DATA SECURITY

THE PROTECTION OF YOUR INFORMATION

IS OUR PRIME DIRECTIVE

OVERVIEW

BUILDING SECURITY

THEFT ALARMS • POINT OF ENTRY • INTERIOR & EXTERIOR CLOSED-CIRCUIT CAMERA MONITORING
IMPACT-RESISTANT WINDOWS • MOTION SENSOR STORAGE • KEY CARD ACCESS

SOFTWARE SECURITY

CENTRALIZED DATA MANAGEMENT • SSL ENCRYPTION MAILING DATA UPLOAD/TRANSMISSION
PGP DISK SOFTWARE • ENCRYPTION STORAGE

POSTAL SECURITY

SENSITIVE/CONFIDENTIAL STOCK • KEY CARD ACCESS • CLOSED-CIRCUIT CAMERA MONITORING

EMPLOYEE SECURITY

BACKGROUND CHECKS • ONGOING TRAINING & EMPLOYEE ENHANCEMENT

COMPLIANCE/AUDIT

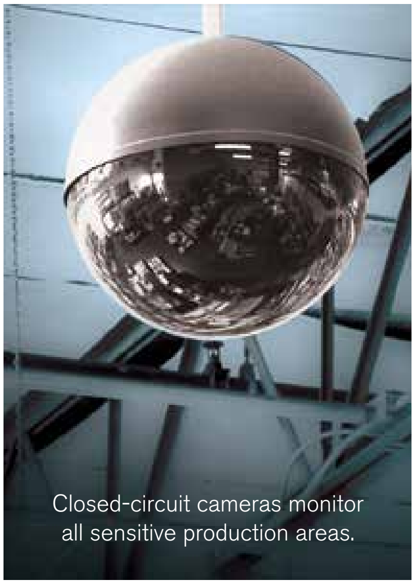
POLICIES AND PROCEDURES • RECURRING SITE AUDIT CHECKS • SYSTEM PENETRATION TESTING
NETWORK VULNERABILITY ASSESSMENTS

A MEASURE OF SECURITY

THAT NO ONE ELSE MEASURES UP AGAINST

Sure your proprietary information may be safe and secure in the vault of your company, but what about when it's sent outside? En route? With a vendor? Or at a mailing house? Are you currently doing everything you can to ensure your clientele that their vital identity information is well protected by your organization?

With Westamerica Communications, you will have complete confidence that your data receives security measures that are unprecedented in our industry. From the moment we begin working with you, until the time your communication piece leaves our facility—the processes and procedures that we have in place will put your mind at ease.



Closed-circuit cameras monitor all sensitive production areas.

Your most important asset is your clients' trust. Cherish it. Our greatest asset is your company's trust. The following pages describe the comprehensive measures we've taken to affirm the utmost in security to keep your data safe and to earn your trust. We have gone above and beyond the industry standard in our security practices as we do in all of the services we provide.

BUILDING SECURITY

KEEPING OUTSIDERS OUT

MAXIMUM SECURITY 24/7

The first part of protecting our clients' valuable information begins by keeping the unwanted away from entering our facility. We've incorporated several different deterrents to maintain maximum security at all times.

THEFT ALARMS

Perimeter doors, including all roll-up doors, have alarm points and interior motion sensors. All windows throughout our facility have glass breakage sensors. The data processing room is separated from the main warehouse and has a separate alarm zone and code so any unauthorized entry into that area will trigger an alert. Skylights on the rooftop are guarded by electronic beams to defend against overhead entry.

POINTS OF ENTRY

All pedestrian doors are equipped with reinforced guarding hardware to deter forced entry. To obtain access into the mailhouse, personnel must use a keycard. Each authorized employee with a keycard has restrictions programmed into the card, thus limiting their hours of access to appropriate times of the day when other personnel are present. An additional card access system is also on the four doors leading into the data processing room. Again, these entry points will only allow access under time-controlled limits and for select employees only. All roll-up door openings have locked, six-foot, steel folding gates which serve to thwart access and entry by unauthorized people or personnel. Closed-circuit cameras monitor the building's outer perimeter as well.

INSIDE

Mounted closed-circuit cameras (with 24-hour recording) are strategically positioned over all areas of production (folding, inserting and packaging), as well as over entrance and exit doors. Within the secure data processing room, additional cameras cover the laser image processing (including lettercheck programs) as well as the entrance and exit doors.

WINDOWS

All glass windows within the data processing room, both interior and exterior, have been treated with an impact-resistant security film.

STORAGE

All sensitive materials (lettercheck stock, printed letterchecks, and work-in-progress files) are kept in a secure storage room adjacent to the data center. Key-card access is limited to authorized personnel under video surveillance. Furthermore, work-in-progress CDs, and/or tapes with data, are converted to digital format, transferred to encrypted volumes on our servers and destroyed immediately after use.

LIGHTING

As an additional deterrent, the exterior of the building is illuminated at night through the use of security lighting and motion-activated lighting.

SOFTWARE SECURITY

KEEPING YOUR DATA SECURED

Our number one goal is to keep our client's proprietary information exclusive to the proprietor. We have implemented many different procedures covering how data flows from the client through project completion—carefully and constantly protected.

CENTRALIZED DATA MANAGEMENT

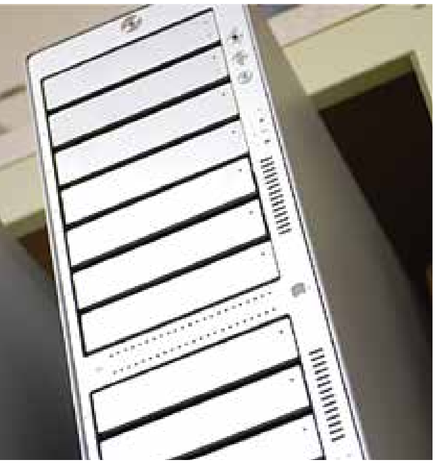
All client mailing data/information is centralized on our secure server in a separate room. This room is behind two locked doors with very limited key-card access. The inside of the room is under camera surveillance and has a motion sensor as well as a sensor above the ceiling to alarm against overhead entry. Additionally, this room has its own separate alarm zone and key pad.

During project workflow, clients are able to upload data securely and easily through an SSL encryption interface developed specifically for us. Access to this portal is restricted to customers only. This portal bypasses other, more commonly used, unsecured ways of transferring data such as e-mail and FTP. All clients' mailing data is then stored on a secure server in which an Encrypted Disk software is employed. Access to this server, as well as passwords to the Encrypted Disk, are restricted to only those people directly processing data. If new data is received via CD, tape or other disk (submitted by client/source in an encrypted format), mailhouse personnel copy the material on to an encrypted virtual disk where it is secured with a 256-bit encryption.

Once the data is verified and validated, mailhouse personnel then log and destroy the media that carried the data (unless by prior written authorization from the client, Westamerica Communications will not return original media containing data, but will, instead, destroy it). When a project is ready to drop at the post office, mailhouse personnel log the job as "complete" and move the data to a new holding folder, which is also on an Encrypted Disk.

The data remains encrypted the entire time it is in our care, whether on the original encrypted medium from the client, or residing encrypted on our secure server in the IT department. The holding folder is then deleted using PGP Wipe, logged as deleted, signed off and placed within the project file database. Final notification of drop date and data deletion will be sent in e-mail format to the client upon project completion for audit purposes.

In the case of a client sending data for multiple drops, we maintain that data on our system only with authorization from the client. The same procedures will then apply.



24-hour surveillance and video recording.
Separate access controls are in place for the data center.

POSTAL SECURITY

KEEPING MAIL IN CHECK

Making sure that the only eyes to see your materials are the postal carrier's and the intended recipient's is another aspect that Westamerica Communications monitors for maximum protection.

SENSITIVE/CONFIDENTIAL STOCK (with personal or account information)

All projects that are awaiting mail drops are packaged on skids using USPS-approved protocol and security-wrapped to completely enclose the skid as it awaits delivery to the post office. While awaiting delivery, such skids are held in a holding area monitored by closed-circuit cameras.

Projects with delayed drop dates are kept in a secure data room that is only accessible with a special key-card.

Any stock printed incorrectly, or wasted as part of the make-ready process, is immediately verified and shredded.

For tracking purposes, all lettercheck projects include the validation of starting and finishing quantities, and are signed off by the mailhouse manager. After the printing and the verification of quantities, employees handle the folding, inserting and packing of the project for delivery. Final verification and sign-off is the responsibility of the mailhouse manager.

All finished projects are security-wrapped in preparation for postal delivery.
Closed-circuit camera requires **badge entry** for employees.

EMPLOYEE SECURITY

KEEPING PERSONNEL IN CHECK

The team we've assembled at Westamerica Communications is unlike any other. All of our personnel have been hand-chosen and put under a microscope before they even set foot into our facility.

BACKGROUND CHECKS

As a company policy, we perform background checks on all new employees. These checks include DMV records, criminal records, credit checks and reference reviews. We also drug test for all new employees and conduct random testing for all existing mailhouse employees.

TRAINING

We train (and retrain) all employees in the various aspects of security and procedures on an ongoing basis. This training is conducted both formally and informally. It includes detailed information about our workflow procedures, security guidelines and overall company practices.

COMPLIANCE

KEEPING IN CHECK

One of the most critical elements of our security measures and procedures is the ability our clients have to determine the safeness of their data with our company. We have retained an outside operational, security management consulting firm to review and assess our operation and develop a comprehensive policy and procedure document which addresses such concerns as: risk assessment, database encryption, virus protection, physical security controls, logs/tracking, workflow processes, disaster recovery, training, hiring, recurring site audit checks, system penetration testing and network vulnerability assessment, incident response plans, customer awareness, privacy applications and others as well. This document is regularly reviewed, tested and updated.

We invite our current clients, and those considering utilizing our services, to visit our facility and conduct their own tests. We want you to be confident that everything that can be done to protect your valuable data will be. If you have a concern about any area of our operation, we will address it directly and take the appropriate action to ensure full compliance with your individual request.

We understand that not all businesses operate in this manner, but perhaps not all businesses value their clients' data the way we do. We are **Westamerica Communications**, the place you can trust.

Westamerica
Communications

26012 Atlantic Ocean, Lake Forest, CA 92630

Phone 949 462.3600 | Fax 949 462.3700 | mywestamerica.com