Vinocom.NET
Technology Services
5011 Pritchard Ohltown Road
Newton Falls, Ohio 44444
(330) 307-2354
WWW.VINOCOM.NET

iDrive Online Backup - Data Security

Encryption

Your data is encrypted with 256-bit AES encryption on transfer and storage. On sign up, provide your private encryption key (known only to you and not stored anywhere on our servers) or opt for the system-based encryption key. We recommend that you choose your own private encryption key to maintain utmost data confidentiality.

Physical security

The IDrive application is hosted at our data centers in the United States. The world-class facilities are custom designed with raised floors, HVAC temperature control systems with separate cooling zones and seismically braced racks. They offer the widest range of physical security features, including state-of-the-art smoke detection and fire suppression systems, motion sensors, 24/7 secured access, video camera surveillance and security breach alarms.

Network security

We have periodic third party reviews of our network infrastructure to check for known application and service vulnerabilities.

Backup of Backups

Your data resides on RAID-protected industry leading storage devices with multiple levels of redundancy. In addition, data is periodically backed up to another set of devices for additional security.

iDrive Compliance

Are you mandated by a governing agency?

Allow IDrive to assist your organization to comply with the regulations governing your industry.

What is motivating your Disaster Recovery Plan?

Many businesses now face federal and governing agency mandates to maintain complete backup records of all their electronic business transactions. Industry-specific regulations to impose confidentiality, industry portability, and preservation of financial records force many organizations to implement processes to support data backup and recovery objectives.

IDrive can assist companies within the medical, accounting and legal professions to comply with these new standards to avoid the penalties now being levied against violators of HIPAA, SOX, GLBA, SEC / NASD.

IDrive assists your company meet the compliance mandate by providing:

- ✓ Secure data transfer/storage using 256-bit AES encryption
- ✓ Encrypted data storage to prevent tampering / alterations / unauthorized access
- ✓ Date and time stamped data access by each user
- ✓ 24/7 data access via any broadband connection

Note: Many of the compliance items require usage of the optional private encryption key that is known only to the user and not stored on IDrive servers.

iDrive – HIPAA Compliance

Health Insurance Portability and Accountability Act Compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the result of efforts by the federal government to ensure healthcare data practices allow patients to easily move jobs, insurance, and/or healthcare providers.

The goals and objectives of this legislation are to streamline industry inefficiencies, reduce paperwork, make it easier to detect and prosecute fraud and abuse, while enabling workers of all professions to change jobs easily even if they (or family members) had pre-existing medical conditions.

HIPAA requires the ability to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of information. Healthcare organizations are required to individually assess their security and privacy requirements and take suitable measures to implement electronic data protection (both in transit and in storage). As proposed, a HIPAA-compliant information system must include a combination of administrative procedures, physical safeguards, and technical measures to protect patient information while it is stored and transmitted across communications networks. IDrive Inc. provides critical data security protection without compromising patient privacy and can help customers achieve HIPAA compliance.

IDrive assists healthcare providers to be HIPAA compliant in the following manner:

- ✓ Unauthorized access to individually identifiable health records is strictly forbidden; data is encrypted and transmitted securely to a vault that resides at a world-class data center that provides SOC approved data protection service.
- ✓ Access to the vaults and the data center is strictly controlled through administrative procedures, physical safeguards, and technical security measures to prevent unauthorized use or disclosure of customer data.
- ✓ Data remains on the IDrive servers for as long as you wish to retain it.

iDrive – SOX Compliance

Sarbanes-Oxley (SOX) Act Compliance

The Sarbanes-Oxley (SOX) Act of 2002 legislates how long and the manner in which companies store their financial records. Created largely in response to the Enron and WorldCom scandals, the SOX act is designed to safeguard against accounting errors and other illegal financial activities. In placing a more rigorous requirement on financial reports the storing of the records becomes vitally important because the trail of transactions must be secure.

The act specifically states that electronic records must be saved for at least five years to ensure that the auditors and other regulators can easily obtain requested documents.

The regulated companies in choosing a storage method will therefore look to a format that will insure it can satisfy the legal requirements of the SOX, i.e. the increased use of online remote data storage facilities / programs.

As an online data storage facility, IDrive is not privy to the contents of the information stored for a client. The customer must maintain responsibility for ensuring that it is in compliance as to what information is being kept and who in the organization (including independent auditors) has access. IDrive is only responsible for the availability and security of the information being stored and has put safe guards in place to ensure appropriate quality control standards.

IDrive assists with SOX compliance in the following manner:

- ✓ The data files backed up are encrypted on transfer and stored using AES 256-bit encryption and automatically decrypted during restores. The encryption is based on the private encryption key so that the data stored on IDrive servers cannot be decrypted by anybody other than you or a designate
- ✓ Your files are logged with a date and time stamp each time they are accessed
- ✓ All backups are immediately available from the web
- ✓ Data remains on the IDrive servers for as long as you want to retain it

iDrive – GLBA Compliance

Gramm-Leach-Bliley Compliance

All customers of financial institutions who maintain a relationship or obtain products or services such as those listed here are protected under GLBA.

GLBA affects a wide range of financial institutions such as banks, thrifts, credit unions and insurance firms as well as any firm engaged in activities including:

- Mortgage Lending
- Credit Card Activities
- Securities Brokerage Activities (Including Dealers and Advisors)
- Insurance Sales (Underwriters and Agents)
- Tax Planning and Preparation Services
- Investment Advice

A wide range of non-public personal information and personally identifiable financial information is subject to the privacy controls of GLBA.

IDrive answers security concerns in the following manner:

- ✓ The data is encrypted before transmission, always maintained in encrypted state and immediately available if required
- ✓ Data access is restricted by password authentication and is date and time-stamped by user
- ✓ Client access is only through authorized personnel with the encryption password, which is known only to the user
- ✓ Detailed reporting gives regulators a clear idea of the chain of custody of the stored information, and rapid access, should it be required

Data will remain housed in the IDrive customer storage areas for as long as the client retains it. IDrive does not have access to the contents of the data files stored, so it is up to the client to maintain the data in a manner that is compliant with GLBA.

iDrive - SEC / NASD Compliance

Securities and Exchange Commission (SEC) / National Association of Securities Dealers (NASD)

The Securities and Exchange Commission (SEC) and the National Association of Securities Dealers (NASD) have instituted regulations that demand compliance surrounding the storage of financial records and electronic communications.

IDrive assists IT departments with SEC / NASD regulations in the following manner:

- ✓ The data is automatically verified each time a backup takes place
- ✓ The data is available for online restores 24 x 7. All backups are stored with the catalogs (indexes) and accessible to authorized users at all times
- ✓ The data resides on RAID-protected industry leading NAS / SAN storage devices with multiple levels of redundancy. In addition, a regular data backup guarantees its availability when required.

Source: www.idrive.com

Source: http://www.idrive.com/online-backup-compliance.htm