SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and

The Customer

for

The Emergency Mass Notification System

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and the Serviced Customer. The parties agree as follows:

I. Service Description

Everbridge is a cloud-based, third-party SaaS (Software as a Service) platform, that enables users to send targeted notifications to individuals or groups. The platform offers a range of features designed to improve communication and the State of Maryland has fielded this tool as an emergency notification system.

Everbridge provides participating state agencies with a reliable, real-time emergency communication platform to quickly notify stakeholders during critical events. The platform supports multiple communication channels, including phone, SMS, email, and mobile app alerts, ensuring messages reach recipients when it matters most.

A. Standard Service:

The notification service procured through DoIT is the Everbridge Mass Notification module. This service enables organizations to connect with and inform their entire community before, during, and after a critical event through targeted, two-way communications. The following components are included with the standard service:

1. Rapid multi-channel emergency notifications (SMS, email, voice, app push)
2. Automated workflows and escalation policies
3. Geotargeted alerts for specific locations or populations
4. Integration with existing state systems and databases

5. Reporting and analytics for audit and compliance

B. Service Exclusions:

Following elements are excluded from the standard service offering:

1. IT Alerting Module (add on feature) - IT System integrations, on-call scheduling, alert automations and resolution
2. Integration with third party platforms such as Alertus (add on feature)
3. Crisis Management Module (add on feature)
4. Automated Weather Alerting (add on feature)

C. Optional Services

There are no optional services that can be added to the service at this time.

II. Service Dependencies

DoIT Services:	• **Management Controls**
	  ○ Enforcing policies and procedures related to securing the platform
	
	• **Operational Controls**
	  ○ Completed Everbridge administrator roles and responsibilities acknowledgement form (customer responsibility)
	  ○ Reviewing onboarding and compliance checklists (customer responsibility)
	
	•
	
	• **Log Collection and Analysis:** Ingesting security logs from Everbridge is fundamental to maintaining a robust security posture. These logs can serve as the raw data for various security functions, including:
	  ○ Intrusion Detection and Prevention: Identifying and blocking malicious activity.
	  ○ Security Information and Event Management (SIEM): Correlating events, detecting threats, and generating reports.
	  ○ Incident Response: Facilitating investigation and remediation of security incidents.
	  ○ Compliance Reporting: Demonstrating adherence to regulatory requirements

Technical:	• Integration with Single Sign On (SSO) capabilities for the Everbridge Manager and Member portals • Enforcing two-factor authentication for both portals if SSO is unavailable or degraded**.**
Non-Technical:	• Client role definitions for escalation • The customer will provide 24 x 7 x 365 points of contact (3) for coordinating outages, emergency maintenance/restoration (with appropriate application access to provide technical assistance), and change management.

III. Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

A. DoIT Responsibilities for Customer

DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed services:

1. **Management Controls**
   - **a)** Enforcing policies and procedures related to securing the platform
2. **Operational Controls**
   - **a)** Everbridge administrator roles and responsibilities acknowledgement form
   - **b)** Reviewing onboarding and compliance checklists
3. **Technical Controls**
   - **a)** Integration with Single Sign On (SSO) capabilities for the Everbridge Manager and Member portals
   - **b)** Enforcing two-factor authentication for both portals if SSO is unavailable or degraded
4. **Log Collection and Analysis:** Ingesting security logs from Everbridge is fundamental to maintaining a robust security posture. These logs can serve as the raw data for various security functions, including:
   - a) Intrusion Detection and Prevention: Identifying and blocking malicious activity.
   - b) Security Information and Event Management (SIEM): Correlating events, detecting threats, and generating reports.
   - c) Incident Response: Facilitating investigation and remediation of security incidents.
   - d) Compliance Reporting: Demonstrating adherence to regulatory requirements

B. Customer Responsibilities

The Customer shall be responsible for the following activities:

1. **Security**

    a) Maintaining the security of the platform by following best practices, policies, standards, terms of usage[1], and legal[2] requirements for user access and data management. This may include activities like enforcing password complexity requirements, monitoring for suspicious activity, removing users no longer requiring access, and reporting security incidents.
    b) Managing Everbridge User Roles, Privacy Policies, or Access Controls
2. **User Data Management**
    a) Manage their organization's user data within the platform (adding, removing, or updating contacts)
    b) Upon a user's role termination or transition date facilitating deactivation within 24 hours of the user's roll-off date.
    c) Perform monthly audits of users and contact accounts must be conducted to facilitate accuracy and enforce account cleanup procedures.
3. **Messaging**
    a) Developing and transmitting messages through the platform and to the designated group.
4. **System Usage, Testing, and User Training**
    a) Establishing procedures for system usage to include backup and recovery of data
    b) Confirming personnel are trained on usage
    c) Conducting system tests periodically and reporting any issues to Everbridge
    d) Creating and maintaining system documentation (user guides, message templates, standard operating procedures)
    e) Identifying and developing "Use Cases" applicable to the agency.

IV. Service Level Agreements (SLA's)

A. Availability

DoIT subscribes to this third party service from Everbridge and the vendor shall use commercially reasonable best efforts to achieve Availability of 99.99% or

[1] https://www.everbridge.com/about/legal/everbridge-terms-of-use/
[2] https://www.everbridge.com/about/legal/

greater in each calendar quarter, with such quarters beginning as of 12:00 a.m. Pacific Standard Time on the first day of a given calendar quarter and ending at 11:59:59 p.m. Pacific Standard Time on the last day of a given calendar quarter.

“Availability” shall mean the ability to access the Services and send a notification to one or more delivery methods per recipient.

B. Maintenance
The Everbridge vendor may modify the service without degrading its functionality or security features.

While not a specific uptime percentage, Everbridge will use "best efforts" to notify clients of suspensions for maintenance or other issues through the client portal or email.

“Scheduled Maintenance” means maintenance scheduled in advance to implement updates and/or perform system maintenance. In general, the timing of Scheduled Maintenance will be posted at least two (2) business days prior to the Scheduled Maintenance window. If Scheduled Maintenance is expected to interrupt Availability, then a Scheduled Maintenance service advisory will be posted to the Customer Support Center website.

C. Outages:
It is recommended for all administrators to subscribe for any outage notifications at https://evbgcem.statuspage.io/. Everbridge pushes notifications to all registered users of any upcoming maintenance or outages through this portal.

D. Service Delivery
DoIT will deliver the requested services to the customer in a timely manner according to the following standards.

Category	Measure
Initial Ticket Response and Customer Contact	24 hours
Everbridge Customer Service	All issues beyond DoIT SSO control.

V. Support and Service Management

A. Support
DoIT will provide support via telephone and email according to the SLA’s outlined above.

1. The DoIT Service Desk is available twenty-four (24) hours a day, seven (7) days a week, to provide Tier 1 telephone support for non emergency
2. Tier 2 support will be provided during regular business hours (8 am - 5 pm) Monday thru Friday, excluding state holidays and state closings.
3. Tier 3 support will be provided as needed to address further escalations
4. DoIT will serve as the primary support provider of the service outlined herein except when third-party vendors are employed.

B. Incident Management

Non emergency Incidents reported to the DoIT Service Desk will be triaged and managed based on priority as follows*:

Priority (P)	Description	Response Time	Target Resolution
P1	An incident that results in a total cessation of service across the Customer, *unrelated to DoIT SSO or callback number*.	P1 - Everbridge System Issue: The Agency must contact Everbridge Customer Support immediately.	Everbridge's P1 Target Resolution (24 hours)
P2	An incident that results in a partial cessation or disruption of service, administrative access issues *related to SSO*, or loss of other essential business functions.	P2 - DoIT SSO Issue: 4 hours	2 business days
P3	Disruption of service for of non-essential functionality, service questions, and administrative requests such as account creation, deletion, and changes, *unrelated to DoIT scope*.	P3 - Everbridge Non-Critical Issue: The Agency must contact Everbridge Customer Support.	Everbridge's P3 Target Resolution (5 business days)

- **For Everbridge System/Service Outages (P1/P3):** Agencies are strongly encouraged to subscribe to outage notifications at https://evbgcem.statuspage.io/.
- **Escalation:** In case of persistent problems unrelated to DoIT's scope (SSO and callback number), the agency's authorized administrators must directly call the Everbridge Customer Support Center. For any issue impacting the agency's ability to use the service, the agency can reach out to the DoIT Tech PM and/or the Everbridge Technical PM.

  - ***Emergency Incidents reported to Everbridge***

Everbridge understands that our customers rely upon our platform for assured critical communications, especially for health, safety, and critical business processes. Everbridge takes incidents extremely seriously and works non-stop to resolve customer-impacting incidents. To provide a high level of service to our customers, Everbridge utilizes operational processes based upon the IT Infrastructure Library (ITIL) framework, a de facto industry standard for IT service management. Root Cause Analysis (RCA) is a component of the ITIL problem management process.

As outlined above, our first priority with any service degradation is to restore service and resume normal operation. Once service is restored the focus changes to analysis, determining the root cause, and preventing recurrence. Prevention may contain actions to improve detection through monitoring, building out additional or replacement infrastructure, or developing software enhancements. It may take several days of investigation and cross-team coordination to develop the appropriate course of action to best serve our customers. Engineering teams from many different disciplines become involved in the resolution and review of incidents that are impactful to the platform and to our customers.

Request Management

Requests to move, add, or change service shall be handled as follows:

1. New Service(s)
   Entities seeking to utilize the service or deploy optional services outlined herein must:
   a) Submit a request via email to doit.intake@maryland.gov explaining the business needs or challenges.
      - DoIT will evaluate the request to ensure that the service meets the entity's business needs.
2. Service Modifications
   To increase, decrease, or alter existing service, the Customer must:
   a) Submit a request via email to doit.intake@maryland.gov
      - Service modifications include increasing or decreasing quantity of Organisations, Add or remove Administrators.
      - DoIT will log the request and assign it to the appropriate team for fulfillment.

- Requests that involve increases to costs will result in billing changes to the agencies which will require a Statement of Work and fund certification to make the change.

C. Outages
It is recommended for all administrators to subscribe for any outage notifications at https://evbgcem.statuspage.io/. Everbridge pushes notifications to all registered users of any upcoming maintenance or outages through this portal.

D. Support and Service Management Exclusions:Support and Service Management Exclusions:
While DoIT strives to tailor support and maintenance activities to match the customer’s mission, there may be limitations that hinder our ability to satisfy changing business needs. As such, support and service management activities do not include:

1. Non-Service Provider Systems**:** Issues caused by the Customer’s or a third party's hardware, operating systems, networks (LAN/WAN), software, or data not directly provisioned or managed by DoIT or Everbridge. This includes customer-side connectivity or configuration errors (e.g., firewalls, VPNs).
2. Custom Code/Integrations: Support for code, scripts, or connectors developed or modified by the Customer or a third party that interacts with the Everbridge's platform. Only the core APIs and documented integration points are supported.
3. Data Issues and User Errors: Rectification of data corruption, loss, incorrect configuration, or quality issues resulting from user negligence, misuse, or failure to follow procedures.
4. Unauthorized Modifications: Issues arising from unauthorized attempts to modify, alter, or reverse-engineer the Service Provider’s platform or configuration outside of approved tools.
5. Outdated Versions: Support for issues encountered using a version of the Service after its official end-of-life.
6. Force Majeure Events**:** Suspension of support obligations due to events beyond the Service Provider's reasonable control (e.g., acts of God, war, disasters, utility failures).
7. Third-Party Product Support: DoIT nor Everbridge is not responsible for troubleshooting or supporting third-party software or hardware used with the Service.

VI. Costs for Service

DoIT provides this service via a shared service model, which allows the state to recognize reduced pricing based on economies of scale. Currently the cost for

Everbridge Pro service is covered by Department of Information Technology (DoIT) cyber security funding.

VII. Termination of Service

A. The customer must provide ninety (90) days advance written notice to terminate services. Due to the nature of the state financial system budgeting for IT services, terminations will only be effective at the end of the fiscal year following the conclusion of the ninety (90) day notice period.

VIII. Warranty, Limitations, and Exclusions

This section is not applicable.