

## EXHIBIT 1

### HOSTING SERVICE REQUIREMENTS

#### **General**

1. Security for the State's Data hosted by Contractor or its subcontractors, if any, is the responsibility of Contractor and will not require customization by ITS.
2. Contractor shall complete, as part of their bid submission, a Consensus Assessment Initiative Questionnaire (CAIQ) including on an annual basis thereafter. The form is available at Cloud Security Alliance (<https://cloudsecurityalliance.org/>).
3. All requirements are applicable to the Development, Testing and Live Production Environments.
4. The Live Production environment must be logically separate from the other environments.
5. The technical and professional activities required for establishing, managing, and maintaining the environment are the responsibilities of the Contractor.
6. Details of any change to the NY Alert application or service will be recorded and all changes will be implemented in a controlled manner. All changes to the NY Alert application will be submitted to the ITS NY Alert Support Team two weeks prior to implementation whenever possible. Emergency changes that must be made immediately to avoid or correct system degradation will be submitted as soon as possible but no later than 2 hours after implementation. The ITS NY Alert Support Team will submit these changes to the ITS Change Management team.
7. The Contractor must document its security policy, practices and procedures related to the hosting services provided to ITS and make such information available to ITS upon request. Contractor must have a documented security monitoring and incident reporting and handling procedure approved by ITS prior to the system going live as part of the Support and Maintenance Plan.
8. Remediation plans following a security incident shall be provided to and approved by ITS.
9. The Contractor must allow the State, including OSC, to audit any facility which maintains NYS data or is used in the performance of this Contract. The State, including OSC, may perform this audit with a third party at its discretion.

10. Vulnerability Scanning:
  - a) ITS will also have the option to perform monthly environment vulnerability scanning. Contractor must address all high and medium vulnerabilities found during scanning in a reasonable timeframe as agreed upon with ITS.
  - b) ITS will have the option to perform application scanning and web server scanning, as needed. Contractor must address all high and medium vulnerabilities found during scanning in a reasonable timeframe as agreed upon with ITS.
11. Security incidents affecting State Data must be reported to ITS within **two hours** of the Contractor's knowledge of such incident.
12. ITS will determine when live data will populate any hosted database. Once ITS declares that the system is "live," all Contractor or sub-Contractor staff that need access to the application, database, server or backup data/media must be pre-approved by ITS before access is granted. Audit logs must capture all access to the application, database, server or backup data/media (log information to include username, event type, event operation, event details, successful/unsuccessful authentication events, system start/stop, hardware attachment/detachment, system alerts and error messages and other security events, unsuccessful attempts to access/modify/delete data being logged or data in the event table) and available to ITS. All audit logs should be to write-once media only. ITS must have access to all audit logs.
13. Contractor agrees that it shall perform the hosting services in a manner consistent with the following requirements:
  - a) Host all State data and maintain and implement procedures to logically segregate and secure State data from Contractor's data and data belonging to Contractor's other customers, including other governmental entities.
  - b) Establish and maintain appropriate environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the hosting Services and any State data, and to prevent unauthorized access, alteration or interference by third parties of the same.
  - c) Utilize industry best practices and technology (including appropriate firewall protection, intrusion prevention tools, and intrusion detection tools) to protect, safeguard, and secure the System and State Data against unauthorized access, use, and disclosure. Contractor shall constantly monitor for any attempted unauthorized access to, or use or disclosure of, any of such materials and shall immediately take all necessary and appropriate action in the event any such attempt is discovered, promptly notifying ITS of any material or significant breach of security with respect to any such materials.

- d) When software vulnerabilities are revealed and addressed by a vendor patch, Contractor will obtain the patch from the applicable vendor and categorizes the urgency of application as either “critical” or “non-critical” in nature. The determination of the critical versus non-critical nature of patches is solely at the reasonable discretion of Contractor in consultation with ITS. Contractor will apply all critical security patches, hot fixes, or service packs as they are tested and determined safe for installation.

### **Hosted Maintenance and Support**

The Contractor will provide the following hosted equipment maintenance and support over the period of the Agreement that includes:

- a) Software - All upgrades, releases and fixes to the Software must be thoroughly tested at the Contractor's site before they are released to NYS or put in production. The Contractor will apply hot-fixes and service packs as needed to address anomalies and security concerns. Software support applies to the all internally developed and all third party software including operating system, backups, antivirus software, and any application software.
- b) Hardware - Apply Firmware and BIOS updates as needed to address anomalies and security concerns. Updates must be tested internally prior to install.
- c) Server - Standard hardware and software maintenance as listed above to ensure reliability and optimal performance. This maintenance must occur weekly, monthly and quarterly depending on tasks.
- d) Servers
- An Uninterruptible Power Supply must protect all servers.
  - Must have redundant network cards, network circuits, and power source for fail-over.
  - All servers must be located in a security locked room accessible only by authorized personnel
  - All outside connections must pass through an approved Firewall.
  - All servers must pass an ITS approved vulnerability scan, with remediation.
  - All servers have their OS upgraded upon release with ample time allowed for bug fixes.
- e) Firewall - Must be deployed using current industry best practice model. Logs are to be monitored and maintained for twelve months to ensure reliability and security.
- f) Anti-Virus – Contractor must provide a reliable industry-standard anti-virus system to all systems. Virus definition file maintenance and updates must be done daily to ensure complete virus protection. System must have weekly proactive scans during off peak periods.
- g) Internet Connectivity - Must be redundant connections with burstable bandwidth support. The connectivity must automatically adjust to handle increased load during an alert.
- h) Telephone Lines - Service must be maintained and operational tested at regular intervals.
- i) Encryption & Server Certificates - Must be registered and installed on all web servers. All web traffic must be encrypted.

**j) Domain Names** – Must be registered for both the primary and alternate sites. Domain Name Services for all public facing web servers and all internal systems must be maintained and redundant.

**l) Server Computers** – Increased hardware capacity may be needed to deal with system expansion and performance needs. The site infrastructure hosting the systems must have the capacity to add additional servers and meet power needs.

**m) Infrastructure Hardware** - Should be added as needed to deal with system expansion and performance needs. The site infrastructure hosting the systems must have the capacity to add additional equipment and meet power needs.

**o) Power Systems as Needed** - The site infrastructure hosting the systems must have the capacity to add additional power to meet growing needs.

**p) Power Redundancy**- The data center is required to be connected to the public utilities via redundant power grid connections for primary power requirements.

- After 15 seconds of consecutive downtime, a generator will be required to supply power to the entire data center.
- The Data Center should store enough fuel on-site for extended run-time of greater than 1 week.
- Note: Reasonable Advance notice must be given to ITS of any major upgrades or system changes that the Contractor will be performing. ITS reserves the right to defer these changes if desired.

**System Availability/Outages and Service Credits/Maintenance:**

- i.** The System shall be accessible by all users 24x7x365 and available 99.982% of the time per month except for:
  - a.** Planned Maintenance not to exceed two (2) hours per month for which ITS shall have at least ten (10) days advanced notice and will be planned for ITS non-core business hours as much as practicable;
  - b.** Unavailability caused by circumstances beyond Contractor's control including force majeure, but only to the extent the unavailability was not the result of Contractor's failure to take all reasonable and commercial care to mitigate or prevent the unavailability. Any disputes regarding unavailability of the System shall be managed using the dispute resolution procedure set out herein.
- ii.** Contractors must provide the State the root cause of the outage, analysis and proposed resolution plan.
- iii.** Contractor shall have the system to be scalable to maintain performance during peak user access intervals.
- iv.** In the event Contractor fails to meet and maintain the time requirements set forth herein including but not limited to monthly system availability of at least 99.982% with no single downtime of greater than 90 minutes duration and downtime not exceeding 0.5% of the time in a month, Contractor will be responsible for the following Service Credits:

**Service Credits:** ITS will be provided with all service credits from Contractor within thirty (30) days or within a reasonable time of the availability failure. Contractor will identify the relevant incident number in addition to the start times and end times of unavailability. Contractor will provide a credit on the next monthly invoice following any unavailability. Credit will be calculated as for that month as follows:

For every thirty minute period by which system unavailability exceeds the specified 90 minute maximum requirement that the system continues to be unavailable the Contractor shall pay on demand to ITS or by ITS may set off against any amount then due and owing from the State to Contractor the amount of \$5,000 for each thirty minutes or part of a thirty minute period that the system remains down. The amount due will be computed by thirty minute increments or part thereof with no proration until the system has been restored to operation.

Credits can accumulate due to multiple incidents in the same month or multiple months if no invoice is issued. If an entire monthly invoice needs to be credited than the next monthly invoice shall be used until all appropriate credits are provided to ITS. Credits can also be used by ITS towards billable service hours at ITS discretion. Amounts due hereunder shall be in addition to any other amount due ITS.

ITS, at its sole discretion, may elect to waive any service credits based upon precipitating events such as: catastrophic failure, multiple simultaneous failures and/or acknowledgement of Contractor's best effort to sustain/restore service.

No provision of this section precludes the State from pursuing any other remedies to which it may be entitled under the Contract.

**System Performance and Capacity Monitoring:**

Contractor services include 24x7x365 performance and capacity monitoring and managed escalation services to address System issues. The performance and capacity monitoring will include:

- a) Monitor, collect, and analyze Server utilization data for CPU, memory, and disk space;
- b) Compile configuration data and usage patterns;
- c) Monitor Server performance;
- d) Establish thresholds and exception reporting procedures;
- e) Perform tuning based on available performance data;
- f) Review Server capacity trends;
- g) With the State's assistance, establish a schedule for Contractor's performance of Server maintenance (for example, virus and malicious software detection, backup, disk space cleanup) and for implementing modifications and enhancements to the Web Hosting Environment so as to minimally impact availability of the Web Hosting Environment;

- h)** Fire detection and suppression system for early detection of fires and suppression in a manner that does not damage equipment;
- i)** Air conditioning monitored facilities to control for temperature and humidity;
- j)** Facility monitoring for electrical and mechanical failures, fire detection, and leak detection;
- k)** Support services including system and network monitoring of backbone routers, WAN interfaces, routers, switches, and servers;
- l)** Network problem detection, tracking, and resolution process;
- m)** In the event of System failures, email notifications will be provided to ITS. Contractor will respond to all system failures per ITS pre-approved procedures.

**System Reporting Requirements:**

The Contractor will provide the following reporting, monthly, quarterly and annually and ad hoc, as requested, or as otherwise agreed upon by the parties:

- i.** Service Availability Reports
- ii.** Outage Summary Report
  - a)** The start and end time of each outage;
  - b)** The duration of the outage;
  - d)** Reason for the outage, if not known then an a delivery date of a root cause analysis report will be given by the contractor;
  - e)** Description of the actions required to resolve the outage problem;
  - f)** Total time the Service was unavailable; and
- iv.** System performance and Capacity Reports
- v.** Capacity Summary Report

The Contractor shall provide the reports/documentation as a condition precedent to payment under the Contract. Failure to provide a report required within the due dates set forth in the paragraph, below, shall subject the Contractor to the penalties set forth herein. Upon notice, the Contractor shall have an opportunity to cure the default or be subject to Contract termination. The State's failure to demand or receive required documentations shall not be deemed a waiver of rights under this paragraph.

All reports shall be delivered electronically. The parties to the Contract shall agree to an electronic format (e.g., application and required data elements) for each of the reports set forth in this section. Each report shall be transmitted to ITS electronically via the internet utilizing encryption standards and protocols approved by the State and the system used shall generate an electronic ticket acknowledging transmission.

All reports required under this Section shall be due within ten (10) business days after the last day of the required reporting period. In the event they are not received by this time, ITS shall notify the Contractor who shall have five (5) business days from the date of written notification to produce the report. In the event the Contractor fails to produce and deliver the specified report within this time frame, and the report is material to the State's administration of the project, the Prime Contractor shall pay liquidated damages in the sum of \$5,000.00 per business day until the report is received in writing by the State to the designated contact. The

(i) failure of the State to collect said amounts as liquidated damages or to provide the foregoing notice, or (ii) the payment by the State of amounts otherwise due Contractor shall not be deemed a waiver by the State of the right to enforce the provisions of this paragraph. The State reserves the right upon written notice to Contractor, to modify the frequency and reporting deadlines set forth above.

Note: Each month shall stand on its own in terms of the application of penalties for service levels.