This sample rider is not required for submission with your grant application. An Incident Response Rider will need to be executed within 30 days of award.

Cybersecurity Incident Response Rider

The terms and conditions set forth in this Cybersecurity Incident Response Rider ("IR Rider") apply to the Florida Digital Service, a part of the Florida Department of Management Services ("FLDS"), and the GRANTEE ("Grantee") in connection with the Grantee Data Sharing Agreement ("DSA") between FLDS and Grantee. Capitalized terms not otherwise defined herein are as defined in the DSA. In the event of a conflict between this IR Rider, the DSA, and any other rider, the terms of this IR Rider shall control.

I. Definitions

A. Cloud Console – The global administrative accounts for Software Entitlements directly managed and licensed by FLDS.

B. Customer Account – The accounts for Software Entitlements directly utilized by Grantee.

C. Local Government Cybersecurity Grant Program ("the Program") – The Program established by the 2022-2023 General Appropriations Act to improve county and municipal cybersecurity posture and resiliency.

D. Information Technology Resources – As defined in section 282.0041, Florida Statutes, data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. As used in this IR Rider, 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.

E. Managing Organization – The entity managing the use of the Software Entitlements and their Cloud Consoles. As used in this IR Rider, the Managing Organization is FLDS.

F. Protected Grantee Data – Data, not including Telemetry Data, maintained and generated by Grantee, which shall not be Accessed or Accessible by, or sent to, Software Entitlements.

G. Solution Data – Data, reports, or other information generated by Software Entitlements. This may be derived from, but does not include, Telemetry Data.

H. Telemetry Data –Data generated by Grantee through automated communication processes from multiple data sources and processed by Software Entitlements.

I. View - The permissions Grantee grants to FLDS to see Telemetry and Solutions Data provided to the Managing Organization by Customer Accounts. A View does not permit FLDS Access to Protected Grantee Data.

II. Purpose

FLDS and Grantee enter into this IR Rider to establish the terms and conditions for FLDS access to assist Grantee with responding to incidents.

III. Incident Response

A. **Incident Response Support**. Upon discovery of an incident, as determined by Grantee or FLDS, Grantee may request, or FLDS may offer to provide, incident response support. Access to Grantee Information Technology Resources shall be limited to the extent expressly agreed to by Grantee. Such Access and support are unilaterally terminable at any time by either Party. FLDS may establish, and Grantee shall comply with, protocols or procedures for reporting and requesting support for incidents under this IR Rider, responding to incidents, and the types of support available to be provided for an incident. Grantee shall mitigate the impact of the incident and preserve all relevant documents, records, and data. Grantee shall cooperate and coordinate with FLDS in responding to incidents where incident response support is received, including, but not limited to:

1. Assisting with any incident response related investigation by FLDS;
2. Providing FLDS with physical access to the affected facilities and operations;
3. Facilitating interviews with Grantee personnel; and
4. Making all relevant records, logs, files, data reporting, and other materials available to FLDS or Grantee-authorized third parties.

FLDS shall only Access Covered Data, other Grantee data, and Grantee Information Technology Resources as permitted by Grantee. Any specific limitations on such Access shall be documented.

Upon termination of each instance of incident response support, regardless of the reason for such termination, Grantee shall assist FLDS with any close-out or post-incident documentation upon request.

B. **Covered Data and Personally Identifiable Information**. FLDS will not disclose Covered Data or other data made Accessible during incident response support to any third party unless required by law or as authorized by Grantee. In the event such data is required by law to be disclosed, FLDS shall make best efforts to notify Grantee prior to such disclosure.

IV. FLDS Role and Responsibilities

FLDS shall provide Grantee with the option to utilize the Software Entitlements to enhance the Grantee's cybersecurity and protect the Grantee's infrastructure from threats.

FLDS will Access a View of the Telemetry Data and Solution Data. FLDS will only use Telemetry and Solutions Data for the purpose of developing and implementing the Program; identifying and responding to risks and incidents; and in furtherance of meeting FLDS' and Grantee's statutory and regulatory obligations. FLDS will not disclose the Telemetry Data and Solutions Data to any third party unless required by law or as otherwise authorized by Grantee. FLDS will provide incident response services and resources as allowed and agreed to by FLDS and Grantee in responding to risks and incident.

V. Grantee Roles and Responsibilities

Grantee shall cooperate with and provide all assistance necessary to FLDS' incident response support.

VI. Indemnification

See section W. Indemnification, of the Agreement.

VII. Liability and Termination of Incident Response Support

Except as described in the DSA or other riders, incident response services and resources of FLDS or Grantee-authorized third parties shall be provided by FLDS without warranty by, and without liability to, FLDS or such Grantee-authorized third parties. Upon request, FLDS or Grantee-authorized third parties shall provide reasonable assistance to return Grantee Information Technology Resources to the operational status prior to the involvement of FLDS incident response support.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK