



# SISE DATA PROVIDER AGREEMENT

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

Name and address of the "DATA PROVIDER": \_\_\_\_\_

This DATA PROVIDER AGREEMENT, effective as of the date first written above, is between the All Hazards Consortium ("AHC") and the DATA PROVIDER identified above.

**WHEREAS**, AHC is a nonprofit organization focused on public/private collaboration in support of homeland security, business continuity, and disaster preparedness, response & recovery.

**WHEREAS**, to further its mission, AHC, in conjunction with other organizations, has developed a cloud-based exchange (e.g., the SISE [Sensitive Information Sharing Environment]) to facilitate the sharing and synchronizing of certain proprietary and/or sensitive information to be used for operational purposes during periods of emergency response and recovery, and such information shall be treated as "SENSITIVE INFORMATION" hereunder;

**WHEREAS**, the DATA PROVIDER, in connection with its operations, desires to provide information to the AHC and the SISE to be provided to pre-approved representatives from governmental agencies, businesses and other organizations (the "DATA USER(s)") to synchronize situational awareness and further facilitate collaboration, information sharing, decision making, and operational coordination between these governmental agencies, businesses and organizations in a no-fault, FOIA (Freedom of Information Act) free, private sector operated information sharing environment; and

**WHEREAS**, AHC and the DATA PROVIDER is willing to disclose SENSITIVE INFORMATION to the DATA USER(s) and provide the SISE DATA USER with access to specific SENSITIVE INFORMATION, for the purposes set forth above pursuant to the restrictions, protections, and other provisions hereof.

**WHEREAS**, AHC and the SISE will use technology that supports the sharing of data without USER(s) taking possession of the data and to protect data from FOIA (Freedom of Information Requests) and non-operational use by non-approved SISE DATA USER(s).

**NOW, THEREFORE**, in consideration of the mutual covenants and promises set forth herein, the parties hereto agree as follows:

1. SENSITIVE INFORMATION may include, but not be limited to::
  - a. datasets, geospatial data, video, tabular data, maps, spreadsheets, pictures, apps, website links, documents and/or information provided to the SISE from the DATA PROVIDER, or to which the DATA PROVIDER provides access, in oral, electronic, or written form, whether or not marked or identified as sensitive for competitive, legal, or other reasons.
  - b. all copies of all such documents and/or information,



- c. all other media or content that contains such SENSITIVE INFORMATION, or other documents based upon or derived from SENSITIVE INFORMATION, prepared by the DATA PROVIDER in connection with its operations during emergency response situations.
  - d. information relating to the SISE Use Cases approved by the SISE Working Group and Committees.
  - e. For purposes of clarity,
    - i. "SENSITIVE INFORMATION" does not have the same meaning as the government's data labeling for FOUO (for operational use only), classified, secret or top secret information.
    - ii. all information such as customer name, customer address, customer account number, customer id number, customer social services number, either alone or in combination, employee name, employee id number, employee address, social security number, driver's license number, taxpayer identification number, federal or state tax identification number, employer identification number, United States passport number, green card number/USCIS#, PII (Protected Critical Infrastructure Information, LES (Law Enforcement Sensitive), sensitive or reserved data for both internal and external communications will be categorized as too sensitive and **may not** be provided to the SISE based on DATA PROVIDER preference.
2. The AHC/SISE shall:
- a. hold SENSITIVE INFORMATION in strict confidence,
  - b. not disclose SENSITIVE INFORMATION to any other person(s), organization(s), agency(s), firm(s) or corporation(s) (including, but not limited to, parents, subsidiaries, or affiliates of the AHC/SISE) outside of the SISE unless previously approved by the DATA PROVIDER,
  - c. not use SENSITIVE INFORMATION other than in connection with its AHC/SISE operations during emergency response and/or recovery situations and in accordance with the Use Case(s) set forth by the SISE Working Group,
  - d. limit reproduction of SENSITIVE INFORMATION to the extent required for its operations during emergency response and/or recovery situations or the SISE Use Case planning processes,
  - e. when applicable, store SENSITIVE INFORMATION, based on DATA PROVIDER permissions, in a secure location that is not accessible to any person not authorized or vetted by the SISE to receive the SENSITIVE INFORMATION under the SISE provisions hereof, and
  - f. otherwise use at least the same degree of care to avoid publication or dissemination of SENSITIVE INFORMATION to its employees (or would employ) with respect to its own sensitive information which it does not (or would not) desire to have published or disseminated.
3. AHC/SISE and the DATA PROVIDERS, at any time, shall have the right to request adequate assurances that the foregoing restrictions and protections concerning SENSITIVE INFORMATION are being observed and the DATA USER(s) shall be obligated to promptly provide AHC and the DATA PROVIDER with the requested assurances.



4. Notwithstanding the provisions of paragraph 2 hereof, and based on specific Use Case restrictions, the SISE DATA USER(s) may need to disclose SENSITIVE INFORMATION to their directors, officers, employees, and in house contractors (collectively, "Agents") who have a legitimate "need to know" of such SENSITIVE INFORMATION in connection with the DATA USER(s) operations during emergency response situations, provided that each Agent first:
  - a. is advised by DATA USER(s) of the sensitive nature of such SENSITIVE INFORMATION; and
  - b. is caused by the DATA USER(s) to agree in writing to be bound by and observe the provisions of this SISE DATA USER AGREEMENT as though the Agent(s) were a SISE DATA USER;
  - c. Notwithstanding the foregoing, the DATA USER shall be responsible to AHC for any act or omission of the DATA USER Agents which, if committed by the DATA USER, would constitute a breach of this DATA USER AGREEMENT; and
  - d. data sharing or access to the information, unless otherwise defined, shall be limited screen sharing technology or access to the SISE's cloud based, information exchange platform and the specific information products.
  
5. The SISE will provide multiple tiers of DATA USER access security to protect SENSITIVE INFORMATION:
  - a. Tier 1 – data supporting use cases in this tier will be accessible by SISE DATA USER(s) who are vetted and approved via the SISE identity verification process that includes the creation of a SISE DATA USER profile, agreement with SISE DATA USER AGREEMENT terms & conditions. User profiles will contain user submitted information: name, organization, address, cell phone, valid email, and other survey information relevant to the users work and areas of interest.
  - b. Tier 2 – data supporting use cases in this level will be accessible by vetted SISE USER(s) from Tier 1 with the additional protections of a new agreement and use of a 2-factor authentication process for each login.
  - c. Tier 3 - data supporting use cases in this level will be accessible by vetted SISE Users from Tier 1 with the additional protections to be defined by the DATA PROVIDER.
  
6. Notwithstanding the provisions of paragraph 2 hereof, in the event that the DATA USER or its Agents, pursuant to applicable law or regulation or legal process, are requested or required to disclose any SENSITIVE INFORMATION, the DATA USER shall;
  - a. provide AHC with prompt written notice of such request or requirement in order to enable AHC and the applicable DATA PROVIDER(s) to consult with the DATA USER with regard to the steps that may be taken by AHC or the applicable DATA PROVIDERS to reduce the extent of SENSITIVE INFORMATION that must be disclosed and/or;
  - b. to enable AHC or the applicable DATA PROVIDERS to seek an appropriate protective order or other remedy reducing the extent of SENSITIVE INFORMATION that must be disclosed.
  - c. In any event, the DATA USER and its Agents shall disclose only such SENSITIVE INFORMATION which they are advised by legal counsel is legally required in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by AHC or the applicable DATA PROVIDERS) and,



- d. the DATA USER and its Agents shall use reasonable efforts to ensure that all SENSITIVE INFORMATION that is so disclosed will be accorded the appropriate treatment.
7. In some cases, the DATA PROVIDER may share digital information with the SISE DATA USER(s) via email or other digital or non-digital formats. Where applicable, within five (5) days after the earlier of (a) the end of the emergency response and/or recovery situation has ended (as defined by the AHC/SISE) for which the SENSITIVE INFORMATION was accessed, and (b) AHC's written demand, the DATA USER(s) shall:
  - a. destroy and delete, and cause its Agents to destroy and delete the SENSITIVE INFORMATION including all copies of all documents and of all other media that contain any SENSITIVE INFORMATION and all copies of any extracts, compilations, screen shots, studies or other documents prepared by the DATA USER or its Agents based on or derived from SENSITIVE INFORMATION; and,
  - b. certify to the AHC that the destruction and deletion by the DATA USER and its Agents required by clause (a) above has occurred by having a duly authorized officer of the DATA USER (or, if the DATA USER is not a corporation, agency, or other entity with officers, then the DATA USER shall have an authorized person of similar position and authority in the DATA USER's organization) complete, execute and deliver to AHC (at the address for AHC pursuant to paragraph 10 hereof) via a certification in the form attached hereto as **Exhibit A**. Compliance with this paragraph 5 shall not relieve the DATA USER from compliance with the other provisions of this DATA USER AGREEMENT.
6. Nothing in this DATA PROVIDER AGREEMENT shall be construed as granting or conferring any rights, by license or otherwise, expressly, implicitly, or otherwise, under any patents, copyrights, or trade secrets of AHC or any of the DATA PROVIDER to the DATA USER(s). Nothing in this DATA PROVIDER AGREEMENT shall be construed as requiring the disclosure of, or the granting of access to, any SENSITIVE INFORMATION to the DATA USER, and the DATA USER's access to SENSITIVE INFORMATION may be terminated at any time. No rights or obligations other than those expressly stated herein shall be implied from this DATA PROVIDER AGREEMENT.
7. The DATA USER understands and agrees that neither AHC/SISE nor any of the DATA PROVIDER(s) are making any representations or warranties, express or implied, as to the accuracy or completeness of the SENSITIVE INFORMATION, or any portion thereof, and that AHC and the DATA PROVIDER disclaim any and all liability from the use or reliance on the SENSITIVE INFORMATION.
8. The DATA USER and its Agents shall not be relieved of their obligations hereunder with respect to any SENSITIVE INFORMATION by reason of its availability to the public by publication or otherwise at any time and regardless of whether it was available to the public before or after it was disclosed pursuant to this DATA PROVIDER AGREEMENT.
9. The parties acknowledge that disclosure or misuse of SENSITIVE INFORMATION in violation of this DATA PROVIDER AGREEMENT may result in irreparable harm to AHC and the DATA PROVIDER, the amount of which may be difficult to ascertain, and which could not be adequately compensated by monetary damages, and that therefore AHC and the applicable DATA USERS are entitled to specific



performance and/or injunctive relief to enforce compliance with the provisions of this DATA PROVIDER/USER AGREEMENTS. The DATA PROVIDER agrees to waive any requirement for the securing or posting of any bond or other security in connection with AHC or any DATA USERS obtaining any such injunctive or other equitable relief.

10. All notices and other correspondence hereunder shall be in writing and shall be sent by certified mail (return receipt requested), by personal delivery, or by a nationally recognized overnight courier service, as follows:

If to the DATA PROVIDER:

- to the name and address for the DATA PROVIDER first written above

If to AHC:

- All Hazards Consortium, 47 E. South Street, Suite 201, Frederick, MD 20701
- Attn: Tom Moran, Executive Director

A parties may change the address or addressee for notices and other correspondence to it hereunder by notifying the other party by written notice given pursuant hereto.

11. The DATA PROVIDER irrevocably submits to the jurisdiction of the courts located within MARYLAND with regard to any dispute or controversy arising out of or relating to this DATA PROVIDER AGREEMENT. The DATA PROVIDER agrees that service of process on it in relation to such jurisdiction may be made by certified mail, return receipt requested, addressed to the AHC at the address for the AHC pursuant to paragraph 10 hereof and that such service shall be deemed sufficient even under circumstances where, apart from this paragraph 11, there would be no jurisdictional basis for such service. The AHC agrees that service of process on it may also be affected in any manner permitted by law.
12. This DATA PROVIDER AGREEMENT shall be interpreted, and the rights and obligations of the parties determined, in accordance with the laws of - MARYLAND without recourse to such state's choice of law rules.
13. This DATA PROVIDER AGREEMENT may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall together constitute one and the same instrument. Copies of this DATA PROVIDER AGREEMENT and copies of signatures on this DATA PROVIDER AGREEMENT, including any such copies delivered by facsimile or .pdf, shall be treated for all purposes as originals.
14. This DATA PROVIDER AGREEMENT may not be amended or modified except in a writing signed by both parties.
15. This DATA PROVIDER AGREEMENT shall be binding upon, and inure to the benefit of, the permitted successors and assigns of each party; provided, however, that this DATA PROVIDER AGREEMENT may not be assigned by a party without the prior written consent of the other party and any purported assignment without such consent shall be void.
16. This DATA PROVIDER AGREEMENT constitutes the entire agreement between the parties with respect to the subject matter hereof and any prior or contemporaneous oral or written



agreements or understandings with respect to such subject matter are merged herein.

- 17. This DATA PROVIDER AGREEMENT shall be construed as to its fair meaning and not strictly for or against either party.
- 18. No portion of this DATA PROVIDER AGREEMENT is binding upon a party until it is executed on behalf of that party in the space provided below and delivered to the other party. Prior to such execution and delivery, neither the submission, exchange, return, discussion, nor the negotiation of this document, whether or not this document is then designated as a “draft” document, shall have any binding effect on a party.
- 19. The DATA PROVIDERS are third party beneficiaries of this DATA PROVIDER AGREEMENT and may enforce those provisions of this DATA PROVIDER AGREEMENT in which the DATA PROVIDERS are specifically referenced.
- 20. The AHC does not endorse or guarantee any the 3rd party links to DATA PROVIDER websites, portals, apps, etc. The products and services offered on DATA PROVIDER sites are not products of the AHC and the AHC cannot attest to the accuracy of information provided by the linked sites. Linking to a DATA PROVIDER website does not constitute endorsement by AHC, or any of its stakeholders (e.g., officers, working group members, contactors, employees or public/private stakeholders, sponsors, etc.) of the sponsors of the site or the datasets, information or products presented on the site(s). Other websites which DATA USERS may link to from the AHC are not bound by AHC Security & Privacy Policies, of this DATA PROVIDER AGREEMENT.
- 21. As with all disasters, this information is subject to change without notice. The All Hazards Consortium, the SISE, the Multi-State Fleet Response Working Group, the companies involved, and the government organizations, expressly disclaim any liability whatsoever, for any usage of this information by its recipient. Recipient’s usage of this data constitutes a waiver of any claim it may have with respect to its use of the data. Please consider all information operationally confidential.

IN WITNESS WHEREOF, the parties have executed and delivered this DATA PROVIDER AGREEMENT as of the effective date first above written.

ALL HAZARDS CONSORTIUM

\_\_\_\_\_  
[NAME OF DATA PROVIDER]

By: \_\_\_\_\_

By: \_\_\_\_\_

Name (print): \_\_\_\_\_

Name (print): \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_



# EXHIBIT A

## Certification Of Data Destruction & Deletion Form

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

I, the undersigned certify that all SISE related data and information, as outlined in the SISE User agreement has been destroyed in accordance with the terms of the agreement (e.g., Section 7).

Name: \_\_\_\_\_

Organizational : \_\_\_\_\_

Address: \_\_\_\_\_

Address: \_\_\_\_\_

City, State, ZIP: \_\_\_\_\_

Signature: \_\_\_\_\_

Title: \_\_\_\_\_

Please email signed form to: [info@ahcusa.org](mailto:info@ahcusa.org)

Or Mail to: All Hazards Consortium ,47, East South Street, Suite 201, Frederick, MD 21701



## EXHIBIT B

### Data File Formats

SISE Members agree to provide/share data in one (1) or more of the following formats:

1. XML - (Extensible Markup Language) - is a set of rules for encoding documents in machine-readable form
2. KML – (formerly Keyhole Markup Language) - KML is an XML language focused on geographic visualization, including annotation of maps and images.
3. KMZ – A KMZ file consists of a main KML file and zero or more supporting files that are packaged using a Zip utility into one unit, called an archive. The KMZ file can then be stored and shared/accessed as a single entity
4. GeorSS – Geo RSS (Really Simple Syndication) is a family of web feed formats used to publish frequently updated content (in this case - Geographically referenced content). There are currently two encodings of GeorSS – GeorSS Simple and GeorSS Geography Markup Language (GML) which is an XML grammar for expressing geographical features.
5. WMS - Web Map Service Interface Standard (WMS) provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases
6. REST Services – Representational State Transfer (REST) Services Application Programming Interface (API) supports various formats, including KML, HTML, lyr (layer file), nmf (ArcGIS Explorer map file), jsapi (JavaScript), ve (Virtual Earth), and gmaps (Google Maps)
7. ATOM - The Atom Syndication Format is an XML language used for web feeds.

**Note:** If the primary file format of the dataset is KML or KMZ, members agree to provide/share data in at least one additional alternative file format listed above. In addition, members agree to develop a common protocol/approach for providing access to data using secure and non-secure http (<https://> and <http://>) as appropriate.





## EXHIBIT C

### Definitions

| Term                 | Definition  |
|----------------------|---|
| SISE                 | <p>The Sensitive Information Sharing Environment (SISE) is a private sector operated trust framework that supports operational information sharing between industry and government before, during and after storms, disasters and disruptions.</p> <p>The SISE provides the legal, policy, process, and technical framework for sensitive (but not secret or top secret) information to be organized and shared on a use case basis.</p> <p>The SISE is managed by the private sector and parts of it are shared with government for collaboration and decision making needs.</p> <p>The SISE is governed by the private sector and operated under the All Hazard Consortium.</p> |
| SISE-NET             | <p>SISE-net is a private sector driven initiative to enhance disaster response coordination by synchronizing multiple utility and state operations center data for specific use cases (e.g. damage assessments, road closures, supply chain disruptions, open/closed facilities, etc....)</p> <p>Video URL: <a href="https://www.youtube.com/watch?v=MfAU_o7HfO8">https://www.youtube.com/watch?v=MfAU_o7HfO8</a></p>   |
| SISE Data User       | Any approved person granted access to the SISE and has agreed to all disclaimers and the SISE User Agreement  |
| SISE Data Provider   | Any approved person or organization that shares information (electronic, print, etc..) with the SISE or the SISE community.   |
| Participating Member | Jurisdictions who have signed the MOA   |
| AHC                  | <p>The AHC is an established 501c3 organization formed in 2005.</p> <p>URL: <a href="http://www.ahcusa.org">www.ahcusa.org</a></p> <p>The AHC facilitates groups of practitioners dedicated to solving cross-sector operational problems and sharing information before during and after any type of disaster.</p> <p>As a Maryland 501c3, the AHC is EXEMPT of from FOIA (Freedom of Information Act) requests from unapproved, non-operational users (media, competitors, research, etc..).</p>   |