CIRT Terms of Service

TERMS OF SERVICE FOR

MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER® (MS-ISAC®)

CYBERSECURITY INCIDENT RESPONSE TEAM ("CIRT")

These terms of service ("Terms") set forth the terms by which the Multi-State Sharing and Analysis Center® (MS-ISAC®), a division of the Center for Internet Security® (CIS®),CIRT will provide Incident Response and Planning Services and Computer Forensics and Analysis Services (collectively the "CIRT Services") to State, Local, Tribal and Territorial ("SLTT") government entities (each an "SLTT" and collectively "SLTTs"), specifically in this case (name of requesting SLTT) _____, at no cost to the SLTT.

1. Definitions

A. Incident Response and Planning Services shall mean assistance in responding to a cybersecurity incident involving the system, network or equipment of a SLTT.
B. Computer Forensic and Analysis Services shall mean assistance to SLTTs with analysis of computers, servers, hard drives, and other computer or network equipment to assess for indicators of compromise, malicious activity, or anomalous behavior, and provide recommendations for remediation.

2. Terms Applicable to Incident Response and Planning Services

A. SLTTs may contact CIRT at any time to request assistance with incident response. CIRT staff will conduct an initial call or email with the SLTT to determine the scope of the incident.
B. Following initial scope, the level of involvement by CIRT will be based on the type and severity of the incident and the support needs of the SLTT. The incident response service provided by CIRT will generally be provided on a remote basis. In certain extreme circumstances, CIRT may provide on-site incident response services, but in no event will CIRT staff perform remediation on any affected SLTT system.
C. CIRT may require that the SLTT provide logs and other applicable files for analysis by CIRT. These files may be accessed by CIRT via the use of an agent installed by SLTT on the affected system by SLTT, which agent will provide CIRT access to select the necessary data and artifacts, and the agent will push the selected data to CIRT's secure file server.
D. As part of the Incident Response and Planning Services, CIRT will provide remediation recommendations to assist with the incident. These recommendations are based on the information provided by the SLTT, and may vary in effectiveness based on the level of information provided and the SLTT's infrastructure. Upon request, CIRT will provide a report documenting the incident response details and recommendations provided by CIRT.
E. Upon completion of Incident Response and Planning Services, any files uploaded to CIRT's secure file server will be deleted. CIRT shall maintain a copy of the files transferred to the CIRT secured file server for a period of up to one (1) year after completion of the Incident Response and Planning Services, unless otherwise requested by the SLTT.
    i. In the event an SLTT determines an incident response case handled by the CIRT may result in litigation or a criminal investigation, the SLTT is required to provide the MS-ISAC with a preservation request to ensure evidence is not destroyed.

3. Terms Applicable to Computer Forensics and Analysis Service

A. Computer Forensics and Analysis Services are generally prioritized by CIRT in the order that requests are received. The MS-ISAC reserves the right to triage and reprioritize cases in the certain circumstances, such as a major nationwide cyber incident. In these circumstances, the MS-ISAC will prioritize cases based upon CIRT protocol, weighing the risk to national security and sensitivity of the data for each competing case.

B. CIRT typically requests that a forensic image of the affected system or device be sent to CIRT for analysis versus the original drive. These must be sent by commercial shipping, using protected packaging to avoid damage during transit. In the event the SLTT does not have the ability to create a forensic image, CIRT will provide technical assistance or if no other option exists, request the original evidence be submitted for analysis. In some instances, CIRT may request only certain information from a system (such as event logs) and will provide technical direction to the SLTT on how to obtain that evidence and submit it for analysis.

    I. Please note, there is a separate procedure for the submission of items considered evidence and require that chain of custody to be maintained. Please see section 4 below.

C. The MS-ISAC agrees to maintain strict confidentiality of all data submitted for analysis, whether on physical media or electronically.

D. Upon completion of the analysis, CIRT will provide the SLTT with a report of the findings, including an executive summary, analysis details, indicators of compromise, and recommendations. These recommendations are based on the information provided by the SLTT, and may vary in effectiveness based on the level of information provided and the SLTT's infrastructure.

E. Upon closure of the case, the forensic image drive or other media will be returned to the SLTT. Data on the CIRT file server will be retained for up to one (1) year, unless otherwise requested by the SLTT.

    I. In the event an SLTT determines an incident response case handled by the CIRT may result in litigation or a criminal investigation, the SLTT is required to provide the MS-ISAC with a preservation request to ensure evidence is not destroyed.

4. Terms Applicable to All CIRT Services

A. MS-ISAC CIRT shall provide chain of custody documentation for handling of information and/or equipment provided to MS-ISAC by the SLTT in performing CIRT Services. The SLTT must inform CIRT in advance or at the time of receipt of such information of the need to follow chain of custody procedures and must provide any applicable chain of custody form already started by the SLTT.

B. Prior to sending electronic evidence, it is requested that a hash value (e.g., MD5 or SHA1) be generated to be compared against when the evidence is first examined by CIRT. This can be accomplished by placing all the evidence that will be submitted into a zip file and then generating a hash value of that file that can be sent to CIRT via email.

C. If chain of custody is necessary, it is recommended the evidence be mailed registered mail. If for some reason that option is unavailable, it is recommended to then use priority express or priority mail.

    i. Although most expensive, registered mail receives tracking and receives a hand-to-hand transfer with a log book and a seal along the way. Insurance is included based upon the estimated value of the item (up to $50k).

    ii. Priority Express (1-2 day) or Priority Mail (2-3 days) have tracking as well and offer free insurance ($100 for Express and $50 for Priority). Signature Confirmation services can be added on to obtain a signature receipt when the intended recipient receives the mail piece.

D. All evidence returned through mail by CIRT to the submitting agency will be returned using registered mail to maintain the chain of custody.
E. At first examination of any item of evidence, CIRT shall generate a hash value prior to conducting any forensic activities. An additional hash value will be generated at the end of an examination prior to returning evidence to the requesting agency.
F. In the event that the cybersecurity incident results in litigation or other formal proceedings, CIRT staff will be available to provide testimony limited to the provision of CIRT Services.

5. Confidentiality Obligations

A. In connection with performing the CIRT Services, MS-ISAC acknowledges that certain confidential or proprietary information of the SLTT, its employees and/or those constituencies the SLTT serves may be disclosed to MS-ISAC in the process of conducting the CIRT Services, without limitation: information regarding the infrastructure and security of the SLTT's information systems; confidential personal information regarding the SLTT's employees or constituents; information concerning ongoing law enforcement matters; personal health information concerning the SLTT's employees or constituents; information about the SLTT's financial or business operations; or other documents or data that the SLTT deems confidential or proprietary ("Confidential Information"). MS-ISAC agrees to hold the SLTT's Confidential Information in confidence to the same extent and the same manner as MS-ISAC protects its own confidential information, and in accordance with any information protection requirements imposed by statute or regulation relating to the particular Confidential Information (i.e. PII, HIPAA, CJIS, PCI-DSS etc.).
B. Except as otherwise set forth in these Terms, the SLTT's information will not be released in any identifiable form without the express written permission of such party or as required pursuant to lawfully authorized subpoena or similar compulsive directive or is required to be disclosed by law. The parties agree to use all reasonable steps to ensure that Confidential Information received under this Agreement is not disclosed in violation of this Section. These confidentiality obligations shall survive the termination of this Agreement.
C. Notwithstanding the foregoing, the SLTT acknowledges and agrees that MS-ISAC CIRT:
    I. shall share with the Federal Bureau of Investigation any evidence of child pornography discovered in the course of an incident response, in accordance with applicable federal law;
    II. shall, unless specifically prohibited by the submitting SLTT, provide incident related information, including updates on any previously reported incidents, to the US Department of Homeland Security ("DHS") in the daily status reports provided by MS-ISAC CIRT to DHS as required by the Cooperative Agreement between DHS and CIS (which Cooperative Agreement funds the MS-ISAC CIRT and the CIRT Services), and that such information will not be anonymized;
    III. may provide incident related information, including updates on any previously reported incidents, to other federal partners, provided that such partners have agreed to protect the confidentiality of such information shared with them to the same extent as required under these Terms; and
    IV. shall protect the security and privacy of the SLTT's data by restricting the dissemination of attribution and/or details about the incident at the written direction of the SLTT in accordance with TLP guidance.
    V. may otherwise share information identified during the CIRT Services, including without limitation, identified malware, signatures of compromise and other incident related information, with others, provided that the information is shared on an anonymized basis.

6. Limitation of Liability. The SLTT recognizes that the nature of the CIRT Services are only one component of its overall security program, that it is impossible to detect, disclose and/or resolve every vulnerability or security hazard, and that the SLTT is always responsible for monitoring and managing its security environment and mitigating the risks associated with any potential or actual security hazard. The MS-ISAC is not responsible for any loss of SLTT data resulting from the cybersecurity incident and the SLTT acknowledges that it is responsible for backup of its systems.

7. Governing Law. Unless otherwise specifically prohibited by the laws of the SLTT's jurisdiction, any disputes arising in connection with the CIRT Services or these Terms shall be governed and interpreted by the laws of the State of New York without regard to its conflict of law provisions. In the event that the laws of the SLTT's jurisdiction require that the laws of its jurisdiction apply to all contracts entered into by the SLTT, then the laws of that jurisdiction shall apply.

8. Entire Agreement. These Terms constitute the entire agreement between the MS-ISAC CIRT and the SLTT with respect to the CIRT Services, superseding any prior representations, discussions, negotiations or other agreement, whether written or oral, between the parties.

☐ I acknowledge that I understand and agree to the aforementioned terms and conditions as set forth by the MS-ISAC for the performance of CIRT services and have the authority to accept these terms and conditions on behalf of my organization.

☐ I **do not** authorize the MS-ISAC to share any information about this incident with external parties, except that which is required by law.

X _____

Authorized SLTT Representative