



DOCUMENT SCANNING SYSTEMS & IMAGING

Peace of Mind and Tranquility
Dissemination Document
for DSSI Clients



UPDATED: June 2010

Disasters come in all shapes and sizes as well as from multiple sources. It is the very nature and impact of these disasters that causes companies to seek better ways to store, manage and protect their data. A recent survey among 1,259 IT professionals stated the following reasons for implementing a Disaster Recovery program:

- ❖ Hardware/Software failures 38%
- ❖ Viruses, hackers and other external threats 26%
- ❖ Natural Disasters 15%
- ❖ Accidental or malicious employee behavior 13%
- ❖ Terrorism or other man-made disasters 10%

It is because of these types of threats that DSSI has taken great strides to address potential threats and implement the proper policies, procedures and equipment. Our number one goal is to provide peace of mind to our clients that their documents are in good hands. In our 15 year history, we have provided this peace of mind to thousands of clients and successfully converted millions of documents without incident. Our clients have trusted us with some of the most vital records and confidential documents including medical records, EKGs, bank records, loan documents, credit files, critical infrastructure drawings, litigation files, personnel files, I-9 Forms, land surveys, as-builts, minutes, ordinances, resolutions, police reports, criminal records, engineering documents, patent pending files, payables, receivables, contracts and hundreds of other document types.

Below is a summary of the disaster prevention and recovery procedures that we have implemented to continue our long history of successful document handling, conversion and delivery.



Building Security

- ❖ Intrusion alarms have been positioned at every conventional and unconventional point of entry in the DSSI facility. Intrusion alarms project a loud siren and flashing lights, which calls attention to the intrusion from peripheral passersby usually resulting in the departure of the perpetrators.
- ❖ A simultaneous alert is sent to our remote, contracted security agency, which deploys an armed response to the DSSI facility in order to secure the facility.
- ❖ A contracted security agency conducts 24-hour, Random Security Patrol to the DSSI Facility
- ❖ Within the DSSI facility, motion sensors are in place at all points of entry and strategically placed internally to trigger the intrusion alarm should anyone attempt unauthorized access at any conventional or unconventional point of entry.
- ❖ Early Detection smoke alarms are in place to provide awareness that a fire may be developing. The detection system provides warning signs that trigger a series of events culminating in the performance of fire extinguishing by fire elimination specialists.
- ❖ The alarm system operates on power and a dedicated phone line to the contracted agency with a back-up power supply in place. In addition, radio transmission is in place as a back-up and acts as a failover in the event that phone line transmission becomes unavailable.

Network Security

- ❖ DSSI maintains two, distinct networks. One for Administrative and Sales purposes with outside (Internet) access and one for Production and Conversion of documents which is a closed network, isolated from the outside world.
- ❖ The DSSI Production network is a closed network and does NOT have access to the Internet, Email or other networks.
- ❖ All aspects of document conversion (outlined in the “DSSI Production Process” document) are managed within the Production Network.
- ❖ The Production Network has workstations dedicated to specific processes with workflow managed at the Server Station.

- ❖ Each workstation has an encrypted password that is changed each week and each workstation operator has a unique log-on and an assigned task for the assigned project.
- ❖ Though production PCs operate on a closed network, each workstation has installed spyware and virus protection software to monitor for intrusions that might occur through unconventional means.
- ❖ DSSI Network Security is managed by three individuals to verify that proper procedures are being followed. Our IT Director, Our System and Support Manager and Our Production Manager all oversee, test and verify the processes in place.
- ❖ DSSI knowledge workers are each assigned access rights according to their individual level of responsibility. These access rights ranges from ability to scan, perform data entry, perform quality control, view batch manager and a myriad of other duties.
- ❖ All work performed in the either DSSI Network is routinely backed up in the event that a circumstances arise that could cause data to be lost or unrecoverable. All backed up data is replicated to an off-site disaster recovery site with a SAS-70 Certification.
- ❖ Only authorized personnel can back-up data or initiate a data recovery event.
- ❖ All backed up data is overwritten with the most recent data

Personnel

- ❖ A comprehensive background checks is performed on every employee prior to being hired. All background checks are performed by A-Check, a division of the ACT-1 Group who is also the parent company of DSSI.
- ❖ All DSSI personnel possess a high level of document imaging experience. DSSI production managers, project managers and team leaders average more than 8 years with DSSI. This extensive experience allows DSSI to offer a strong level of confidence to our clients that their documents will be handled with competence and processed in the most efficient, secure methods available.
- ❖ All new DSSI employees undergo a probation period in which they are trained in all security procedures relevant to their job duties.



Document Security

- ❖ Every document container that arrives at our facility is bar-coded and scanned into the DSSI Tracker. At this time a Project Manager is assigned as the project lead and begins the allocation of resources to complete the job. The DSSI Tracker tracks documents through the production process, creates an audit trail and a report of all activity and human encounters during the imaging process.

The screenshot displays the DSSI Tracker application window. The interface is divided into several sections:

- Client Detail:** Shows information for 'APPLE ONE', including its name and organizational unit.
- Client Projects:** A table listing various projects with columns for ID, Name, Number, Client, Status, Lead, and Date. The table includes entries for 'APPLE ONE' and 'APPLE ONE FAC'.
- Tracking:** A detailed table of tracking information with columns for ID, Name, Number, Client, Project, Date, Priority, Description, and Followup Description. This table lists numerous projects, many starting with 'CREATE 1 NEW DOC CONTAINER(S) INDEX = 1' or '2'.
- Client List:** A scrollable list of clients on the left side of the window, with 'APPLE ONE' selected.

At the bottom of the window, there is a status bar indicating the current user (THOMAS J. TALAMANTEZ), department (SALES), and organizational unit (IMAGING). The date and time are shown as 6/23/2010 11:54 AM.

- ❖ Through security controls built into our Capture software, we are able to control access to scanned documents, limiting exposure and ensuring that production staff only has access to data necessary to complete the assigned task.
- ❖ Workstations in the production network are configured to prevent unauthorized downloads or copying of documents. In addition, workstations do not have access to network printers.
- ❖ Workstations are locked down to prevent access to external devices by blocking USB ports and fire wire ports

Transportation Security

- ❖ DSSI Account Manager will assign a Project Manager to the CLIENT to maintain Quality Control over the course of this SERVICE LEVEL AGREEMENT providing CLIENT with primary and secondary accountability contacts.
- ❖ DSSI will establish a schedule of pick-up and delivery of files between CLIENT and the DSSI facility. Transportation will include the delivery of electronic document media and the pick-up of boxed, hard copy files to be transported to DSSI for conversion.
- ❖ DSSI will provide protective seals or tamper proof tape to be placed on file boxes prior to transport to maintain the integrity and confidentiality of boxed files during transit.
- ❖ DSSI will verify file count for each box prior to placing protective seals or tamper proof tape on file boxes.
- ❖ CLIENT will provide a file log for each file box, listing each file in each box. File log will be verified by DSSI driver and signed by CLIENT authorized representative and DSSI representative. Each party will retain a copy of the file log.
- ❖ All documents will be transported in “Dual Control” which will be comprised of a driver and a document handler and/or the Project Manager.
- ❖ DSSI offers clients the option of having armed security accompany the documents during transport to production facility. DSSI Sales Rep can provide pricing for this additional service.
- ❖ The Project Manager will inspect boxes upon arrival at DSSI facility to ensure that seals have not been broken during transit. If seals are broken upon arrival at DSSI facility, Project Manager will verify content of boxes against the log file to confirm content. Any discrepancies will be reported to the CLIENT immediately.
- ❖ DSSI transportation vehicles are secured by alarms and/or kill switch. In addition, fire extinguishers and cell phones are maintained in the vehicles.



Security Protocols

- ❖ DSSI maintain unique log-in to each workstation and maintenance logs create audit trails of PC usage; workstations automatically log-off after 2 minutes of idleness
- ❖ DSSI password policy calls for passwords to be changed every month, disallowing the use of previously used passwords.
- ❖ DSSI does not allow food in the production area; only beverages with covers or tops are allowed in production and only in designated areas away from documents.
- ❖ Network printers and photocopiers are not connected to the production network; those connected to our open network are password protected
- ❖ Cell phone and cameras are not allowed in production, but remain in a designated area for personal items of production staff.
- ❖ Each staff member has a security badges with photos
- ❖ When documents exit the production process, they are staged in the post production area by the project manager where the production manager, in dual control with the project manager validate the next steps for the documents whether that be to return to the client or to stage for shredding.

Insurance Policy

- ❖ DSSI maintain general liability insurance. It is recommended to all clients that their general liability business insurance contain a “valuable papers clause” that extends coverage to documents at off-site facilities.

Testing and Review Process

- ❖ DSSI does an annual review of security procedures and does bi-annual testing of all procedures for continuity assurance.

