Policy for Remote Access for LHC Board of Directors

To the LHC Board Data Room

This Policy of the Louisiana Housing Corporation ("LHC") governs the policy and process by which the LHC Board of Directors ("Users") are granted access to Data in the LHC Board Data Room ("Data Room"):

1. Definition of Users

For the purposes of this Policy, authorized Users of the Data Room shall be limited to duly appointed and sworn-in members of the LHC Board of Directors as authorized in the LHC Act (LA R.S. 40:600.89).

2. Data Access to be Provided

The LHC Board Data Room shall consist of non-competitive, non-private, non-sensitive, non-confidential data from LHC Program Files (with certain exceptions listed herein), Policy Data and Reporting. The Data Room shall not include data from Program Files related to Homelessness Solutions, Rental Assistance, Energy Assistance, PBCA, Single Family Loan, and certain Disaster Recovery Programs data as those files contain personally identifiable information ("PII") and/or personally protected information ("PPI"). The Data contained in the Data Room shall include a "look back" period of five (5) years.

3. **Data Not Provided in Data Room**

If the need arises for a User to access information that is not provided in the Data Room, a request of the User shall be made, in writing, to the LHC Executive Director and the LHC Board Secretary and such request will be reviewed by the Department Head and a member of the Legal Department who must approve the provision of the Data and in what form to be provided. Data pertaining to RFP responses and other competitive open funding rounds shall not be provided until the funding process is complete.

4. **Use of Data**

The use of the Data in the Data Room shall only be used for relevant LHC business purposes and will be "Read Only" access. The Data in the Data room shall not be copied, printed, photographed, screenshotted, or otherwise saved or distributed for any

DRAFT

purpose. The Data Room and the Data it houses shall not be revealed, shown, left unattended or otherwise made accessible to a third-party. Requests for copies may be made to the LHC. Access to the Data must be done in accordance with this Policy and use of the Data must be in accordance with this Policy, all applicable LHC policies and applicable law.

5. **Requirements to Access the Data in the Data Room**

a. Computers used to access the Data Room must meet one of these minimum specifications which must remain updated to facilitate software End of Life, critical patch releases or vulnerability disclosures:

    1. Windows 10 or Windows 11 operating systems with all current security patches;
    2. MacOS12 (Monterey), 13 (Ventura) or 14 (Sonoma) with all current patches;
    3. ChromeOS 126 with all current security patches.

b. The Data Room shall only be accessed using one of the following up-to-date browsers OR the Parallels Desktop Client:
    1. Blink based (Chrome, Edge, Brave, Opera)
    2. Safari
    3. Firefox

c. A virus scanner is recommended for all systems and required for Windows systems. Some examples of acceptable virus scanners are as follows:
    1. Paid: Norton, McAfee, Symantec, WebRoot, Sophos Home
    2. Free: Microsoft Defender Antivirus, ClamAV (ClamWin)
    3. Freemium: AVG, Avira, Avast, BitDefender

d. Wi-Fi connections must be WPA2, WPA3 or WPA Enterprise. The Data Room shall not be accessed on networks that are open to the public, unfamiliar or do not require a password.

e. A smart phone running either iOS or Android can be used to access the Data Room only if it has installed and is running a TOTP Authenticator app. The LHC Technology Services (TS) Department can provide information on how to install the TOTP Authenticator app and is available, upon request, to assist with process.

f. The User must complete a training course on cybersecurity. The training is offered through the State of Louisiana or the User can attend an LHC hosted cybersecurity seminar within 30 days of request for access. The User can also attend a CISA federal cybersecurity training, which is an online training that provides a certificate of completion. One of the acceptable cybersecurity training options must be completed prior to access being provided.

DRAFT

g. The User must sign a Non-Disclosure Agreement provided by LHC prior to accessing the Data Room or any Data contained therein.
h. The User must comply with all LHC policies and manuals regarding the acceptable use of Data, which will be provided to the User including any requirements related to privacy, non-password sharing and inappropriate use of the Data.

6. Consequences for Failure to Comply

Failure to comply with the requirements set forth in this Policy may result in termination of the ability of the User to access the Data Room and/or may be subject to civil or criminal proceedings depending on the type of violation.

7. Use of the System May be Reviewed

The Use of the Data Room may be audited or reviewed for compliance or otherwise as deemed appropriate and necessary by the LHC.

DRAFT