

GOV CLAIM TECHNOLOGIES, LLC

NIMS Logic Acceptable Use Policy

NIMS Logic Incident Management Platform

Effective Date: September 23, 2026

1. Purpose and Scope

This Acceptable Use Policy (“AUP”) governs the use of the NIMS Logic incident management platform and all related services (the “Services”) provided by Gov Claim Technologies, LLC (“Vendor”) under the Master Subscription and Services Agreement (the “Agreement”) between Vendor and the subscribing agency (“Client”). Capitalized terms not defined in this AUP have the meanings given in the Agreement.

This AUP applies to all individuals who access or use the Services, regardless of organizational affiliation, including Client’s employees, contractors, volunteers, guest users, mutual-aid personnel, field operators, and any other persons whom Client authorizes or admits to the Services (collectively, “Users”). Client is responsible for ensuring that all Users are aware of and comply with this AUP.

2. Permitted Use

The Services are designed and licensed exclusively for emergency management, incident coordination, resource tracking, and related public-safety functions consistent with the National Incident Management System (NIMS) and the Incident Command System (ICS). Users shall use the Services solely for the following purposes:

- Incident documentation, planning, and coordination, including the creation, review, approval, and management of ICS forms, Incident Action Plans, operational periods, and related incident records.
- Resource management, including check-in, status tracking, assignment, cost tracking, demobilization, and personnel accountability.
- Organizational and supervisory chain management consistent with ICS principles, including unity of command and span of control.
- Training, exercises, and planned events that simulate or prepare for emergency operations.
- Administrative functions directly related to the management of Client’s emergency management program, including resource inventory, contact management, and organizational configuration.

3. Prohibited Conduct

Users shall not, and Client shall ensure that Users do not, engage in any of the following:

3.1 Unauthorized and Non-Emergency Use.

- Use the Services for any purpose unrelated to emergency management, incident coordination, or public-safety operations.
- Use the Services for personal, commercial, political, or promotional purposes.
- Use the Services to store, process, or transmit data that is not related to Client’s emergency management operations or authorized training activities.

3.2 Security and Access Violations.

- Attempt to access, view, copy, or modify data belonging to another agency or tenant, except as expressly permitted by a declared jurisdictional hierarchy established by Vendor in accordance with Section 4 of the Agreement.
- Share login credentials, access tokens, or authentication information with any other person, or use another person's credentials to access the Services.
- Attempt to circumvent, disable, or interfere with any security feature, access control, or authentication mechanism of the Services.
- Reverse engineer, decompile, disassemble, or attempt to derive the source code, algorithms, data models, or underlying architecture of the Services.
- Use automated tools, scripts, bots, scrapers, or similar technology to access, extract, or collect data from the Services, except through Vendor-provided APIs used in accordance with applicable documentation.
- Introduce or transmit any virus, worm, trojan, ransomware, or other malicious code into or through the Services.
- Probe, scan, or test the vulnerability of the Services or any associated network or system without Vendor's prior written authorization.

3.3 Data Integrity Violations.

- Knowingly enter false, misleading, or fabricated data into ICS forms, Incident Action Plans, resource records, personnel accountability records, cost tracking entries, or any other system records.
- Alter, delete, or tamper with approved Incident Action Plans, audit trails, or other records designated as immutable by the system.
- Misrepresent a User's identity, organizational affiliation, ICS qualifications, or role assignment within the Services.

3.4 Interference and Misuse.

- Take any action that disrupts, degrades, or interferes with the performance, availability, or functionality of the Services for any user or tenant.
- Use the Services in a manner that violates any applicable federal, state, or local law, regulation, or ordinance, including public-records laws, records-retention requirements, and data-protection statutes.
- Use the Services to transmit content that is defamatory, obscene, threatening, harassing, or that infringes the intellectual property rights of any third party.

4. Data Accuracy and Record Integrity

4.1 Client and all Users are responsible for the accuracy, completeness, and timeliness of all data entered into the Services, including ICS forms (ICS 201 through 221), Incident Action Plans, resource check-in and demobilization records, cost tracking entries, and personnel accountability records. The Services are designed to facilitate documentation; they do not independently verify the accuracy of User-entered data.

4.2 Approved Incident Action Plans constitute legal records within the NIMS Logic platform. Once an Incident Action Plan has been approved for an operational period, the system preserves it as an immutable snapshot. Users shall not attempt to circumvent this immutability through any means.

4.3 Users shall promptly report any data entry errors to their supervisor or to Client's designated system administrator so that corrections can be documented through the appropriate amendment or correction workflow within the Services.

5. Planning and Coordination Tool Acknowledgment

5.1 The Services are a planning, documentation, and coordination tool intended to support, not replace, the professional judgment of trained emergency management personnel. The Services do not provide operational directives, and no output of the Services (including resource recommendations, status displays, weather data, mapping information, or analytical summaries) constitutes professional emergency management advice.

5.2 Users acknowledge that weather information displayed within the Services is sourced from third-party providers and is presented for situational awareness only. Mapping and geospatial data are provided by third-party services and may contain inaccuracies. Communications delivered through the Services depend on third-party infrastructure. Client and Users shall not rely solely on any third-party data or service integrated into the platform for life-safety decisions.

5.3 Vendor bears no responsibility for operational decisions made by Client or Users based on information displayed in or generated by the Services, including decisions related to resource deployment, evacuation, personnel safety, or incident strategy.

6. Multi-Agency and Guest User Obligations

6.1 Client is the sponsoring agency for all Users who access the Services under Client's account. Client is responsible for the onboarding, access management, supervision, and acceptable-use compliance of all Users, including mutual-aid personnel, contractors, volunteers, and guest users whom Client authorizes or admits to an incident or to the Services generally.

6.2 External personnel assigned to a Client-managed incident receive data access commensurate with their assigned ICS role as determined by Client through the incident's organizational assignment. Such access is limited to the scope of the incident assignment and terminates upon demobilization, incident closure, or revocation by Client, whichever occurs first.

6.3 Users from assisting agencies shall access only the incident data and resource information to which they have been granted access by the managing agency. Assisting agency Users shall not attempt to access data belonging to the managing agency or any other agency outside the scope of their incident assignment.

6.4 Client shall ensure that all Users, regardless of home agency or employment status, have acknowledged and agreed to comply with this AUP before being granted access to the Services. Client may satisfy this requirement through its own onboarding procedures, provided that such procedures require affirmative acknowledgment of the obligations set forth herein.

7. Account Security

7.1 Each User shall maintain the confidentiality of their login credentials and shall not share, disclose, or permit any other person to use their account. Users are responsible for all activity conducted under their accounts.

7.2 Client shall promptly disable or remove access for any User who is no longer authorized, including personnel who have separated from Client's organization, been demobilized from an incident, or whose authorization has been revoked for any reason.

7.3 Client shall promptly notify Vendor of any known or suspected unauthorized access to the Services, any security incident involving Client's accounts, or any known violation of this AUP.

8. Enforcement and Remedies

8.1 Vendor may, in its reasonable discretion, take any of the following actions in response to a confirmed or reasonably suspected violation of this AUP:

- Issue a written warning to Client identifying the violation and requesting corrective action within a specified timeframe.
- Suspend access for the individual User or Users responsible for the violation, pending investigation and remediation.
- Suspend Client's access to the Services in whole or in part if the violation poses an imminent risk to the security, integrity, or availability of the Services or to other tenants' data.

8.2 Except where an imminent security risk requires immediate action, Vendor will provide Client with reasonable notice before suspending access and will work with Client in good faith to resolve the violation and restore access as promptly as practicable.

8.3 A material or repeated violation of this AUP constitutes a material breach of the Agreement. In the event of such breach, Vendor's remedies include those set forth in the Agreement's termination provisions, in addition to any other remedies available at law or in equity.

8.4 Nothing in this AUP limits Vendor's obligation to maintain the security and availability of the Services for all tenants in accordance with the Agreement and the Service Level Agreement.

9. Modifications

Vendor may update this AUP from time to time to address new security threats, regulatory requirements, or changes in platform functionality. Vendor will provide Client with at least thirty (30) days' written notice of material changes to this AUP. Continued use of the Services after the effective date of a material change constitutes acceptance of the updated AUP. If Client objects to a material change, Client may raise the matter under the dispute resolution provisions of the Agreement.

10. Contact

Questions regarding this AUP or reports of suspected violations should be directed to Vendor at the contact information specified in the Agreement or at:

Gov Claim Technologies, LLC
Attn: Platform Security & Compliance
Email: support@nimslogic.com