Swagit Services

Camera and Broadcast Operations. Granicus may need to operate the camera and broadcast system remotely. Such remote operation requires access via inbound TCP port 2001, outbound TCP ports 21, 80, 443, 1935, 5721, and outbound UDP ports 53, 123. The Client will need to supply Granicus with access to such TCP and UDP ports with respect to the Client's Internet connection. Granicus will not be responsible for remote camera operations should Client fail to give Granicus such access, or if Client's Internet connection is interrupted. Additionally, in the event the Granicus needs to operate such system manually, the Client will provide access to the equipment at the Site designated by the Client in the Scope of Work.

Hardware Warranty. Granicus warrants that: (i) any streaming server hardware provided by Granicus for Swagit services (as identified in the Scope of Work) when used under normal operating conditions will be fully replaced for a period of three (3) years; (ii) all proprietary software for any streaming server shall be maintained in accordance with the Service Level Agreement; and (iii) all hardware and software for the broadcasting equipment (as identified and described in the Scope of Work as "Avior Broadcast System"), will be repaired or replaced with respect to each components manufacturer's warranties.

Version February 2023

Granicus' Service Network. Granicus' content delivery network and service level represents that: (i) it maintains full N+1 redundancy on all service critical-infrastructure in order to protect against outages. Multiple mirror facilities provide diverse geographic redundancy. Within each facility servers have multiple power supplies, network interfaces and RAID protected storage. Granicus is connected to upstream bandwidth providers by multiple gigabit uplinks, transitioning to gigabit and ten-gigabit connections to multiple "tier 1" bandwidth providers, offering route diversity and redundancy. These bandwidth providers maintain 24/7 staffs familiar with mitigating Denial of Service attacks, should the need arise, which they have sufficient capacity to absorb-and-filter; (ii) Granicus utilizes external, 3rd party monitoring services to track server availability metrics. This service tracks availability from approximately 30 international points which helps isolate regional networking issues, in addition to any centralized failures; (iii) Content is stored on Granicus' networks and viewable to the public for a period of three years or as defined by the managed services. All content is stored and backed-up offline indefinitely during the service term. Content can also be stored locally on the Client's network for an indefinite period of time limited only by storage capacity, with the added benefit of cached delivery to local users. Client is consulted before they exceed any storage horizon and may extend the window for additional years; (iv) Content is stored in widely accessible formats and is available for export at any time. Exported data will include multimedia content and associated documents in their native format as well as any structured metadata in XML format. Access to exported content can be via FTP, but in such an event the Client is encouraged to provide a portable hard drive to ease the transition of storage and bandwidth intensive content; and (v) the Client may verify compliance with these policies at any time in consultation with Granicus engineers and officers.

Version February 2023