records, all Information Assets, regardless of the media, and all Network and Information Systems. County shall monitor, periodically assess, and update its security controls and risk to ensure continued effectiveness of those controls.
- 8.4. **Security Risk Management Plan.** County shall ensure the level of security and privacy protection required in accordance with this Privacy and Security Agreement is documented in a security risk management plan. County shall make its security risk management plan available to ODHS for review upon request.
- 8.5. **Audit Rights and Access.** County shall maintain records in such a manner as to clearly document its compliance with and performance under this Privacy and Security Agreement, and provide ODHS, the Oregon Secretary of State, the federal government, and their duly authorized representatives access to County’s officers, agents, contractors, subcontractors, employees, facilities and records for ODHS to:
  - 8.5.1. Determine County’s compliance with this Privacy and Security Agreement,
  - 8.5.2. Validate County’s written security risk management plan, or
  - 8.5.3. Gather or verify any additional information ODHS may require to meet any state or federal laws, rules, or orders regarding Information Assets.

- 8.5.4. Access to facilities, systems, and records under this section will be granted following reasonable notice to the County. Records include paper or electronic form, system security logs, and related system components and tools (including hardware and software), required to perform examinations and audits, and to make excerpts and transcripts, including for data forensics.

## 9. ACCESS TO ODHS SYSTEMS.

- 9.1. **ODHS Review of User Requests.** If required for Access, ODHS will review requests, including forms such as the IAR, and will:
  - 9.1.1. Notify County of the approval or denial of its request for each User for whom Access has been requested;
  - 9.1.2. Provide any unique log-on identifier required for authorized Access;
  - 9.1.3. Provide updates to approved inquiry processes and instructions to County.
- 9.2. **County's Responsibilities for User Accounts.** County shall facilitate completion of any forms (such as the IAR) for each person for whom Access is requested.
  - 9.2.1. County is responsible for all activities that occur through its Access, including for any acts related to a lost or stolen User ID or password.
  - 9.2.2. County is responsible for ensuring information provided by its Users is accurate, complete, and up to date.
  - 9.2.3. County shall immediately notify ODHS when a User, group of Users, or County, no longer requires Access whether due to changes in duties or due to changes in County's programs related to this Agreement.
- 9.3. **Security and Disposal.** County shall maintain security of equipment, and ensure the proper handling, storage and disposal of all Information Assets accessed, obtained, or reproduced by County and its Users to prevent inadvertent destruction or loss. County shall ensure proper disposal of equipment and Information Assets when authorized use ends, consistent with County's record retention obligations and obligations regarding Information Assets under this Agreement.
- 9.4. **Prevention of Unauthorized Access.** County shall prevent any Access to State of Oregon Network and Information Systems by its Users that is not authorized in accordance with this Agreement and applicable law, and shall implement and maintain safeguards to prevent unauthorized access.
- 9.5. **Access from Outside the US and its Territories.** County Access to the state network from outside the US and its territories is prohibited unless approved by the ODHS|OHA Chief Information Risk Officer (CIRO). If approved, the County shall provide ODHS|OHA with the IP addresses, or IP address range, to be used to Access the network. Any changes to the provided IP addresses, or IP range, shall be immediately communicated to ODHS|OHA or Access could be affected.

- 9.5.1. County shall not allow use of any Information Asset in any country or territory in any manner prohibited by governing applicable law, rule, or policy.
- 9.6. **Authorized Access and Use Only.** No User may Access or use Data for any purpose other than those specifically authorized through this Agreement.
  - 9.6.1. Users shall not use Access to obtain or attempt to obtain any Data or Information Assets not authorized or intentionally made available.
  - 9.6.2. The use and disclosure of any Information Asset is strictly limited to the minimum information necessary to the exchange of Data between the parties described in Exhibit H, Part 2.
  - 9.6.3. Except as otherwise specified or approved by ODHS, neither County nor its Users may modify, alter, delete, or destroy any Information Asset.
- 9.7. **Revocation or Termination of Access.** Breach, or wrongful use or disclosure of Information Assets by the County or its Users, may cause the immediate revocation of the Access granted through this Agreement, in the sole discretion of ODHS, or ODHS may specify a reasonable opportunity for the County to cure the unauthorized use or disclosure and end the violation, and terminate the Access if the County does not do so within the time specified by ODHS. Legal actions also may be taken for violations of applicable regulations and laws.
- 9.8. **No Unauthorized Distribution.** County shall not sell, make available, or provide Information Assets in any form to any other persons or organizations, and shall not use the Information Assets for any purposes other than as allowed under this Agreement and applicable law.
- 9.9. **No Impairment.** County shall not use this Access in any manner which could damage, disable, overburden, or impair Network and Information Systems or interfere with any other entity's use or benefit of Network and Information Systems.
- 9.10. **Prohibition on Data Mining.** County shall not capture, maintain, scan, index, share or use Data stored or transmitted by virtue of this interconnection, or otherwise use any data-mining technology, for any non-authorized activity. For purposes of this requirement, "non-authorized activity" means the data mining or processing of data, stored or transmitted through the Network and Information Systems, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security analysis that is not explicitly authorized in this Agreement.
- 9.11. **Incidents and Breaches.** County shall comply, and shall cause its subcontractors to comply, with any requirements for identifying and addressing an Incident or Breach. This requirement applies regardless of whether the Incident or Breach was accidental or otherwise.

## **10. SUSPENSION OR TERMINATION.**

- 10.1. This Privacy and Security Agreement may be terminated at any time by written agreement of the parties.
- 10.2. This Privacy and Security Agreement may be terminated by either party upon thirty (30) calendar days' written notice to the other party.
- 10.3. Access and this Privacy and Security Agreement may be terminated immediately upon written notice from the County if Access is no longer needed by the County.
- 10.4. ODHS may immediately revoke the Access granted to the County for County's failure to comply with the requirements of this Privacy and Security Agreement. In such event, ODHS will provide subsequent written notice to the County's point of contact. ODHS may, to the extent it determines it is reasonable and able to do so, provide advance notice to the County to cure any deficiency or breach of this Privacy and Security Agreement.
- 10.5. Either party may terminate this Privacy and Security Agreement, and ODHS may modify Access, upon written notice if there are changes to or revised interpretations of federal or state laws, rules, or regulations, or if either party has changes in policies that require such action.

**11. RETURN OF INFORMATION ASSETS.** Upon expiration or termination of the Agreement or this Privacy and Security Agreement for any reason whatsoever, the County shall immediately deliver to ODHS all of ODHS' Information Assets, including Data and Client Records, that are in the possession or under the control of the County in whatever stage and form of recordation such property is expressed or embodied at that time.

11.1. Except as necessary to meet obligations under Exhibit E "Standard Terms and Conditions", Section 16 "Records Maintenance, Access", the County shall not retain any copies of Information Assets. County shall notify ODHS of any conditions that make returning all ODHS Information Assets not feasible. Upon ODHS' written acknowledgement that returning all Information Assets is not feasible, the County shall purge or destroy retained Data in all its forms in accordance with the most current version of NIST SP 800-88 (or other agreed-upon standard) and on request provide ODHS with written certification of sanitization.

11.2. County shall maintain protections required by law or the Agreement for any retained State of Oregon Information Asset for so long as the County (including through any subcontractor) retains it.

**12. INDEMNIFICATION AND INSURANCE.** Indemnification and insurance coverages provided by the County under the Agreement apply to this Privacy and Security Agreement.

- 13. COSTS.** Each party will bear its own costs related to the acquisition of all equipment, software, data lines or connections necessary for Access, unless otherwise agreed to by written agreement between the parties. Each party is responsible for securing compatible hardware, equipment, and software, and network connections. Each party is responsible for complying with the licenses for third party products, including software and services that allow Access.
- 14. SURVIVAL.** Access and rights to use Information Assets ceases upon termination of this Privacy and Security Agreement. Rights and obligations which expressly or by their nature survive termination do so survive, and include this section, provisions regarding warranties and liabilities, indemnification, and confidentiality and non-disclosure.
- 15. INTERPRETATION.** Any ambiguity in this Privacy and Security Agreement will be resolved to permit ODHS to comply with applicable privacy and security laws and State of Oregon and ODHS policies interpreting those laws.
- 16. SUBCONTRACTORS.** County shall ensure all subcontractors providing services related to this Privacy and Security Agreement are held to the same requirements as the County.

**EXHIBIT H, PART 2**  
**THIRD PARTY INFORMATION SYSTEM ACCESS REQUEST (FORM MSC 0785)**  
**See Attached**

## Third Party Information System Access Request

An DHS or OHA program completes this form to request access for a **third-party entity\*** (*organization or individual*) to data within an DHS or OHA information system or network.

*\*Please note that each entity only needs one form.*

 Hover over **blue** text for more information.

Request type ( <i>required</i> ): New request (ISPO will add agreement number)	Agreement number: blank
---	----------------------------

### Section 1. Third party information

This section defines the third party needing access to DHS/OHA network and information system(s). A third party is any individual or entity that is not part of the DHS/OHA workforce. Workforce means employees, volunteers, trainees and other individuals whose DHS or OHA work is under that agency’s direct control. This applies to paid and unpaid workforce members.

#### Third-party agreement administrator contact information

*This individual signs the contracts for the third party. (This is NOT a DHS/OHA employee.)*

Organization/entity name: Tillamook County	
Contact name ( <i>first, last</i> ):	Bill Baertlein, Isabel Gilda
Position/title:	Unsure
Work street address:	201 Laurel Ave.,
City, State, ZIP:	Tillamook, OR 97141
Phone:	(503) 842-3403
Email:	bbaertle@co.tillamook.or.us, igilda@co.tillamook.or.us
Website address ( <i>optional</i> ):	

#### Additional contact for third party

*This individual will be the contact for setting up or terminating users for the third party. (This is not a DHS/OHA employee.)*

Same contact information as above.

## Section 2. Governing contract details

A DHS/OHA employee fills out this section. If a [governing contract](#) applies, please complete all applicable fields, below.

Does a governing contract establish a need for access?  Yes  No

### Background checks

Please ensure all applicable required background checks are completed. DHS and OHA systems containing or accessing regulated data may require additional background check requirements beyond the pre-employment background checks. Regulated data sets requiring additional background checks include but are not limited to:

- Criminal Justice Information (CJI) in the Criminal Justice Information Services (CJIS) policy, 5.12.1 Personnel Security Policy and Procedures
- Federal tax information (FTI) as documented in Internal Revenue Service (IRS) Publication 1075, 5.1.1 Background Investigation Minimum Requirements.

Direct questions related to the background check process to [BCU.Info@state.or.us](mailto:BCU.Info@state.or.us) or 503-378-5470 or 1-888-272-5545.

## Section 3. Access description

### Reason for access

Describe in detail the [business need](#) for access:

3rd party needs to access CAM, eXPRS and ASPEN to provide complete case management entity contract requirements. Individual access will be based on each user and their responsibilities.

Requested access start date: \_\_\_\_\_

### Method of access

Check all methods the third party will use to access DHS/OHA information systems.

- DHS/OHA on-site Will only use DHS/OHA supplied PC, laptop or workstation:  Yes  No
- Remote access via [VPN](#) Will only use DHS/OHA supplied PC, laptop or workstation:  Yes  No
- Remote access via [Citrix](#)
- Access to folder on [Secure File Transfer Protocol \(SFTP\) server](#)
- Other (*explain below*): Will only use DHS/OHA supplied PC, laptop or workstation:  Yes  No

### Access and information flow will occur from:

DHS/OHA to third party (i.e., third party has access to DHS/OHA's information assets and systems)

### Scope of access

List all system names the third party needs to access. (*This form authorizes access for the third-party organization as a whole. A partner number [P#] and a network login are needed to access the following information systems. The system-specific [individual user access request forms](#) must be used to request access for individual third-party employees using the system.*)

- Email:** DHS/OHA email account authorized. This authorizes the third party to get DHS/OHA email accounts after receiving a completed individual user access request form for each individual.

- Network:** Network login authorized. This authorizes the third party to get DHS/OHA network login IDs after receiving a completed individual user access request form for each individual.

## System 1

**Name of system: CAM**

Type of access requested: Read/write (please describe):

Description of access:

Per the contract, CDDP must record all serious incidents, complaints of abuse, death reviews, and abuse investigations in the ODHS approved Centralized Abuse Management (CAM) System.

Expiration date of access:

### Information type

Will information being shared or accessed be identifiable (*i.e., names, DOB, address, etc.*)?

Yes  No

**If yes**, what protected information will be shared or accessed? (*Check all that apply.*)

- Protected health information (PHI)  Personally identifiable information (PII)  
 Financial information  Federal tax information (FTI)  
 Criminal justice information (CJI)  Payment card information (PCI)  
 Social Security Administration (SSA data)  
 Other (*list below*):

### Information owner review (*internal use only*)

Name of reviewer: Lea Ann Stutheit

Review date: insert

### Access determination:

Role or group assigned (*if applicable*):

Access is: Choose one

Reason for determination:

## System 2

**Name of system: eXPRS**

Type of access requested: Read/write (please describe):

Description of access:

Per the contract, CDDP shall upload all applicable documentation supporting the service authorization and rates within eXPRS.

Expiration date of access:

### Information type

Will information being shared or accessed be identifiable (*i.e., names, DOB, address, etc.*)?

Yes  No

### Information owner review (*internal use only*)

Name of reviewer: Lea Ann Stutheit

Review date: insert

### Access determination:

Role or group assigned (*if applicable*):

Access is: Choose one

Reason for determination:

**System 3**

**Name of system: ASPEN**

Type of access requested: Read/write (please describe):

Description of access:  
To provide complete case management entity contract requirements.

Expiration date of access:

**Information type**

Will information being shared or accessed be identifiable (i.e., names, DOB, address, etc.)?

Yes  No

If yes, what protected information will be shared or accessed? (Check all that apply.)

Protected health information (PHI)  Personally identifiable information (PII)

Financial information  Federal tax information (FTI)

Criminal justice information (CJI)  Payment card information (PCI)

Social Security Administration (SSA data)

Other (list below):

**Information owner review (internal use only)**

Name of reviewer: ISPO will staff to ASPEN BA Review date:

**Access determination:**

Role or group assigned (if applicable):

Access is: Choose one

Reason for determination:

Check all methods the third party will use to access DHS/OHA information systems.

**Section 4. Program sponsor**

The **program sponsor** is the DHS or OHA manager who sponsors the requested access. That person must monitor and ensure the third party complies with the terms and conditions of the access agreement. (Note that the program sponsor is usually the contract administrator of the governing contract authorizing the access.)

**Verification of need to know:**

As program sponsor, I certify that sections 1 through 3 of this form note the minimum necessary access.

Date: insert \_\_\_\_\_

Name (first, last):	Lea Ann Stutheit
Position/title:	COO
Office:	DHS
Program:	ODDS
District name:	N/A

Work street address:	550 Capitol St NE
City, State, ZIP:	Salem, OR 97301
Phone ( <i>include ext.</i> ):	503-945-6675
Email:	leaann.stutheit@dhsoha.state.or.us

## Section 5. Program requestor

The [program requestor](#) is the DHS or OHA staff person who works with the third party on a day-to-day basis. That person requests the access agreement for the third party. The requestor can be the same person as the program sponsor or contract administrator. However, a program can list separate requestors/contract administrators. This will ensure all relevant parties receive contract communication and expiration notices.

**Check this box and skip this section if the program requestor is also the program sponsor.**

## Submission

Click the submit button below to submit electronically, or email this completed form to the Information Exchange (InfoEx) Program within the Information Security and Privacy Office at [DHSOHA.InfoEx@dhsoha.state.or.us](mailto:DHSOHA.InfoEx@dhsoha.state.or.us). You can also email this address if you need more help.

Policy reference: <https://apps.state.or.us/Forms/Served/de090-003.pdf>

**Submit by email**

### DHS/OHA Information Security and Privacy Office use only

Date received:	Date completed:
Date approved by all information owners:	Date executed:
Notes:	
Completed by:	