State of Hawaii
NON-Employee
Remote Access Agreement

The State of Hawaii, Office of Enterprise Technology Services, hereby known as the “State”,
maintains remote access for certain Remote Users who require an electronic connection to State
systems from off-site locations to support government business.

Remote Access Agreement

1. **Acceptable Use standard.** Remote User agrees to read and adhere to the State’s Acceptable Use
   policy (103.001) while connected to and utilizing any information system remotely.

2. **Protection of Confidential Information.** Remote User agrees to protect the confidentiality,
   integrity and availability of all electronic information at all times. Remote User
   agrees to comply with all organizational policies, state and federal laws and regulations concerning
   the security and privacy of confidential information.

3. **Passwords and Codes.** Remote User agrees to NOT share passwords, codes, credentials, or user
   accounts with others.

4. **Appropriate Safeguards.** Remote User agrees to take proper steps to ensure the security of the
   device in which they connect to State systems remotely. Remote User agrees not to copy
   information accessed remotely to local devices and or portable devices. Printing information is
   also not permitted unless specific authorization has been granted.

5. **Auditing and logging.** Remote User agrees that his/her remote access is subject to review and/or
   audit by the State. Upon notice, Remote User agrees to return any State-owned portable
   device for purposes of ensuring compliance with this Agreement and the policies described herein.

6. **Response to Confidentiality Concerns.** Remote User acknowledges that if the State
   determines in its discretion that remote access has been compromised by unauthorized parties, or
   that remote access has been misused, any or all of the following actions may be taken:
   a. Remote Access terminated or disabled.
   b. Notification to Remote User and/or Remote User’s supervisor of concerns related to
      remote access.
   c. Termination of this agreement.
   d. Notification of the human resources department, information security officer, and/or
      information privacy officer may occur.

7. **Notification of Breach.** During the term of this Agreement, Remote User shall notify the State
   within (24) hours of any suspected or actual breach of security, intrusion or unauthorized use of
   disclosed confidential information of which Remote User becomes aware.
8. **Non-Disclosure Statement.** Remote User acknowledges and agrees that access of information through use of State systems warrants access to the State’s network and confidential information. Authorized individuals listed on this form who access the State System shall treat the data contained therein as confidential, and shall not disclose or otherwise make available such information and data to any other person, except in accordance with all applicable information confidentiality laws, rules and regulations. Do not print or access information unless authorized to do so. Remote User agrees to abide by applicable federal and state laws and regulations governing the privacy and security of protected information. Violators will be prosecuted to the full extent of the law for criminal charges and/or monetary damages and shall indemnify and hold harmless the State against all liability resulting from violations or alleged violations. Remote User shall ensure to the State that all information shall not be accessed through equipment at any site not previously approved by the State. Remote User shall immediately notify the State of any unauthorized access via their computer system.

9. **Termination of Agreement.** Should the authorized user no longer require access to the system, notification of such change shall be made within 24 hours to the State. Upon termination, all access information shall be destroyed or returned to the State. Notwithstanding the foregoing, State reserves the right to terminate this Agreement at any time.

10. **Personal Device Authorization Responsibilities.** Remote User will comply with the following for authorization of personal device for State work:
   - Provide hardware manufacturer, model, hostname and operating system version
   - Provide the anti-malware software installed on device
   - The device must require a password to unlock/access device
   - Local drives are required to be encrypted at all times
   - Ensure operating system software has the most recent updates applied (within 30 days)
   - Ensure critical operating system updates are applied immediately (within 14 days)
   - Ensure anti-malware software has the most recent updates applied (within 30 days)
   - Resubmit this form if approved hardware information changes

11. **Secure Access Data Requirements.** Remote User is prohibited from any action that would compromise good data custodian practices. These include:
   - State of Hawaii owned data will be stored in secured cloud storage platforms at a priority
   - Remote User is prohibited from conducting work on shared hardware
   - Remote User is prohibited from connecting to VPN through insecure wireless access points
   - Remote User will notify ETS Security Staff upon awareness of endpoint compromise
   - Remote User will facilitate access to ETS Security Staff if required for remediation
State of Hawaii
NON-Employee
Remote Access Agreement

Remote Access Agreement Acknowledgement
By completing and signing this form, you acknowledge that you have read and understand the
aforementioned agreements and all supported policies that pertain to it. All policies are available upon
request from the State.

To complete this form: Fill out all sections of this form, Please print clearly. Incomplete or illegible forms will
not be processed and may be returned, Return this page only. All other pages are for your records.

### Remote User Information:

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Department Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Email Address</th>
<th>State of Hawaii Sponsor's Name/Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(The State representative approving remote access)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supervisor Name</th>
<th>Supervisor Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardware Make and Model</th>
<th>Operating System</th>
<th>Anti-malware Installed</th>
<th>Encryption?</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remote User Signature
(If you have read the above and agree to all terms and conditions contained therein.)

<table>
<thead>
<tr>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Authorized State Agent Signature
(If authorized remote access for the above non-employee.)

<table>
<thead>
<tr>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Note: This form is only an acknowledgment for the authorization of remote access and does not grant the user
access to any information system within the State of Hawaii network infrastructure. All requests for access
to information systems must be completed and submitted by a State of Hawaii Sponsor.

Attach completed forms to "Internet VPN" ITRS ticket
ACKNOWLEDGEMENT OF POLICIES

IFB SPB-2022-03

Provision of Tenant Income Recertification Services for the Section 8 Subsidy Program on Oahu

Bidder hereby acknowledges and agrees to comply with the following State of Hawaii policies/agreement as provided in Attachments 16, Attachment 17, and Attachment 18 of Invitation for Bids SPB-2022-03:

- State of Hawaii Office of Enterprise Technology Services Policy No. 508 – Secure Device Policy;
- State of Hawaii Office of Enterprise Technology Services Policy No. 508.01 - Secure Device Standards;
- State of Hawaii Office of Enterprise Technology Services Policy No. 509 – Secure Access Policy – Next Generation Network; and
- State of Hawaii Department of Human Resources Development Policy No. 103.001 – Acceptable Usage of IT Resources.

State of Hawaii Non-Employee Remote Access Agreement

Signed Acknowledgement/Agreement to the specific policy/agreement shall be provided to the HPHA prior to commencement of services should a Contract be awarded.

Legal Name of Bidder (Company Name)

Authorized Signature

Name and Title of Authorized Signer
Statement of Experience

All questions 1 through 5 must be answered and the data given must be clear and comprehensive. If necessary, add separate sheets for items marked (*).

1. Name of offeror.

2. How many years have you/your company been engaged in providing Federal Section 8 or public housing tenant income recertification services?

3. *List individuals who will be dedicated to performing services under the resulting Contract if awarded and provide their experience in Section 8 or public housing tenant income recertification services.

4. *Have you ever defaulted on a contract? If so, where and why?

5. List three (3) professional references to include name, company/agency, contact phone and email address.

The undersigned hereby authorizes and requests any person, firm, or corporation to furnish any information requested by the Hawaii Public Housing Authority in verification of the recitals comprising this Statement of Experience.

______________________________________________
Legal Name of Bidder (Company Name)

______________________________________________
Authorized Signature

(Offeror may submit additional information if desired.)

IFB SPB-2022-03
Tenant Income Recertification