GlobalMeet Security Measures

"Content" is Personal Data and any other information provided to Supplier by Customer.

1. Service Organization Control Report. Each calendar year Supplier shall provide to Customer at no additional cost a copy of an unqualified Type 2 Service Organization Control 2 Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy in accordance with AT Section 101 and Trust Services Principles Criteria and Illustrations TPA Section 100 from independent auditors (or applicable similar independent security controls audit acceptable to Customer), of Supplier's controls and systems relating to the Supplier Service and attesting to the suitability of the design and operating effectiveness of controls throughout the period. Such reports shall continuously cover the periods including the term of this agreement and any extension, and including the period while Supplier retains Content.

2. Security Program. Supplier shall establish, implement, and maintain reasonable staffing, policies and this program of technical and organizational security measures appropriate to (1) prevent any access to Content in a manner not authorized, and (2) comply with and meet all applicable industry standards. Supplier shall ensure that its information security staff has reasonable and necessary experience in information and network security. Supplier shall designate a data protection officer (or a responsible person if a data protection officer is not required by law).

3. Security Assessment. Upon request at no additional cost, Supplier will complete Customer's security self-assessment and will make appropriate Supplier personnel available to discuss the results. Supplier agrees to remedy material items per Customer's reasonable request.

4. Network-Level Requirements
   a. Supplier must use firewall(s) to protect hosts and networks handling Content including implementing a "Demilitarized Zone" or "DMZ" network or sub-network that sits between a trusted internal network and an untrusted external network to prevent direct access from outside to internal hosts and Content. Inbound packets from the untrusted external network must terminate within the DMZ and must not be allowed to flow directly through to the trusted internal network. All inbound packets which flow to the trusted internal network must only originate within the DMZ.
   b. Supplier shall maintain intrusion detection and/or prevention and shall implement continuous monitoring and response processes to prevent Content from unauthorized disclosure, misuse, alteration, or destruction.
   c. When using wireless networking technologies to perform Services, Supplier shall ensure that all of Customer's Content transmitted is protected by the use of appropriate encryption technologies sufficient to protect the confidentiality of the Content and shall regularly scan, identify, and disable unauthorized wireless access points.
   d. Firewall rules shall be documented, along with the business reason for each, and the business need and the firewall configuration must be audited quarterly, with any unnecessary rules removed, and other issues corrected, with good record keeping.
   e. Supplier shall implement continuous security monitoring and response processes for the firewalls, intrusion detection and/or prevention systems, wireless networking, endpoint protection systems, and network segment(s) on which hosts handling Content are logically located in order to prevent Content from unauthorized disclosure, misuse, alteration, or destruction.

5. Host/System/Device Requirements

a. Supplier must use Supplier-provided equipment and/or systems to handle and protect Content. Unless expressly authorized by Customer in writing, Content may not be processed or stored on personal equipment, personal e-mail accounts or other personal software.

b. Supplier must implement system hardening for hosts and devices handling and protecting Content. Hardening standards shall be written, be consistent with industry-accepted system hardening standards such as CIS, ISO, SANS or NIST, and shall be made available to Customer upon request.

c. Supplier must implement a host/device patch and update management program.

a. Supplier shall execute a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities based on industry best practices and potential impact.

b. Workarounds, patches and updates must be installed on all Data-Importer-controlled systems and devices within 30 days of their availability for critical vulnerabilities and immediately, but in no case longer than within 7 days, for emergency-level vulnerabilities.

d. Supplier hosts must be running endpoint protection software on all hosts and systems with on-access antivirus protection enabled, weekly antivirus scans running, and virus definition updated at least once per day. Supplier shall implement response processes to promptly remedy issues reported from the antivirus software.

6. Personnel and Training.

a. Supplier will conduct pre-employment background checks on any of its employees or subcontractors prior to assigning them to positions in which they will have access to Content. To the extent permitted by local laws and regulations, the background checks shall include employment verification, Education verification, criminal convictions, and reference checks.

b. Supplier personnel must provide written commitment to maintain the confidentiality of Content.

c. Supplier personnel who will access Content on Supplier's systems must complete successfully security and data privacy training provided by Supplier prior to such access and annual refresher training provided by Supplier. All training required under this paragraph will be at no additional cost to Customer.

d. Whenever a user leaves its desk unattended during the day and prior to leaving the office at the end of the day, he/she must ensure that documents containing Content are placed in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space.

7. Supplier Vulnerability Assessment. Supplier will conduct a vulnerability assessment against the Supplier Service and Supplier production application and servers on a quarterly basis as well as against any other instances such as test, development, or staging that have access to Content. Vulnerability assessments must include information on current update and patch status for operating system and application level patching. Vulnerability assessments must also check for vulnerabilities (both coding and patching levels) for applications and include, at a minimum, checks against the OWASP Top 10 application vulnerabilities per http://owasp.org/. Within 45 days of completion of the vulnerability assessment, Supplier will provide to Customer a detailed remediation and or mitigation plan and schedule for all vulnerabilities ranked high severity and above.

8. Data Protection. Supplier will protect electronic data used in connection with the Supplier Service.

a. Content at rest in the Supplier Service, production environment, on all backup media, or other storage system/media will be encrypted with a solution that uses 256 bit Advanced Encryption Standard or better, industry standard algorithms.

b. Supplier shall create back-up copies of Content which shall be stored in specially protected environments. Supplier shall perform regular restore tests from those backups.

c. Data at rest in that is not in the Supplier Service or non-production environments shall either be encrypted as specified above or individually identifiable data elements must be replaced with fictitious data.

d. Data in transit shall be protected using TLS 1.3 encryption or stronger.

e. Supplier shall take appropriate measures to (a) properly dispose of Content whether such information is in paper, electronic or other form in a way that the information cannot practicably be read or reconstructed; (b) ensuring the destruction or erasure of electronic media containing Content in a way that the information cannot practicably be read or reconstructed; and/or (c) ensuring that any third party who performs the activities described in the DPA does not retain Content for longer than it needs such information to perform its obligations under the DPA or as per written instructions from Customer or when the agreement is terminated or at the expiry of retention period. In any event, the retention period shall be discussed and received as written instruction from Customer or as standard practice data shall not be retained more than one year from the date of termination of the DPA.

9. Access Controls. Access to Content must be limited to only those Supplier personnel who have been authorized by Supplier and have a clear operational need for such access. Supplier will maintain access controls for all environments holding data used in connection with the Supplier Service, including without limitation:

a. Ensure that all of hosts and devices that process Content and are intended for use by multiple users are located in secure physical facilities with access limited and restricted to authorized individuals only. Video monitoring shall be in place for all facilities where Content is processed. All personnel with access to the systems that process Content shall comply with paragraph 6 above or shall be accompanied by Supplier personnel.

b. All access to the Content and to the physical facilities where Content is processed or stored will be logged and the logs shall be retained for at least 180 days. Supplier shall be able to attribute each access transaction to the individual user;

c. Immediately disable access permissions of terminated personnel;

d. Review appropriateness of system access rights and revoke such rights (e.g., due to personnel termination or role change) on at least a quarterly basis;

e. Use of two-factor authentication (e.g., (1) access-controlled facilities in conjunction with User ID and password, or (2) User ID and one-time use password);

f. Enforcement of strong passwords that are 8 or more characters in length, have a maximum age of 90 days, a minimum age of 2 days, and include at least three of the following four classes of characters: (1) upper case letters, (2) lower case letters, (3) numbers, and (4) special characters (e.g. "!#$%^&*,.?@"). Passwords may not contain the user id; and

g. Hosts shall lock after no more than 15 minutes of idle time, requiring the user to re-authenticate to use the system.

10. Separation. Supplier shall process the data and Content received from different clients to ensure that in each step of the processing the respective client can be identified, so data is always physically or logically separated.

11. Security Breaches. Supplier agrees that it shall:
    a. notify Customer immediately in the event of an inadvertent disclosure of Content, including but not limited to accidental or malicious breaches or other incursions into Supplier's infrastructure or loss of data. Such notice shall include sufficient detail that Customer is able to notify affected parties and to take steps to prevent or minimize harm from such disclosures;
    b. allow Customer to take steps to prevent or minimize hardships from such disclosures;
    c. cooperate with Customer fully in investigating such incidents and mitigating the consequences; and
    d. In the event of an incident, Supplier shall make available key personnel with sufficient knowledge to resolve any data privacy or security issues involving Content, and in particular, work with Customer to determine the scope of the incident, investigate the incident, and prepare a written summary of the incident and corrective action taken; however, such efforts shall not alter or change responsibility between Supplier and Customer for providing such notifications under applicable laws.
12. Business Continuity/Disaster Recovery Requirements.
    a. Maintenance of Plan. Supplier shall maintain and comply with a reasonable disaster recovery, crisis management and/or business continuity plan (the "Plan") acceptable to Customer which is capable of ensuring Supplier shall be able to continue to provide the Supplier Service in accordance with this DPA in the event of a disaster or other significant event (including a force majeure event) that might otherwise impact Supplier's operations.
    b. Testing the Plan. Supplier shall test the Plan with respect to the Supplier Service no less than once each year. Supplier will provide Customer with a summary of the results of such test. Supplier will notify Customer of any material failures in its disaster recovery or business continuity capabilities that Supplier believes would be reasonably likely to impact Supplier's performance of the Services.