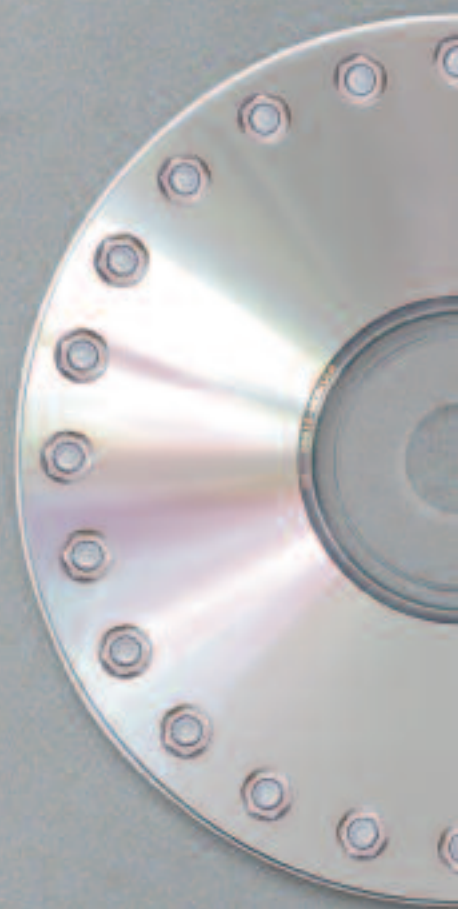




DATA SECURE



AN OVERVIEW with no oversights



BUILDING SECURITY

- Theft Alarms**
- Point of Entry**
- Interior 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**
- Encrypted Storage**

POSTAL SECURITY

- Sensitive/Confidential Stock**
- Key Card Access**
- Closed-Circuit Camera Monitoring**

EMPLOYEE SECURITY

- Background Checks**
- Ongoing Training**

COMPLIANCE/AUDIT

- Policies and Procedures**
- Recurring Site Audit Checks**
- System Penetration Testing**
- Network Vulnerability Assessments**




Keeping PSB in check — Compliance




One of the most critical elements of our new security measures and procedures is the ability of our clients to determine the safeness of their data with our firm. PSB has 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 will be regularly reviewed, tested and updated.

We invite our current clients and those considering utilizing our services to visit our facilities and conduct their own tests. We want you to be absolutely certain that anything that can be done to protect your trusted data will be done. If you have a concern about any area of our operation, we will address it head-on and take the appropriate action to ensure full compliance with your individual request.

We know not all conduct their businesses in this fashion, but then perhaps not all value their clients' data the way we do. We're **PSB, The Marketing SuperSource** — the place you can entrust, beyond a shadow of a doubt.



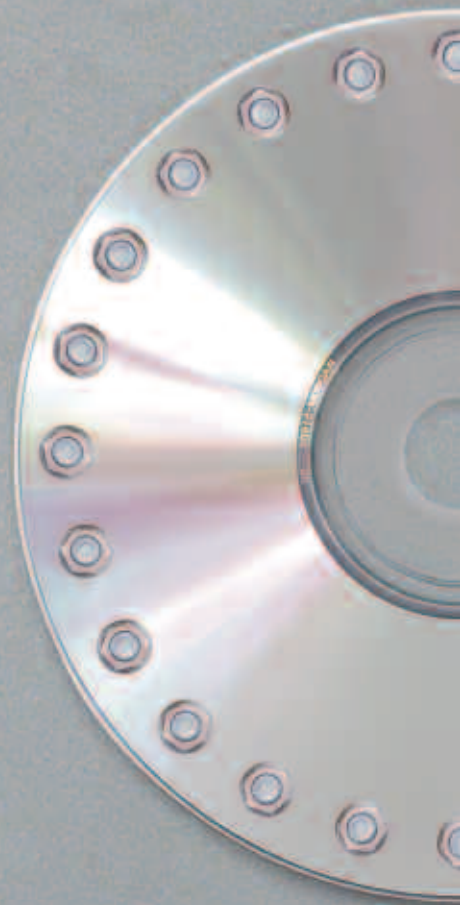
A measure of security
that no one else
measures up against




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


With **PSB, The Marketing SuperSource**, you 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 would make Fort Knox proud.

Your most important asset is your clients' trust. Cherish it. PSB's greatest asset is your company's trust. And to ensure that it's not breached, the following pages describe the extreme measures we've taken to affirm the utmost in secure working environments. Not just raising the bar of security, but placing it out of anyone's reach. It's up and above what you'd expect — but that's just the PSB way of doing business.





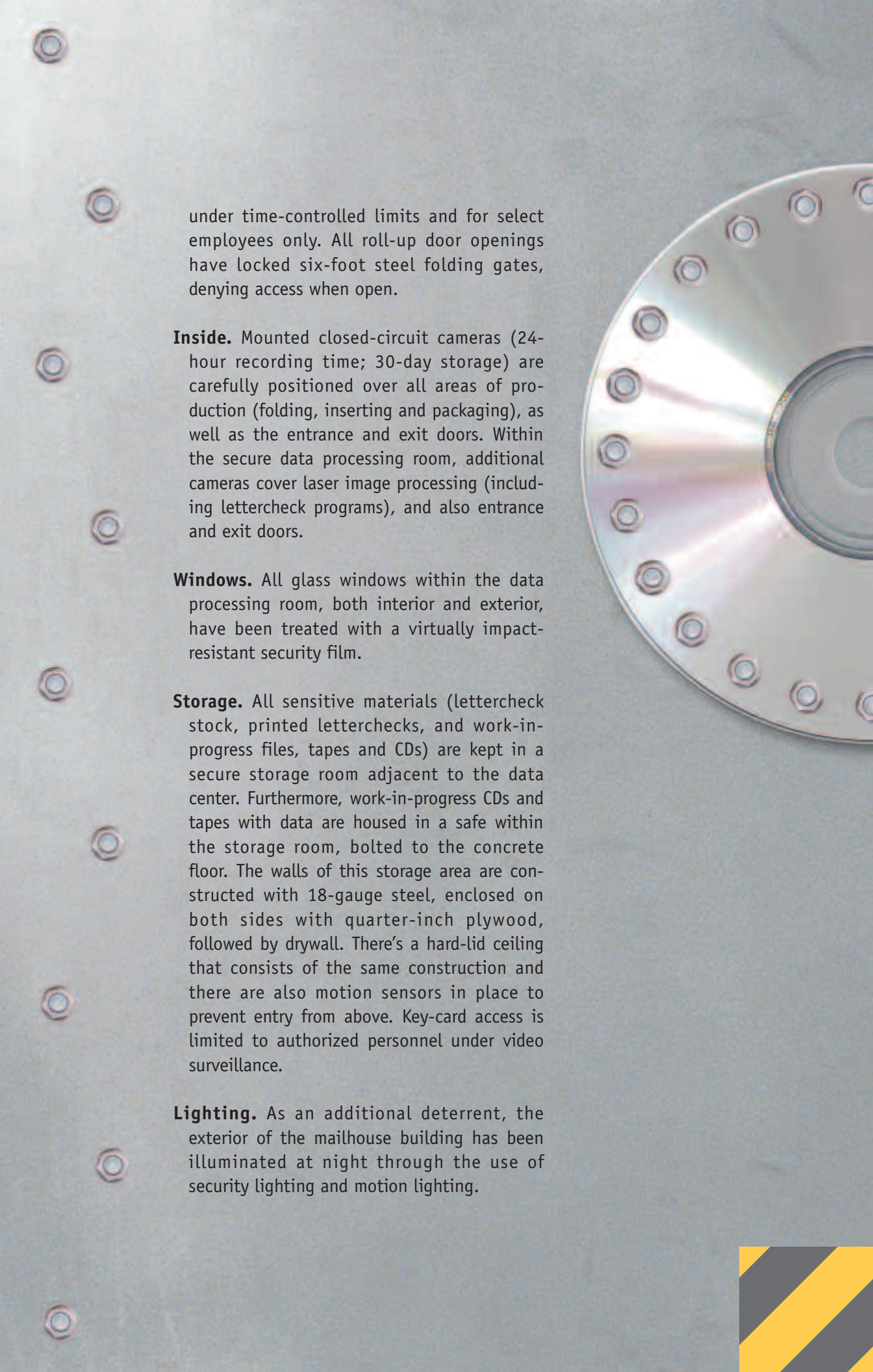
Keeping outsiders out — Building Security



The first part of protecting our client's valuable information begins by keeping the unwanted away from entering our facilities. 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 facilities have glass breakage sensors. The mailhouse data processing room has been separated from our mailing warehouse and has a separate alarm zone and code, so any unauthorized entry into that area will trigger an alert. In our main facility, motion sensors above the ceiling of our IT department monitor client data that is held encrypted on a secure server. Skylights on the mailhouse rooftop are guarded by electronic beams to defend against overhead entry.

Points of Entry. All pedestrian doors have been equipped with reinforced guarding hardware to deter forced entry. To obtain access into the mailhouse, personnel must use a key-card. Each authorized employee with a key-card has restrictions programmed onto the card, thus limiting the hours to appropriate times only. 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 into these areas




under time-controlled limits and for select employees only. All roll-up door openings have locked six-foot steel folding gates, denying access when open.


Inside. Mounted closed-circuit cameras (24-hour recording time; 30-day storage) are carefully positioned over all areas of production (folding, inserting and packaging), as well as the entrance and exit doors. Within the secure data processing room, additional cameras cover laser image processing (including lettercheck programs), and also entrance and exit doors.

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


Storage. All sensitive materials (lettercheck stock, printed letterchecks, and work-in-progress files, tapes and CDs) are kept in a secure storage room adjacent to the data center. Furthermore, work-in-progress CDs and tapes with data are housed in a safe within the storage room, bolted to the concrete floor. The walls of this storage area are constructed with 18-gauge steel, enclosed on both sides with quarter-inch plywood, followed by drywall. There's a hard-lid ceiling that consists of the same construction and there are also motion sensors in place to prevent entry from above. Key-card access is limited to authorized personnel under video surveillance.

Lighting. As an additional deterrent, the exterior of the mailhouse building has been illuminated at night through the use of security lighting and motion lighting.





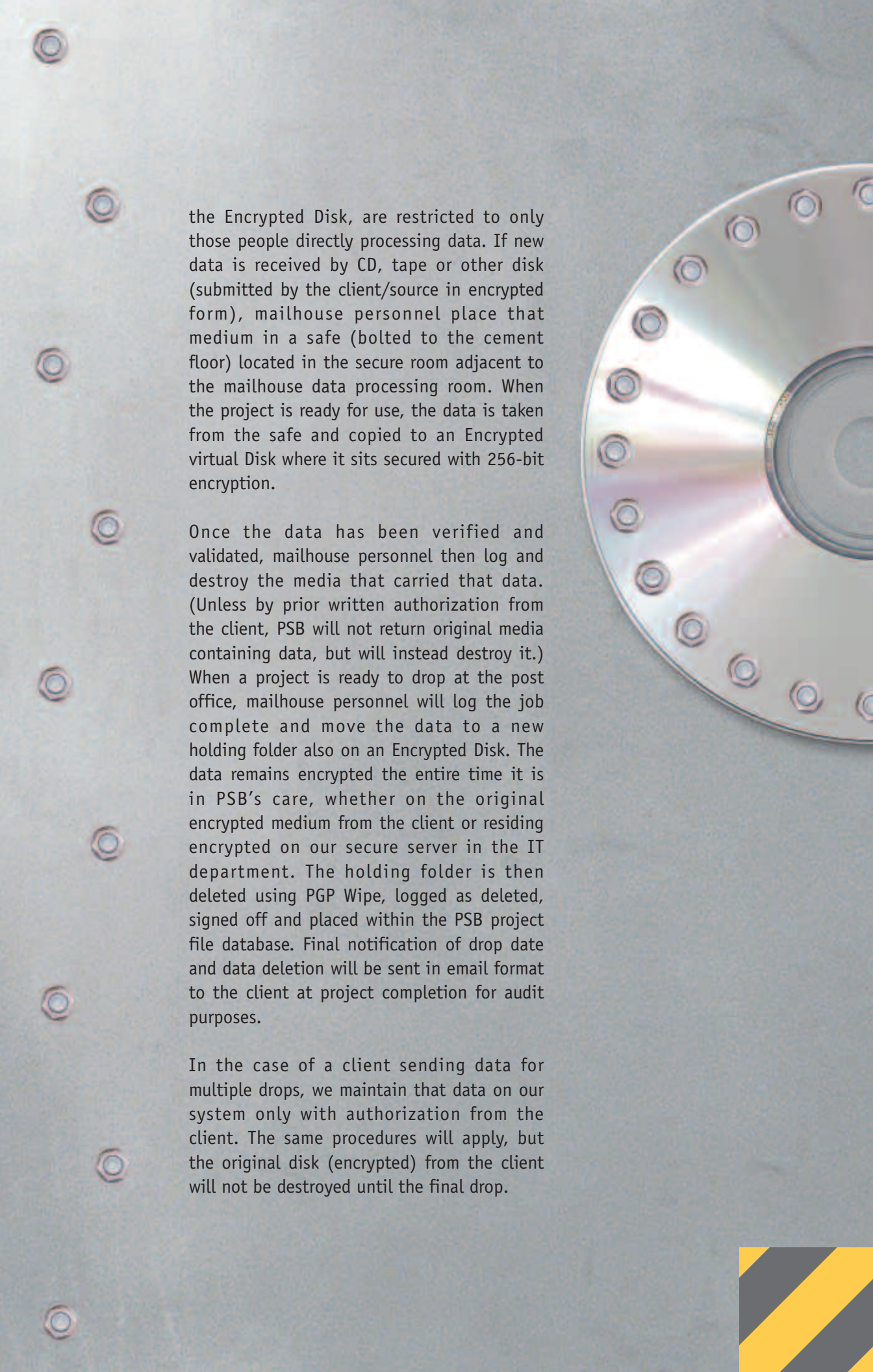
Keeping data in check — Software Security



Our number one goal is to keep our client's proprietary information exclusive to the proprietor. We've 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 has been centralized on our IT department server in the IT room at our main PSB facility. This room is behind two locked doors, the second being the IT department door and has very limited key-card access. The inside of this room is under camera surveillance and has a motion sensor; another sensor is above the ceiling to alarm against overhead entry. The IT 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 PSB. Access to this portal is restricted to PSB customers only. This portal bypasses other, more commonly used, insecure ways of transferring data such as email and FTP. All clients' mailing data is then stored on a secure server in which an Encrypted Disk software has been 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 by CD, tape or other disk (submitted by the client/source in encrypted form), mailhouse personnel place that medium in a safe (bolted to the cement floor) located in the secure room adjacent to the mailhouse data processing room. When the project is ready for use, the data is taken from the safe and copied to an Encrypted virtual Disk where it sits secured with 256-bit encryption.

Once the data has been verified and validated, mailhouse personnel then log and destroy the media that carried that data. (Unless by prior written authorization from the client, PSB 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 will log the job complete and move the data to a new holding folder also on an Encrypted Disk. The data remains encrypted the entire time it is in PSB's 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 PSB project file database. Final notification of drop date and data deletion will be sent in email format to the client at 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 apply, but the original disk (encrypted) from the client will not be destroyed until the final drop.



Keeping mail in check — Postal Security



Making sure the only eyes to see your material are the addressees and the postal carriers is another checkpoint PSB monitors for maximum protection.

- **Sensitive/Confidential Stock** (with personal or account information). All projects that are awaiting mail drops are packaged on skids for delivery to the post office in USPS-approved format and security-wrapped to completely enclose the skid. While awaiting the delivery, such skids are held in a holding area monitored by closed-circuit camera.

Projects with delayed drop-dates are kept in the secure, key-card access room adjacent to the data room.

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

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



Keeping personnel in check - Employee Security



The team we've assembled at PSB 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, PSB performs 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.

Training. We train (and re-train) all employees of the mailhouse in the various aspects of security and procedures on an on-going basis. This training is conducted both formally and informally and includes detailed information about our workflow procedures, security guidelines and overall mailhouse policies.

