

FOR IMMEDIATE RELEASE
CONTACT:

Corporate Communication
WesTex Document Inc.
815 S. Gilbert Dr
Reese Technology Center
Lubbock, TX 79416-2128
800.280.7532



February 2, 2012, Lubbock, TX - The region's premier record's management company was just recognized for meeting high standards for privacy of information. WesTex Document, Inc, with facilities in Lubbock and Amarillo, was recognized by PRISM International (Professional Records & Information Services Management) for meeting their Privacy+ Certification Criteria. The certification was the first in the state of Texas and one of seven in the United States to be awarded under PRISM's new program.

This wasn't the only time that WesTex Document, Inc. was first to achieve high standards for conducting their business. In 1999 they were the first in Texas and the 4th in the country to earn certification from the National Association for Information Destruction (NAID). They are also the only privately held corporation in the country approved for storing records for the nuclear industry, having met the Nuclear Quality Assurance (NQA-1) records management standards.

"When I started WesTex Document Inc in 1997 I knew that I wanted to make Rolex's and not Timex's. They are both watches that tell time, but one sets higher standards for itself, knowing who its customers are," said John Miller, President and CEO of WesTex Document. "I wanted WesTex to be known as the "Rolex" of the records management industry and seek out the very best of customers that want the very best vendor."

The Privacy+ standards are to be met in connection with the safeguarding of client information contained in paper and electronic records. This program is offered on a voluntary basis to all PRISM International companies. The objectives are to ensure the privacy of information in a manner consistent with industry standards as well as protect against unauthorized access or use that may result in harm to any consumer.



- more -

Program Requirements

To become certified, a company must meet the following criteria:

Create a written information privacy policy.

- Designate a privacy officer.
- Implement administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of client information
- As required by law, report to its clients any unauthorized use, disclosure or breach of client information of which it becomes aware.
- Ensure that if agents, including subcontractors, are provided access to client information, they are contractually bound to appropriately protect the information.
- Ensure information is protected against unauthorized access

Privacy Plus Certification Criteria

1. Administrative

- 1.1 Appropriate safeguards to protect the privacy of client information during handling
 - 1.1.1 Written privacy policy
 - 1.1.2 Designated privacy officer
 - 1.1.3 Documented controls and procedures
 - 1.1.3.1 For visitor access to storage areas
 - 1.1.3.2 For handling customer information inside storage areas
 - 1.1.3.3 For handling customer information in transit
 - 1.1.3.4 For employees to report suspected breaches
 - 1.1.3.5 For responding to suspected breaches
 - 1.1.3.6 For responding to clients regarding breaches as required by law
 - 1.1.3.7 For sanctioning employees who violate privacy policies
 - 1.1.4 Testing /auditing of documented controls and procedures
- 1.2 Employee training: all employees exposed to sensitive information trained annually.
 - 1.2.1 On privacy policy
 - 1.2.2 On documented controls and procedures
 - 1.2.3 On awareness of privacy laws and regulations
 - 1.2.4 New employees exposed to sensitive information trained within 30 days of hire date.

- 1.3 Annual privacy risk assessments
 - 1.3.1 Identify privacy risks
 - 1.3.2 Mitigation plan documentation
- 1.4 Contractual controls to ensure that information shared with other third parties is appropriately protected by the third party
- 1.5 Pre-employment screening process in place for all employees
- 1.6 Confidentiality agreements signed by all employees

2. Technical

- 2.1. Applicable safeguards are in place to protect the privacy of client information stored digitally in company's IT systems
 - 2.1.1 Risk-appropriate firewall and anti-virus software installed and properly functioning
 - 2.2 If clients are provided access to their online inventory, then encryption during transmission must be properly installed and utilized

3. Physical

- 3.1 Applicable safeguards are in place to protect physical information against unauthorized access while in transit and in storage
 - 3.1.1 Monitored security system on all storage facilities
 - 3.1.2 All access doors to storage areas either locked or access area is controlled and monitored
 - 3.1.3 Vehicles containing client information are locked at all time

In addition, applicants must certify that at least one representative of their company has attended and completed the Privacy+ Certification preparedness program within the past 12 months.

###