we make housing affordable™
Florida Housing
Finance Corporation

227 North Bronough Street, Suite 5000 • Tallahassee, Florida 32301
850.488.4197 • Fax: 850.488.9809 • www.floridahousing.org

November 27, 2023

Florida Dept. of Management Services
ATTN: Adam Taylor
2555 Shumard Oak Boulevard
Tallahassee, FL 32399
Sent via e-mail to: Adam.Taylor@dms.fl.gov

Re: Termination of Agreement #DMS-22/23-136

Dear Mr. Taylor:

In accordance with Section VII. B. of our State Affiliate Data Sharing Agreement referenced above, please accept this letter as Florida Housing Finance Corporation's notice of intent to terminate the contract, effective December 27, 2023. We would like to thank you and your team for working with us over the past several months on this initiative and look forward to opportunities to partner again in the future.

Sincerely,

Angeliki G. Sellers
Chief Financial Officer

AGS/jam

cc: Jeremy Rogers, Department of Management Services
David Hearn, Florida Housing Finance Corporation
Bryan Spaulding, Florida Housing Finance Corporation

DMS-22/23-136

State Affiliate Data Sharing Agreement
between

Florida Department of Management Services
and

STATE AFFILIATE

This Agreement ("Agreement") is between the Florida Department of Management Services, on behalf of the Florida Digital Service ("FLDS"), and the Florida Housing Finance Corporation, a public instrumentality that performs an essential public function as codified in Section 420.504(2), Florida Statutes ("State Affiliate"). FLDS and State Affiliate are referred to herein individually as a "Party" or collectively as the "Parties."

Purposes

FLDS and State Affiliate enter into this Agreement in accordance with the Program. State Affiliate desires to utilize software licenses, applications, and solutions, as applicable, in connection with one or more projects (the "Projects") as described in one or more riders attached hereto (the "Project Rider" or collectively the "Project Riders"), and to integrate such with the State's Cybersecurity Operations Center (CSOC). Pursuant to section 282.318(3), Florida Statutes, FLDS's State Chief Information Officer is responsible for "the development, operation, and oversight of cybersecurity for state technology systems," which necessarily includes those of state agencies and other public instrumentalities that perform essential public functions, such as the State Affiliate. This Agreement describes the terms and conditions for the use of software licenses, applications, and solutions and protection of Covered Data, including requirements to safeguard the availability, confidentiality, and integrity of Covered Data in furtherance of the security objectives of Chapter 282, F.S.

I. Definitions

A. Access – The authorization to inspect, review, transmit, duplicate, communicate with, retrieve data from, or otherwise make use of any Covered Data, regardless of type, form, or nature of storage. "Access" to a computer system or network includes local and remote access, as applicable.

B. Agreement Coordinators – The individuals appointed by the signatories to this Agreement as the point of contact for this Agreement, who are responsible for ensuring that the Authorized Users comply with the activities identified herein.

C. Authorized Purpose – The purpose(s) for which an Authorized Third Party may access, use, or disclose the Covered Data.

D. Authorized Third Party – An individual, state agency, other Florida state or local governmental entity, or a private sector contractor or service provider of the State Affiliate which receives Covered Data.

E. Authorized User – An individual granted Access or to use Software Entitlement by either

FLDS or State Affiliate.

F. Covered Data – The limited subset of security data that is derived from State Affiliate's use of any Software Entitlements as defined in the attached Rider(s); an State Affiliate's confidential or proprietary information; and personal information as defined under section 501.171, F.S., and any other applicable privacy or data breach notification laws as may exist.

G. Data Breach – Either (1) any unauthorized access to, or use or disclosure of, Covered Data for any purpose other than as expressly permitted by this Agreement or required by law; or (2) a breach of privacy or of the security of the Covered Data. Good faith access of data by an employee or agent of the State Affiliate does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

H. Florida Enterprise Cybersecurity Resiliency Program ("the Program") – refers to the Program established by FLDS in accordance with the 2021-2022 General Appropriations Act to enhance the state's enterprise cybersecurity framework, identify and respond to risks, develop specialized training and awareness campaigns, and protect the infrastructure of state government from threats by implementing initiatives designed to meet the recommendations in the Florida Cybersecurity Task Force Final Report.

I. HIPAA - Health Insurance Portability and Accountability Act of 1996.

J. Information Technology (IT) Coordinators – The individuals appointed by the signatories to this Agreement as responsible for data flow and other technology-related considerations under this Agreement.

K. Information Technology Resources – As defined in section 282.0041, Florida Statutes, the data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. As used in this Agreement, the term also includes the definition for "Information Technology," as defined in section 282.0041, Florida Statutes, to add equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form.

L. Software Entitlement – Proprietary software utilized under this Agreement, which is identified in a Project Rider, and integrated into the State's CSOC.

II. Responsibilities of the Parties

A. **Data Transmission**. Covered Data shall only be transmitted through secure file transfer protocol or other secure transmission methods utilizing a National Institute of Standards and Technology approved means of electronic encryption as well as password protection and in a file format and layout determined by FLDS. Covered Data shall not be transmitted via any other means, including electronic mail. If applicable to any transmission of the Covered Data, both transmitting and receiving State Affiliate shall completely and

permanently remove Covered Data from any temporary transfer location within twenty-four (24) hours of receipt of the Covered Data.

B. **Compliance with Applicable Laws**. Each Party covenants and agrees that, in the performance of this Agreement, it shall comply with all applicable federal, state, and local laws, statutes, and regulations including, but not limited to, such laws set forth in Article VI as applicable to a Project and such other data privacy or security laws, all as they exist now and as they may be amended from time to time ("Applicable Laws"). In the event of any notice of a material violation of Applicable Laws, or an investigation into an alleged material violation, the affected Party shall promptly notify the other in writing of such notice.

C. **Compliance with Information Security Standards**. Each Party covenants and agrees to comply with Rule Chapter 60GG-2, Florida Administrative Code ("Security Standards"), with respect to its obligations under this Agreement. State Affiliate shall implement the Security Standards with respect to its obligations under this Agreement as an "Agency," regardless of whether they meet the definition of "Agency" in Rule Chapter 60GG-2, Florida Administrative Code.

FLDS, State Affiliate, and Authorized Third Parties shall implement reasonable and appropriate administrative, technical, and physical safeguards to maintain the security and protect the confidentiality, integrity, and availability of Access.

State Affiliate shall instruct all its Authorized Users with the opportunity for Access on the safeguards and requirements of the Agreement and all applicable federal and state requirements.

D. **HIPAA Business Associate Agreement.** To the extent that a Party is acting as a Business Associate (as defined by HIPAA) of the other Party, the Parties further agree to enter into a Business Associate Agreement as necessary, in the form of a mutually agreed-upon appendix to the Agreement.

E. **Incorporation and Compliance with Exhibits, Appendices and Riders, if Applicable.** The Project Riders, and any exhibits or appendices to this Agreement are hereby incorporated and made a part hereof and are an integral part of this Agreement. Each Rider, Exhibit, and Appendix attached hereto or referred to herein are hereby incorporated in and made a part of this Agreement as if set forth in full herein.

III. FLDS Role and Responsibilities

A. FLDS is responsible for:

1. Processing Covered Data in accordance with the State Cybersecurity Act;

2. Facilitating data sharing with the State Affiliate and/or an Authorized Third Party in accordance with this Agreement;

3. Providing the State Affiliate with the option to integrate its Software Entitlements with the CSOC; and

4. Protecting the integrity of Covered Data obtained by FLDS through State Affiliate's integration of any of the Software Entitlements with the CSOC. FLDS will not disclose this Covered Data to any third party unless required by law or as otherwise authorized by State Affiliate.

B. FLDS will only access, use, or disclose Covered Data, as permitted by State Affiliate, as required by Applicable Law, or as necessary for completion of its responsibilities under this Agreement, including any Project Riders. FLDS will ensure that its Authorized Users only access, use, or disclose Covered Data, as permitted by State Affiliate, as required by Applicable Law, or as necessary for completion of its responsibilities for any Projects, as assigned by FLDS.

C. FLDS will exercise reasonable care and no less than the same degree of care FLDS uses to protect its own confidential information to prevent confidential information from being used in a manner that is not expressly a purpose authorized in this Agreement or as required by Applicable Law.

IV. State Affiliate's Role and Responsibilities

A. Covered Data is and shall remain the property of State Affiliate.

B. State Affiliate is solely responsible for its Access to and use of Software Entitlements and Covered Data, including:

1. Procuring the Software Entitlement for State Affiliate's use and taking all steps necessary to allow integration of the Software Entitlement into the CSOC.

2. Ensuring a level of security appropriate to the risk in respect of Covered Data;

3. Securing State Affiliate's and its Authorized Users' systems and devices that can Access FLDS systems and Software Entitlements and complying with the Security Standards;

4. Selecting and/or ensuring that State Affiliate has selected its Authorized Users; activating and deactivating the Access, credentials, and privileges of its Authorized Users; and managing access controls to the FLDS system and Software Entitlements in a timely manner in accordance with the Security Standards;

5. Securing the account authentication credentials, systems, and devices of State Affiliate personnel who the State Affiliate designates to be Authorized Users;

6. Managing the compliance of its Authorized Users with the State Affiliate's established security measures and as required by Applicable Law;

7. Maintaining audit logs, as deemed necessary by the State Affiliate to demonstrate compliance with its obligations under this Agreement;

8. Backing up Covered Data, if required by law or State Affiliate policy; and

9. Ensuring that it and its Authorized Users remain in compliance with the terms and

conditions of any Software Entitlements.

C. FLDS is not responsible for, and has no obligation for:

1. Procuring the Software Entitlement for State Affiliate or providing warranty regarding such Software Entitlement or services provided related thereto, regardless of the entity providing such services.

2. Selecting or verifying State Affiliate's Authorized Users, activating or deactivating the Access or credentials of Authorized Users; or

3. Protecting Covered Data that State Affiliate elects to store or transfer outside of FLDS's and its sub-processors' systems (for example, offline or on-premises storage).

V. Unauthorized Disclosure/Data Breach

A. In the event of a Data Breach of the Covered Data while in State Affiliate's (or an Authorized Third Party's) custody or control or as a result of State Affiliate's (or an Authorized Third Party's) access to or use of the Covered Data, which requires the provision of notice in accordance with section 501.171, F.S., or other Applicable Law (including, but not limited to, HIPAA), the Parties agree as follows:

1. State Affiliate shall notify FLDS of the Data Breach not more than 24 hours after discovery that a Data Breach has occurred or is reasonably likely to have occurred.

2. State Affiliate (or its Authorized Third Party) shall be responsible for all costs related to the Data Breach including FLDS' and/or State Affiliate's (or an Authorized Third Party's) costs of complying with all legal requirements, including the requirements for Data Breach notification under Applicable Law, as well as defending any claims, actions, or lawsuits related thereto.

3. If a Data Breach is subject to the notice provisions of section 501.171, F.S., or Applicable Law, the Parties agree to cooperate and work together to ensure full legal compliance and to provide breach notification to the extent required by Applicable Law. State Affiliate shall use its best and diligent efforts to identify the individuals entitled to receive notice of the Data Breach and obtain the names and mailing information of such individuals, so that FLDS and/or State Affiliate are able to distribute the notices within the legally required time periods. FLDS and/or State Affiliate, as applicable, shall bear its internal administrative and other costs incurred in identifying the affected individuals and their mailing information.

4. In the event of a Data Breach, including the privacy or security of the Covered Data, while in the custody or control of the State Affiliate, if the State Affiliate must provide notice as a result of the requirements contained in section 501.171, F.S., or other Applicable Law, the State Affiliate shall submit a draft of the notice to FLDS for prior review and approval of the contents of the notice, prior to disseminating the notice. Such approval shall not be unreasonably delayed or withheld.

B. If State Affiliate experiences a breach of the security of its systems that results in a breach of the security of FLDS's systems ("FLDS Breach"), State Affiliate shall be responsible for all costs related to the FLDS Breach including FLDS's costs of complying with all legal requirements, including any costs for data breach notification under section 501.171, F.S.,

or Applicable Law, as well as defending any claims, actions, or lawsuits against the FLDS related thereto. State Affiliate, at its own expense, shall cooperate fully with FLDS in the investigation, eradication, remediation, and recovery from the FLDS Breach.

C. If FLDS experiences a breach of the security of its systems that results in a breach of the security of State Affiliate's systems ("State Affiliate Breach"), FLDS shall be responsible for all costs related to the State Affiliate Breach including State Affiliate's costs of complying with all legal requirements, including the requirements for data breach notification under section 501.171, F.S., or Applicable Law, as well as defending any claims, actions or lawsuits related thereto. FLDS, at its own expense, shall cooperate fully with State Affiliate in the investigation, eradication, remediation, and recovery from the State Affiliate Breach.

D. If either FLDS or State Affiliate is obligated under this Section to pay costs incurred by the other Party, the Party required to pay such costs shall submit a draft of the legal notifications and other public communications to the other Party for prompt review and approval of the contents prior to disseminating the notification or communication. Such approval shall not be unreasonably delayed or withheld.

E. The Parties understand and agree the provisions of this Agreement relating to the protection and security of the Covered Data constitute a material condition of this Agreement.

VI. Additional Terms Applicable to Certain Circumstances.

A. The Parties shall define the type of Covered Data to be utilized in connection with each Project as set forth in the attached Project Rider(s). Such Covered Data may include confidential or sensitive information that is subject to additional confidentiality or security requirements as set forth in this Article VI and such Project Rider. In the event of a conflict between the terms and conditions of this Article VI and the remainder of the Agreement, the terms and conditions of Article VI shall control. Moreover, a Project may include the use of information described in more than one of the provisions set forth in this Article VI, or it may include the use of information not described in this Article VI. In the event of a conflict between or among the terms and conditions of Subsections B, C, D or E of this Article VI, the more restrictive terms and conditions shall apply unless otherwise provided by Applicable Law or guidance by the applicable regulatory enforcement agencies or bodies.

B. **CJIS**. The terms and conditions of this Section VI.B. apply when Covered Data involved in a Project includes criminal justice information.

1. CJIS Covered Data. Covered Data may also include, but shall not be limited to, CJIS Covered Data. For purposes of this Agreement, CJIS Covered Data shall mean criminal justice information that is provided by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) system and that is necessary for law enforcement and civil agencies to perform their missions, including, but not limited to, biometric, identity history, biographic, property, and case/incident history data.

2. Disclosure of CJIS Covered Data. The disclosure of CJIS Covered Data under the Agreement, as modified by this section, is governed by the CJIS Security Policy, available at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center. In accordance with the CJIS Security Policy and 28 CFR Part 20, use of the CJIS system under the Agreement is restricted to: detection, apprehension, detention, pretrial

release, post-trial release, prosecution, adjudication, correctional supervision, rehabilitation of accused persons or criminal offenders, and other legally authorized purposes.

3. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the CJIS Covered Data under the CJIS Security Policy.

4. Access Requirements. Unique authorization is required for Access to the CJIS Covered Data and must be properly authenticated and recorded for audit purposes, including CJIS security and other applicable audit requirements.

C. **HIPAA and State Protected Health Information.** The terms and conditions of this Section VI.C. apply when Covered Data involved in a Project includes protected health information and such other sensitive health information, the disclosure of which may be limited or restricted by law, including, but not limited to, mental health and drug and alcohol related information.

1. PHI Covered Data. Covered Data may also include, but shall not be limited to, PHI Covered Data. For purposes of this Agreement, "PHI Covered Data" shall mean "protected health information" or "PHI," as such term is defined by HIPAA. PHI shall include, but shall not be limited to, any other medical or health-related information that is afforded greater protection under more restrictive federal or state law, including, but not limited to, the Substance Abuse and Mental Health Services Act (SAMSHA), located at 42 C.F.R. Part 2, the Florida Mental Health Act (the Baker Act), located at Fla. Stat. § 394.451 – 394.47892, and the Hal S. Marchman Alcohol and Other Drug Services Act, located at Fla. Stat. § 397.301 et seq.

2. Disclosure of PHI Covered Data. The disclosure of PHI Covered Data under the Agreement, as modified by this section, is governed by HIPAA and more restrictive federal or state law, as applicable. Accordingly, the disclosure of PHI Covered Data under the Agreement is permitted only with the consent of the individual who is the subject of the PHI Covered Data, by court order that meets the requirements of applicable law, and for other purposes as permitted by Applicable Law.

3. Business Associate Agreement. To the extent that FLDS is a "Business Associate" of State Affiliate, as such term is defined under HIPAA, the Parties agree to enter into a mutually agreeable Business Associate Agreement.

4. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the PHI Covered Data under HIPAA and more restrictive federal or state law, to the extent applicable.

5. Access Requirements. Unique authorization is required for Access and must be properly authenticated and recorded for audit purposes, including HIPAA audit requirements and other audit requirements under more restrictive federal or state law, to the extent applicable.

D. **FERPA**. The terms and conditions of this Section VI.D. apply when Covered Data includes student education records as defined by the Family Educational Rights and Privacy Act, 20 USC §1232g, and its implementing regulations set forth at 34 CFR Part 99 (collectively,

"FERPA").

1. FERPA Covered Data. Covered Data may also include, but shall not be limited to, FERPA Covered Data. For purposes of this Agreement, "FERPA Covered Data" shall mean student education records as defined by FERPA).

2. Disclosure of FERPA Covered Data. The disclosure of FERPA Covered Data under the Agreement, as modified by this section, is governed by FERPA. Accordingly, the disclosure of FERPA Covered Data under the Agreement is permitted with parent or eligible student consent and, without such consent, in the following circumstances: (i) to school officials with legitimate educational interest; (ii) to other schools to which a student is transferring; (iii) to specified officials for audit or evaluation purposes; (iv) to appropriate parties in connection with financial aid to a student; (v) to organizations conducting certain studies for or on behalf of the school; (vi) to accrediting organizations; (vii) to comply with a judicial order or lawfully issued subpoena; (viii) to appropriate officials in cases of health and safety emergencies; (ix) to state and local authorities, within a juvenile justice system, pursuant to specific state law; and (x) as otherwise provided by FERPA.

3. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the FERPA Covered Data under FERPA.

4. Access Requirements. Unique authorization is required for Access and must be properly authenticated and recorded for audit purposes, including FERPA and any other applicable audit requirements.

E. **DPPA**. The terms and conditions of this Section VI.E. apply when Covered Data includes motor vehicle record information.

1. DPPA Covered Data. For purposes of the Agreement, Covered Data may include, but shall not be limited to, DPPA Covered Data. For purposes of this Agreement, "DPPA Covered Data" shall mean motor vehicle information as set forth in the Driver Privacy Protection Act, 18 U.S.C. § 2721 ("DPPA").

2. Disclosure of DPPA Covered Data. The disclosure of DPPA Covered Data under the Agreement, as modified by this section, is governed by DPPA. DPPA prohibits the disclosure of personal information, as defined in 18 U.S.C. § 2725(3), that is contained in motor vehicle records, but such information may be used by any government agency, such as FLDS and State Affiliate, in carrying out its functions. Such personal information may not be re-disclosed by FLDS or State Affiliate, however, except in accordance with the permissible uses set forth at 18 U.S.C. § 2721(b). With certain limited exceptions, DPPA further prohibits the disclosure of highly restricted personal information, as defined in 18 U.S.C. § 2725(4), without the express consent of the individual who is the subject of such information. In accordance with section 119.0712(2)(d)(2), F.S., the emergency contact information contained in a motor vehicle record, without the express consent of the person to whom such emergency contact information applies, may be released only to: (a) law enforcement agencies for purposes of contacting those listed in the event of an emergency; or (b) a receiving facility, hospital, or licensed detoxification or addictions receiving facility pursuant to sections 394.463(2)(a) or 397.6772(1)(a), F.S., for the sole purpose of informing a

patient's emergency contacts of the patient's whereabouts. E-mail addresses that are collected by the Florida Department of Highway Safety and Motor Vehicles also may not be disclosed pursuant to Section 119.0712(2)(c), F.S.

3. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the DPPA Covered Data under DPPA and the Florida Statutes referenced above.

4. Access Requirements. Unique authorization is required for Access and must be properly authenticated and recorded for audit purposes, including, but not limited to, compliance with these terms and conditions.

VII. Duration of Agreement and Designation of Agreement Coordinators

A. This Agreement will be effective on the date on which fully executed by both Parties and will terminate as set forth herein.

B. The Agreement may be mutually terminated by written agreement of the Parties or unilaterally by either party, without cause, provided the terminating party serves the other party's Agreement Coordinator with written notice of an intent to terminate the Agreement in no less than thirty (30) calendar days from the date such notice is sent.

C. In the event either party (the "Breaching Party") fails to fully comply with the terms and conditions of this Agreement, the other party ("Terminating Party") may terminate the Agreement upon no less than twenty-four (24) hours (excluding Saturday, Sunday, and Holidays) notice in writing to the Breaching Party. Such notice may be issued without providing an opportunity for cure if it specifies the nature of the noncompliance and states that provision for cure would adversely affect the interests of the State or is not permitted by law or regulation. Otherwise, notice of termination will be issued after a Breaching Party's failure to fully cure such noncompliance ten (10) days following the date of a written notice of noncompliance issued by the Terminating Party specifying the nature of the noncompliance and the actions required to cure such noncompliance. The Terminating Party's failure to demand performance of any provision of this Agreement shall not be deemed a waiver of such performance. The Terminating Party's waiver of any one breach of any provision of this Agreement shall not be deemed to be a waiver of any other breach and neither event shall be construed to be a modification of the terms and conditions of this Agreement. The provisions herein do not limit the Terminating Party's right to remedies at law or in equity.

D. The Agreement Coordinators and IT Coordinators for this Agreement are:

FLDS Agreement Coordinator:

Adam Taylor
2555 Shumard Oak Boulevard Tallahassee, FL 32399
Adam.Taylor@dms.fl.gov
850-728-6075

FLDS IT Coordinator:

Jeremy Rodgers
2555 Shumard Oak Boulevard Tallahassee, FL 32399
Jeremy.Rodgers@dms.fl.gov
850-509-9919

State Affiliate's Agreement Coordinator:

Bryan Spaulding
Director of IT Security
Bryan.Spaulding@floridahousing.org

State Affiliate's IT Coordinator:

David Hearn
CIO
David.Hearn@floridahousing.org

VIII. Amendments and Changes

A. With the exception of changes to Agreement and/or IT Coordinator designations, any changes, alterations, deletions, or additions to the terms set forth in this Agreement must be by written amendment executed by all Parties. Changes to the Agreement and/or IT Coordinator designations may be accomplished by providing email change notification that is acknowledged by both Parties.

B. The Parties agree to follow and be bound by the terms and conditions of any policy decisions or directives from the federal and state agencies with jurisdiction over the use of the data described herein upon receipt of written notice directing that such rules, policy decisions, or directives apply to this Agreement.

IX. Inspection of Records

Each Party shall permit the other Party and any other applicable state and federal representatives with regulatory oversight over the other Party, or their designees, to conduct inspections described in this paragraph, or to make on-site inspections of records relevant to this Agreement to ensure compliance with any state and federal law, regulation, or rule. Such inspections may take place with notice during normal business hours wherever the records are maintained. Each Party shall ensure a system is maintained that is sufficient to permit an audit of such Party's compliance with this Agreement and the requirements specified above. Failure to allow such inspections constitutes a material breach of this Agreement. This Agreement may be terminated in accordance with Section VII.C. for a material breach.

X. Governing Law and Jurisdiction

This Agreement shall be governed by and construed and enforced in accordance with the laws of the State of Florida and shall be binding upon the Parties hereto in the United States and worldwide. A state court of competent jurisdiction in Leon County, Florida, shall be the exclusive venue for any action regarding this Agreement.

XI. State Affiliate Additional Terms

A. Compliance with Laws

1. General Compliance. State Affiliate shall comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business and that are applicable to this Agreement, including those of federal, state, and local agencies having jurisdiction and authority, and shall ensure that any and all subcontractors utilized do the same. This requirement includes, but is not limited to, compliance with Chapters 282 and 287, F.S.; section 501.171, F.S.; Subtitles 60FF and 60GG, F.A.C.; Section 274A of the Immigration and Nationality Act; the Americans with Disabilities Act; the Health Insurance Portability and Accountability Act (HIPAA), if applicable; the Family Educational Rights and Privacy Act, if applicable; the Occupational Safety and Health Act, if applicable; and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status.

2. Conflict with Law. If the requirements of this Agreement conflict with any governing law, codes, or regulations, State Affiliate shall notify FLDS in writing and the Parties will amend this Agreement to comply with the applicable code or regulation.

B. Assignment and Contractors. State Affiliate shall not sell, assign, or transfer any of its rights, duties, or obligations under this Agreement. State Affiliate shall ensure all contractors that have Access to Covered Data or Software Entitlements comply with all requirements of this Agreement. The Software Entitlements shall not be Accessible by, or deployed on, Information Technology Resources not owned, employed, or controlled by State Affiliate.

C. Independent Entities. State Affiliate and its employees, agents, representatives, and subcontractors are not employees or agents of FLDS and are not entitled to the benefits of FLDS employees solely by virtue of this Agreement. FLDS will not be bound by any acts or conduct of State Affiliate or its employees, agents, representatives, or subcontractors.

D. Public Records. Article 1, section 24, Florida Constitution, guarantees every person access to all public records, and section 119.011, F.S., provides a broad definition of "public record." As such, records submitted to FLDS (or any other State agency, including State Affiliate) are public records and are subject to disclosure unless exempt from disclosure by law. It is understood by both Parties that portions of records each Party provides to the other may be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law ("Confidential Information").

In the event a Party receives a request for public records pursuant to Chapter 119, F.S., the Florida Constitution, or other authority (the "Receiving Party"), to which records that were provided by the other Party (the "Disclosing Party") are responsive, the Receiving Party shall provide the Disclosing Party notice of the request and an opportunity to review and redact the records prior to release. If a requestor asserts a right to the Confidential Information redacted by the Disclosing Party, it is the Disclosing Party's responsibility to take the appropriate legal action to assert that the information in question is exempt from disclosure under Chapter 119, F.S., or other applicable law.

In the event a Party becomes subject to a demand (the "Receiving Party") for discovery or disclosure of documents it received from the other Party (the "Disclosing Party") in a legal proceeding, the Receiving Party will give the Disclosing Party notice of the demand or request. If the Disclosing Party believes that Confidential Information is contained in the documents it provided, it shall take the appropriate legal action in response to the demand and to defend its claims of confidentiality. If the Disclosing Party fails to take appropriate and timely action to protect the records it has provided to the Receiving Party, the Disclosing Party agrees that the Receiving Party is permitted to treat those records as not confidential and to provide the unredacted records to the requester and the Disclosing Party shall not pursue any suit, action, or claim, including for damages, against the Receiving Party or its employees, attorneys, agents or volunteers.

IF STATE AFFILIATE HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE STATE AFFILIATE'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT THE TELEPHONE NUMBER, EMAIL ADDRESS AND MAILING ADDRESS PROVIDED FOR THE CONTRACT MANAGER.

E. Employment Eligibility Verification. State Affiliate has an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees in accordance with section 448.095, F.S. By executing this Agreement, State Affiliate certifies that it is registered with, and uses, the E-Verify system for all newly hired employees in accordance with section 448.095, F.S.

This section serves as notice to State Affiliate regarding the requirements of section 448.095, F.S., specifically sub-paragraph (2)(c)1, and FLDS' obligation to terminate the Agreement if it has a good faith belief that State Affiliate has knowingly violated section 448.09(1), F.S. If terminated for such reason, State Affiliate will not be eligible for award of a public contract for at least one (1) year after the date of such termination.

[signature page follows]

IN WITNESS WHEREOF, the Parties hereto execute this Agreement as of this __ day of _____, 2023.

FLORIDA DEPARTMENT OF MANAGEMENT SERVICES

DocuSigned by:
By: Pedro Allende
5E91A9D369EB47C...

Name: Pedro Allende

Title: Secretary

FLORIDA HOUSING FINANCE CORPORATION

DocuSigned by:
By: Michael DiNapoli
0BF0B5310408429...

Name: Michael DiNapoli

Title: Executive Director

RELEVANT FLORIDA STATUTES (2022)

Section 282.0051(1), Florida Statutes (F.S.), in relevant part, grants the Department of Management Services (Department), through the Florida Digital Service (FLDS), authority to develop and publish information technology policy for the management of the state's information technology resources; develop an enterprise architecture that acknowledges the unique needs of the entities within the enterprise in the development and publication of standards and terminologies to facilitate digital interoperability; establish best practices for the procurement of information technology products and cloud-computing services in order to reduce costs, increase the quality of data center services, or improve government services; and conduct annual assessments of state agencies to determine compliance with all information technology standards and guidelines developed and published by the department and provide results of the assessments to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

Section 282.0051(3), F.S., in relevant part, requires the Department, through the FLDS, to create, not later than December 1, 2022, and maintain a comprehensive indexed data catalog in collaboration with the enterprise that lists the data elements housed within the enterprise and the legacy system or application in which these data elements are located; develop and publish, not later than December 1, 2022, in collaboration with the enterprise, a data dictionary for each agency that reflects the nomenclature in the comprehensive indexed data catalog; adopt, by rule, standards that support the creation and deployment of an application programming interface to facilitate integration throughout the enterprise, standards necessary to facilitate a secure ecosystem of data interoperability that is compliant with the enterprise architecture, and standards that facilitate the deployment of applications or solutions to the existing enterprise system in a controlled and phased approach.

Section 282.0051(5), F.S., stipulates that the Department, through the FLDS, may not retrieve or disclose any data without a shared-data agreement in place between the Department and the enterprise entity that has primary custodial responsibility of, or data-sharing responsibility for, that data.

Section 282.318(3), F.S., in relevant part, names the Department, through the FLDS, the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures, and requires the Department, through the FLDS, to adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework; and requires the Department, through the FLDS, to designate an employee of the FLDS as the state chief information security officer responsible for the development, operation, and oversight of cybersecurity for state technology systems who shall be notified of all confirmed or suspected incidents or threats of state agency information technology resources and must report such incidents or threats to the state chief information officer and the Governor; develop, and annually update by February 1, a statewide cybersecurity

strategic plan that includes security goals and objectives for cybersecurity, including the

identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for a cyber incident; and develop and publish for use by state agencies a cybersecurity governance framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and cybersecurity audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency cybersecurity incident response teams and describing their responsibilities for responding to cybersecurity incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to a cybersecurity incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing a cybersecurity incident reporting process that includes procedures for notifying the department and the Department of Law Enforcement of cybersecurity incidents.

10. Incorporating information obtained through detection and response activities into the agency's cybersecurity incident response plans.

11. Developing agency strategic and operational cybersecurity plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

13. Establishing procedures for procuring information technology commodities and services that require the commodity or service to meet the National Institute of Standards and Technology Cybersecurity Framework.

14. Submitting after-action reports following a cybersecurity incident or ransomware

incident. Such guidelines and processes for submitting after action reports must be developed and published by December 1, 2022.

Section 282.318(3), F.S., additionally requires the Department, through the FLDS, to operate and maintain a Cybersecurity Operations Center led by the state chief information security officer, which must be primarily virtual and staffed with tactical detection and incident response personnel and shall serve as a clearinghouse for threat information and coordinate with the Department of Law Enforcement to support state agencies and their response to any confirmed or suspected cybersecurity incident.

Section 282.318(4), F.S., in relevant part, requires each state agency head to conduct, and update every three years, a comprehensive risk assessment to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency; develop, and periodically update, written internal policies and procedures, which include procedures for reporting cybersecurity incidents and ransomware incidents to the Cybercrime Office of the Department of Law Enforcement and the FLDS (such policies and procedures must be consistent with the rules, guidelines, and processes established by the Department to ensure the security of the data, information, and information technology resources of the agency); the internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from section 119.07(1), F.S., except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the FLDS , and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General; implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the department to address identified risks to the data, information, and information technology resources of the agency; the Department, through the FLDS, shall track implementation by state agencies upon development of such remediation plans in coordination with agency inspectors general; and develop a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents which is consistent with the security rules, guidelines, and processes established by the Department through the FLDS.

Section 119.0725, F.S., establishes that records related to agency cybersecurity information are confidential and exempt from section 119.07(1), F.S., and s. 24(a), Art. I of the State Constitution. Section 282.318(5), F.S., further establishes that the portions of risk assessments, evaluations, external audits, and other reports of a state agency's cybersecurity program for the data, information, and information technology resources of the state agency which are held by a state agency are confidential and exempt from section 119.07(1), F.S., and s. 24(a), Art. I of the State Constitution if the disclosure of such portions of records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

(a) Data or information, whether physical or virtual; or

(b) Information technology resources, which include:

1. Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

2. Security information, whether physical or virtual, which relates to the agency's

existing or proposed information technology systems; and

Section 282.318(7), F.S., establishes that portions of records made confidential and exempt in section 282.318(5), F.S., shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the FLDS, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General; such portions of records may be made available to a local government, another state agency, or a federal agency for cybersecurity purposes or in furtherance of the state agency's official duties.

Enterprise E5 and Azure Sentinel Deployment Rider

The terms and conditions set forth in this Project Rider ("Rider") apply to the Florida Digital Service, a part of the Florida Department of Management Services ("FLDS"), and the Florida Housing Finance Corporation ("State Affiliate") in connection with the State Affiliate Data Sharing Agreement ("Agreement") between FLDS and State Affiliate. Capitalized terms not otherwise defined herein are as defined in the Agreement. In the event of a conflict between this Rider and the Agreement, the terms of this Rider shall control.

I. Definitions

A. Customer Tenant – For the purpose of this Rider, the Customer Tenant is the Tenant directly managed and owned by State Affiliate.

B. Florida Enterprise Cybersecurity Resiliency Program ("the Program") – refers to the Program established by FLDS in accordance with the 2021-2022 General Appropriations Act to enhance the state's enterprise cybersecurity framework, identify and respond to risks, develop specialized training and awareness campaigns, and protect the infrastructure of state government from threats by implementing initiatives designed to meet the recommendations in the Florida Cybersecurity Task Force Final Report.

C. Licensed Software Solution – refers to one or more of the following Microsoft 365 E5 software: Defender for Office 365, Defender for Identity, Defender for Endpoint, Azure Active Directory Identity Protection, Microsoft Defender for Cloud Apps, Microsoft Endpoint Manager, and Log Analytics Workspace and Microsoft Sentinel.

D. Managing Organization – For the purpose of this Rider, the Managing Organization is FLDS.

E. Managing Tenant – For the purpose of this Rider, the Managing Tenant is the Tenant directly managed and owned by FLDS.

F. Telemetry Data – For the purpose of this Rider, Telemetry data refers specifically to data generated by automated communication processes from multiple data sources within the Licensed Software Solution and any other data in the Customer Tenant Log Analytics Workspace that is shared with FLDS.

G. Tenant – A Tenant provides identity and access management (IAM) capabilities to applications and resources within the defined environment. A Tenant is an identity security boundary that is directly managed by the owner of the application or resource.

H. View – The permissions granted for FLDS to see Telemetry Data provided to the Managing Tenant by the Customer Tenant. A View does not permit FLDS access to the State Affiliate data.

II. Statement of Work

A. **Purpose/Scope:** FLDS and State Affiliate enter into this Rider to establish the terms and conditions; and to establish the maintenance, use, and disclosure of the Telemetry Data generated by State Affiliate within the Customer Tenant to the Managing Tenant.

B. **FLDS Role and Responsibilities**: Upon request by State Affiliate, FLDS may provide access to the State's Cybersecurity Operations Center.

FLDS will access a View of the Telemetry Data provided within the Managing Tenant via Azure Lighthouse permissions to the Log Analytics Workspace of the Customer's Tenant.

FLDS will only use Telemetry Data for the express purpose of developing and implementing the Program. FLDS will not disclose the Telemetry Data to any third party unless required by law or as otherwise authorized by State Affiliate.

C. **State Affiliate's Role and Responsibilities:** State Affiliate is responsible for its access to and use of the Licensed Software Solution; activating and deactivating the access, credentials, and privileges of its authorized users; and managing access controls to FLDS and software solution licenses. Telemetry Data within the Customer Tenant is and shall remain the property of State Affiliate.

D. **Indemnification**:

a. Each Party shall be fully liable for the actions of its agents, employees, partners, and subcontractors, if any, and shall fully indemnify, defend, and hold harmless the other Party, and its officers, agents, and employees. For the avoidance of doubt, this is not intended to confer benefits on third parties.

b. Nothing contained herein shall constitute a waiver by either Party of its sovereign immunity and the limitation set forth in section 768.28, Florida Statutes.

III. Data Types

The data to be viewed by FLDS within the Managing Tenant is the Telemetry Data provided by the Customer Tenant. Telemetry Data is dependent on which components of the Licensed Software Solution are elected by the State Affiliate and includes the following:

____CJIS Covered Data
____HIPAA and State Protected Health Information
____FERPA Covered Data
____DPPA Covered Data
____Other _____
____N/A