



The Oliver Group

General Security and Controls

Corporate Headquarters

595 Greenhaven Road
Pawcatuck, CT 06379 US

European Office

London, United Kingdom

P: 860.599.9760

F: 860.599.9768

info@the-olivergroup.com

www.the-olivergroup.com

This document has been prepared to provide a summary of the security and controls in place at The Oliver Group (“TOG”). The following outlines various procedures TOG has in place to securely manage client data and mitigate risk of exposure and spoliation.

Chain-of-Custody

TOG maintains strict chain-of-custody procedures, designed to ensure the security and integrity of clients’ data. Upon receipt of media, TOG conducts a catalog of the shipment’s contents. This includes a physical inspection of the media, checks to ensure media is write-protected, creation of the chain-of-custody documents, and the recording of any documentation or details included with the shipment.

The chain-of-custody documents serve as comprehensive media inventory reports and are maintained by TOG throughout the project’s lifecycle. Clients are provided with copies of the chain-of-custody documents for their records.

Data Acquisition

Chain of Custody begins at project at the first moment TOG staff handles client data or physical media. To accurately document acquisition activities, TOG utilizes a series of collection logs and reports designed to maintain all relevant details associated with data collected.

These logs capture:

- Which drives, folders and files have been accessed
- The date, time, and location of the collection
- Full path names
- Where data has been transferred
- Data volumes
- Notes about the collection

- Serial numbers, versions, and other relevant information for all computers, hard drives, etc.

TOG ensures that all data collected is tracked precisely throughout the project’s lifecycle and that a documented source history is generated to provide an accurate means of correlating collected data to its source. TOG’s data collection policies are designed to adhere to the strict chain of custody procedures which investigations of this nature demand.

Additionally, TOG has testified generally about its acquisition and collection methods and protocols, including Chain of Custody. Procedures have not changed since testifying.

Media Intake and Access Control

Upon receipt of media at either our CT or London offices, the TOG Client Services team conducts a review of each piece of media that is received. This includes a physical inspection of the media and the recording of any documentation included with the shipment. The Chain of Custody documents serve as comprehensive inventory reports and are maintained throughout the project. Client will be provided with copies of the Chain of Custody document. An assigned Client Service Representative utilizes internal quality control procedures and documentation which ensures that each project is mapped to the SOW for quality assurance. TOG uses a unique ID for each tape (or other media) and it is logged at intake. Once the project is in production, the log of media is mapped to the log generated by the Production Staff to ensure that each item is processed. Upon completion of the intake process, media is housed within our secure media vault. Media that is received for each client is segregated within containers inside the media vault. When necessary, media is checked out of the vault and transferred to the production area which is accessible only to select staff.

Prior to the work being placed into production, TOG will validate with the client on a kick off call the SOW and items received to ensure the alignment of the project. This is then documented both internally and externally back to the client.

Project Closure

At the conclusion of a project, a Project Closure Document summarizing work performed, deliverables and pricing is delivered to the client for signature. The original media is then prepared to be sent back. The TOG ID and all label information captured during the Chain In process are noted on the Chain Out. The original media is shipped by carrier to the contact/address as designated by the client.

Locations where client and deliverable data is held: Upon receipt of project closure all volumes holding client and deliverable data are destroyed and rebuilt clean using a Two Person Integrity system where the destruction is executed and witnessed by two different personnel.

Physical Security

All doors are locked at all time and access to the premises is controlled via card key, with segregated systems for access to administrative and production areas of the facility. All visitors enter through a secure entrance and must be provided access to the premises by TOG personnel. All visitors are required to sign in and out, and are escorted at all times by TOG personnel while on the premises.

Physical security includes intrusion detection, camera/video surveillance, and fire detection systems which are monitored on a 24/7 basis. Additional security, in the form of on-site unarmed security personnel, can also be

provided depending on the requirements of a specific engagement.

Moreover, TOG often operates 3 shifts, providing additional supervision by TOG personnel of all media and processes.

Data Encryption

TOG makes every effort to protect client data at all phases. TOG provides data encryption services for all data, whether it is acquired at a client location, restored from backup media, in transit, or transported via FTP. While TOG does not mandate encryption for all media, it is highly recommended to all clients. Clients must provide sign-off for any data that they do not wish to be encrypted for delivery.

TOG can encrypt data for all types of media, including hard drives, removable devices, backup tapes, etc. TOG utilizes a number of different encryption tools and methodologies depending on the type of data, media and client requirements. TOG works with each client individually to meet any specific encryption requirements their IT or compliance department may have. NOTE: Data that is received by TOG in an unencrypted format will not be encrypted unless instructed to do so by the client.

Media Storage and Protection

TOG provides highly secure, fire resistive storage in its onsite media vault. Only a limited amount of media is removed from the vault for processing at any given time, substantially mitigating the risk of fire, loss or misuse of the media.

Access to the vault is tightly controlled with only specific personnel having access codes. Furthermore, TOG tracks all media that is stored or removed from the vault so that the location of each piece of media can be determined at any time.

Transportation

Transportation to and from TOG can be via common carrier (e.g. FedEx, UPS), bonded courier, or TOG personnel depending on client requirements. All media received at, or shipped from, TOG is managed through formal intake/ outtake procedures and is fully documented for chain-of-custody.

Data Backup and Disaster Recovery

Backups are created nightly of all deliverable data that is in process for each project. Given the transitory nature of this data, these backups are maintained only until data has been delivered and receipt acknowledged. For long-term projects or online hosted environments, full backups are maintained during the life of the engagement.

TOG has established relationships with its business partners to provide data replication and recovery services as required by its clients on a project-specific basis. This is recommended for larger projects where large volumes of data may be maintained or stored for an extended period of time. For smaller projects, the rapid turnaround time for data delivery typically does not require this level of redundancy.

Network Security and Access

TOG's data center is secured from other areas of the building, with access limited to specific personnel via card keys. TOG maintains

separate business and production networks, providing data segregation. Client/project-specific production environments are also created to provide an additional level of segregation and security. Limited external access is provided to the production network operations, and is available to only specific personnel via encrypted VPN access.

TOG also has strict network security, firewall, intrusion detection and anti-virus protocols in place to further restrict access. TOG has passed several 3rd party audits of its network access and security protocols, and is in the process of obtaining its SAS70 certification.

Internal Documentation

TOG has a comprehensive information technology policy manual which documents procedures and controls in the following areas:

- Physical Security
- Network Security
- Encryption
- Storage
- Transport

Personnel Management

The Oliver Group performs background checks and drug screening of all personnel during the hiring process. All personnel, contractors and vendors are required to sign Confidentiality and Non-Disclosure agreements.