MIS SCIENCES CORPORATION

MIS Cloud Services

Acceptable Use Policy

This Acceptable Use Policy ("AUP") describes activities prohibited on the MIS Sciences Corporation ("MIS") customer and cloud network ("MIS Cloud Services") for the protection of MIS and its Representatives, Services, network, and other customers. This AUP applies to all MIS Cloud Services and offerings, including GovPoint Cloud Services ("GCS"), and to all customers and users of those services. Questions regarding this policy should be directed to abuse@mis-sciences.com.

This AUP may be augmented or superseded by a customer-specific AUP as required by any Statement of Work ("SOW") or Agreement, and with the approval of MIS. Capitalized terms used but not defined in this AUP have the meaning given to them in the applicable Master Services Agreement or other Agreement between MIS and the Customer (the "Agreement").

1. Abuse

Customer shall not use MIS Cloud Services or the network to engage in, foster, solicit, or promote illegal, abusive, or irresponsible behavior, including:

- conduct likely to breach any laws, codes, or regulations applicable to the parties (including conduct infringing or misappropriating intellectual property, trade secrets, or confidential or proprietary information; or which is fraudulent, unfair, deceptive, or defamatory);
- unauthorized access to, monitoring or use of, or interference with an internet account, computer, system, network, data, or traffic;
- intentionally, knowingly, or recklessly introducing any malicious code into the Services;
- conduct that violates the rules or conventions of any newsgroup, domain registrar, email service, bulletin board, chat group, or forum used in conjunction with MIS Cloud Services (including falsifying header information in an email or newsgroup posting);
- if hosted in the MIS FedRAMP environment, any conduct, behavior, or security violation that violates any FedRAMP rule or regulation, failing to cooperate with MIS during any FedRAMP assessment, or failing to remediate any finding in accordance with FedRAMP guidelines;
- deceitfully collecting, transmitting, or using information, or distributing software that covertly gathers or transmits information about a user;
- distributing advertisement-delivery software unless the user affirmatively consents to its download and installation based on clear and conspicuous notice of the nature of the software, and can easily remove the software using standard tools included on major operating systems;
- conduct likely to result in retaliation or adverse action against MIS or its Services, network, website, or Representatives (including conduct resulting in the listing of MIS IP space on an abuse database);
- conduct intended to withhold or cloak identity or contact information, registering to use the Services under a false name, or using an invalid or unauthorized credit card in connection with the Services;

- gambling activity that violates any applicable code of practice, required license, or technical standard;
- use of any MIS-provided shared system in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of system resources; and
- conduct that creates a risk to safety or health, national security, or law enforcement.

2. Offensive Behavior

Customer shall not be abusive or offensive to MIS Representatives. Customer shall not publish, transmit, or store on or via the Services any content, or links to content, that MIS reasonably believes relates in any manner to child sexual abuse material, bestiality, non-consensual sex acts, or live sex acts; or that is excessively violent, incites or threatens violence, contains harassing content or hate speech, violates a person's privacy, or is malicious or morally repugnant.

3. No High-Risk Use

Customer shall not use the MIS Cloud Services in any situation where failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage (including in connection with aircraft or other modes of human mass transportation, or nuclear or chemical facilities).

4. Mail Requirements

For bulk or commercial email sent by or on behalf of Customer using the MIS Cloud Services, or from any network that directly or indirectly refers recipients to a site hosted using the Services (including using third-party distribution lists), Customer shall:

- post a privacy policy for each associated domain;
- post an email address for complaints in a conspicuous place on any associated website, promptly respond to messages sent to that address, and maintain a means to track anonymous complaints;
- obtain affirmative consent to receive email from intended recipients using reasonable means to verify ownership of the email address, honor and notify recipients of consent revocation, and evidence consent within 72 hours of a recipient or MIS request; and
- include the recipient's email address in the email body or "TO" line.

5. Vulnerability Testing

Customer shall not attempt to test the vulnerability of an MIS Cloud Services system or network, or attempt to breach MIS Cloud Services security measures, by any means (Customer may conduct vulnerability testing of its Hosted System only with MIS's prior written consent). EXCEPTION: Customer may, with the approval and coordination of MIS and under the control of a FedRAMP-authorized 3PAO, conduct all necessary testing for the completion of a security or FedRAMP assessment.

6. Export Control

Customer shall ensure that the Services are not used in breach of the export laws, controls, regulations, or sanctions policies of the United States or Customer's applicable jurisdiction. Customer shall ensure that the Services are not used by any person or entity suspected of involvement or affiliation with those involved in activities or causes relating to human trafficking; illegal gambling; terrorism; narcotics trafficking; arms trafficking; or the proliferation, development, design, manufacture, production, stockpiling, or use of nuclear, chemical, or biological weapons, weapons of mass destruction, or missiles.

7. Cooperation with Investigations and Proceedings

Customer agrees that MIS may permit a relevant authority to inspect Customer's content or traffic if MIS is legally required to do so, provided that MIS gives Customer reasonable prior notice where permitted by applicable law and regulation. MIS may report to appropriate authorities any Customer conduct that MIS believes violates applicable law, without notice to Customer (including by providing any information about Customer, its users, or its traffic). MIS may cooperate in response to a formal request from a law enforcement or regulatory agency investigating conduct that MIS believes violates applicable law, or in a civil action that on its face meets the requirements for such a request.

8. Domain Names, IP Addresses, and DNS Records

Customer shall maintain valid information with Customer's domain name registrar for any domain hosted on the MIS network, and shall use only IP addresses assigned to Customer by MIS in connection with the Services. Customer agrees that MIS may modify, transfer, or delete any DNS record or zone on MIS-managed or MIS-operated DNS servers or services upon request from the registrant or administrative contact identified in the registrar's WHOIS system.

9. Changes to This AUP

MIS may amend this AUP by publishing a revised version at www.mis-sciences.com or, in the event of a material adverse AUP change, by providing Customer 30 days' written notice. The revised AUP shall become effective as to Customer on the first to occur of: (i) Customer's execution of a new or additional agreement for all or part of the Services incorporating the revised AUP; (ii) the first day of an Agreement renewal term beginning at least 30 days after publication of the revised AUP; or (iii) expiry of written notice of a material adverse AUP change. If compliance with the revised AUP would adversely affect Customer's use of the Services, Customer may terminate the affected Services (without payment of an early termination fee) by giving MIS written notice of Customer's objection no later than 30 days following the date that the revised AUP would otherwise have become effective as to Customer. Customer may continue using the Services for up to an additional 90 days, subject to the prior version of the AUP, and MIS may elect to waive the AUP change as to Customer, in which case the notice of termination shall be of no effect.

10. AUP Breach

If Customer breaches this AUP (including unintentionally, as a result of Customer's failure to use reasonable security precautions, or as a result of activity occurring without Customer's authorization), MIS may block any content or traffic, suspend the Services, or terminate the Services in accordance with the Agreement. No credit shall be available under any Service Level Agreement for interruptions of Services resulting from an AUP breach. Customer's use of

the Services to assist another person in an activity that would breach this AUP if performed by Customer is itself an AUP breach.

Notwithstanding any cure period in the Agreement, MIS may suspend or block the Services, content, or traffic immediately and without prior notice where MIS reasonably determines that the breach is material, poses a security risk, exposes MIS or others to liability, or involves unlawful conduct. MIS will provide Customer notice of such action as soon as reasonably practicable.

MIS shall have no liability to Customer for any blocking, removal, suspension, termination, reporting, or other enforcement action taken in good faith under this AUP.

MIS has no obligation to monitor Customer content or traffic but reserves the right to do so as necessary to operate and protect the Services, enforce this AUP, and comply with applicable law. MIS's failure to enforce any provision of this AUP in a given instance is not a waiver of its right to enforce that or any other provision.

11. General

Responsibility for users and sub-tenants. Customer is responsible for all activity occurring under its account and for the compliance of its users, employees, contractors, agents, and end users (including any sub-tenants or downstream customers of Customer) with this AUP. Customer shall bind those persons to obligations no less protective than this AUP. Any breach of this AUP by any person using Customer's account, credentials, or Services is deemed a breach by Customer.

Non-exhaustive list. The prohibited activities described in this AUP are illustrative and not exhaustive. MIS may reasonably determine that conduct not specifically listed nonetheless violates this AUP, and may act on that determination.

Costs of remediation. Customer is responsible for the reasonable costs MIS incurs in investigating and remediating Customer's violations of this AUP, including abuse response, removal of MIS IP space from blocklists or abuse databases, and mitigation of malicious or excessive traffic originating from Customer's account or Services.

Indemnification. Violations of this AUP that give rise to third-party claims are subject to the indemnification provisions of the Agreement.