



DISABILITY SPECIALISTS
INCORPORATED

CLIENT DATA SECURITY PROGRAM OVERVIEW

We take data security seriously

Disability Specialists, Inc.
20055 SW Pacific Hwy
Suite 203
Sherwood, OR 97140

www.gotodsi.com

888.279.8304 *(toll free)*

t: 503.620.1055

f: 503.620.2099



Disability Specialists, Inc. is committed to client data security and protection. We have addressed this concern by implementing and maintaining stringent safeguards to protect the security and privacy of our customers, vendors, and joint venture partners (our clients).

To that end, DSI strives to maintain the highest standards of trust, loyalty, integrity, and quality. Our goal is to provide our clients with exceptional service, the highest quality products, and advice, and to make every effort to insure the security and privacy of our clients' confidential information.

DSI has taken the following measures to enhance Data Security.

- ***Network Protection***

DSI is participating in an ongoing program that provides network security scanning and technology risk assessments. Both the internal networks as well as all external network access points are tested on a recurring basis. The audit conventions utilized are a blending of the FDIC and NASD standards due to DSI's housing a mix of confidential financial and medical information for our clients.

- ***Secure Census Data Transmission***

DSI has enhanced the transmission of sensitive information files into and out of our company by implementing a secure website and data transmission processes. The site utilizes the standards based SSL encryption protocol using 128bit encryption. It is used to upload and download sensitive census data transmission files and information between DSI and our clients via our FTP web site.

- ***Biometric Security***

DSI has implemented biometric security protection on all of our desktop computers. Biometric security has been proven superior to the other means of positive identification that rely upon cards, PINs, passwords, or personal information. Biometric Technology analyzes and measures certain biological characteristics (fingerprints) of an individual to create a unique identifier which can be electronically stored and retrieved for positive identification. The fingerprint reader recognition authenticates a user's identity by matching a current scan against the authorized fingerprints stored in the user database, thereby restricting access to unauthorized users.



- ***Sensitive Data Stored Outside of Network***

DSI has taken additional measures to protect our client's data in the improbable event our network security is breached by hackers.

Immediately after DSI receives client census data, an encrypted code converts every individual Social Security Number (SSN) to a new eight digit "DSI Number" (DSIN). The census data, void of any client SSNs, is then imported onto the DSI network. Therefore if our network is hacked, SSNs will not be accessible, lessening the risk of Identity Theft.

The original census data containing SSNs is burned onto CD and then locked in a fireproof safe. Only DSI's President, VP of Operations, Systems Manager, and Accounting Manager have the combination to the safe. When this data is no longer needed the disk is destroyed.

- ***Confidentiality and Non-Disclosure Agreement***

Upon execution of a working agreement between DSI and our client, DSI will agree to be bound by a thoroughly exhaustive confidentiality and non-disclosure agreement. DSI will pledge to maintain appropriate measures that are designed to protect the security, integrity, and confidentiality of any and all customer nonpublic personal information that their client makes accessible to them.

Further, all DSI employees are required to sign a confidentiality and non-disclosure agreement covering, but not limited to, nonpublic personal, financial and medical information concerning DSI's customers.

- ***Hard Copy Protection***

DSI employees are required to take extreme precaution on those occasions when dealing with hard copies of documents containing sensitive and confidential information. All such documents are locked in file cabinets on a nightly basis.

- ***Hard Copy Destruction***

All sensitive documents are immediately shredded once it's determined they are no longer needed. We require from our shredding company "Certificates of Destruction" to ensure proper disposal.