

WHITE PAPER REPORT

Regulatory Compliance: How Remote Data Backups Helps



Remote Data Backups, Inc.

"A Decade of Data Protection"

www.RDBU.com | support@RDBU.com

866.722.2587 (866.7.BACKUP, toll-free)

1.970.493.2466 (international)

Introduction

Organizations today face many compulsory regulatory requirements.

Penalties for enterprises that do not comply with such requirements are severe. Are you protected in the event of an audit — or worse yet — a data loss?

Remote Data Backups solutions provide several ways to satisfy these requirements:

- ✓ Backup services to store electronic data off-site in secure, underground vaults
- ✓ Protection against data loss from natural disasters, human error, or sabotage
- ✓ Easy and complete data recovery
- ✓ Encryption that ensures privacy for sensitive information
- ✓ Coverage for servers, desktops, laptops, and remote computers
- ✓ Defense against disastrous and embarrassing disclosure of data through a lost or stolen notebook computer
- ✓ Data retention for selectable lengths of time (typically seven years)
- ✓ Rapid access and retrieval of information required for legal discovery
- ✓ Automatic and dependable processing
- ✓ Professional and experienced design and support services personnel

Organizations can leverage Remote Data Backups to help meet the challenges of regulatory requirements.

Remote Data Backups backup and recovery and encryption is valuable to many enterprises, not only for providing data protection and business continuity, but also for helping enterprises comply with new regulations. This white paper presents vital information about the regulatory requirements that enterprises must satisfy and how Remote Data Backups helps enterprises to satisfy them.

The Regulatory Challenges

Many enterprises must comply with an increasing number of regulatory requirements affecting their business — or face stiff penalties for non-compliance. The new requirements include these mandates:

- ✓ Protect business, financial, patient, employee, and customer information regardless of its format or medium — as required in HIPAA, Gramm-Leach-Bliley, and FACTA.
- ✓ Ensure the privacy of individuals — as required by HIPAA, Gramm-Leach-Bliley, and FACTA.
- ✓ Disclose corporate information for the government during compliance audits and for the courts during litigation — as required by the Sarbanes-Oxley Act of 2002 (SOX), and SEC Rule 17a-3 and 17a-4.
- ✓ Verify financial and business integrity for investors — as required by SOX.
- ✓ Demonstrate the security, availability, processing integrity, and confidentiality of the IT infrastructure environment — as required for SysTrust certification.

These mandates cover the growing volume of electronic documents, digital images, audio and video media, email, and instant messages, as well as paper and other physical records. In many cases, no paper records exist: only electronic records exist. Such electronically stored information (ESI) is admissible in court.

Specific regulatory requirements for electronic records also address the following issues:

- ✓ **Tamper-proof records.** SOX Section 802 prescribes penalties for altering or deleting key business documents, including electronic documents. In addition, SOX Section 404 requires enterprises to conduct a management assessment of internal controls, which would include an infrastructure to protect and preserve records and data from destruction, loss, unauthorized alteration, or other misuse.
- ✓ **Records retention.** Public companies must retain records within the SEC's legally specified time period, or for the period defined by their industry-specific regulations or other applicable laws and regulations.
- ✓ **Records disposal.** U.S. Department of Defense directive 5015.2 and its statutory references require deleting data in such a manner that it cannot be recovered using disk-scanning tools. This directive, which pertains to records management products acquired by the Department of Defense, is becoming a best practice for enterprises.
- ✓ **Duplicate storage.** It has become a best practice for enterprises to store duplicate records separately from the originals in a tamper-proof format that they transmit electronically to a remote location.
- ✓ **Legal status of electronic records.** Storing business records digitally does not affect their admissibility. ESI is admissible in court.

Table 1. Industries Affected by Regulatory Compliance

Regulation	Industry Affected					
	Financial Services	Healthcare	Manufacturing / Commercial	Energy	Retail	Government
HIPAA	✓	✓	✓	✓	✓	✓
SarBox	✓	✓	✓	✓	✓	
FACTA	✓	✓	✓	✓	✓	✓
GLB Act	✓					✓
SEC Rules 17a-3 & 17a-4	✓					

Clearly, many regulatory requirements involve Remote Data Backups. What role, then, do solutions that provide Remote Data Backups have in a comprehensive Compliant Records Management (CRM) program? How does Remote Data Backups support your compliance needs? Backup vs. Archiving Enterprises must separate backup data from archived data. Backups are for disaster recovery purposes, containing a snapshot of the system to restore it to its last known state. Archiving meets a long-term need for storing data with a searchable index for easy retrieval, if the need arises. Enterprises must follow retention rules for different types of archived data.

Remote Data Backups: a Critical Component of a CRM Program

Given growing regulatory laws, enterprises face serious obstacles to comply with a multiplicity of requirements.

Backup solutions that provide data protection, such as Remote Data Backups, help enterprises meet their compliance objectives.

HIPAA

HIPAA (Health Insurance Portability and Accountability Act of 1996) was enacted with a goal to support the protection of personally-identifiable health information (PHI). It limits using and disclosing information about the physical or mental health of an identifiable patient without his or her consent or authorization, as well as specifying the need for safeguards to protect PHI.



- ✓ Who must comply: Individuals and enterprises, such as doctors and other healthcare personnel, hospitals, pharmacies, medical billing services, healthcare plans, HMOs, and business associates of these enterprises, such as their accountants and attorneys.
- ✓ What it covers: All medical records and other health information that identifies the individual patient.
- ✓ Pertinent requirements: Administrative, technical, and physical safeguards that protect the privacy of a patient's health information by preventing any intentional or unintentional use or disclosure. In addition, records must be recoverable in the event of a small-scale or large-scale disaster.
- ✓ Penalties for non-compliance: Up to 10-year prison sentence and fines of \$25,000 per year. HIPAA has supplemental standards, in the form of "final rulings," which codify how health care providers and those who handle individually-identifiable patient health records must comply. The rulings include provisions that require compliant backup methodologies to ensure that individually identifiable health records remain private and secure. The security and privacy rulings require a backup plan, a disaster recovery plan, and an emergency mode operation plan (Section 164.308).

How Remote Data Backups Can Help

RDB solutions provide critical data security protection without compromising patient privacy. RDB solutions help enterprises meet or exceed HIPAA regulations.

RDB Solutions Meet Security Requirements

Health care providers must implement comprehensive security systems to ensure that they protect electronic patient records against data loss and unauthorized access. A HIPAA-compliant security system must include administrative procedures, physical safeguards, and technical measures to protect patient information while stored, and while transmitted across communications networks. The RDB solutions implement security and availability features in the following areas:

- ✓ Preserves a retrievable, physically secure, off-site, exact copy of patient records with easy, frequent data backups. Encrypts all data before it leaves the customer's server and keeps it encrypted during transmission and storage. Only the customer has access to the decryption password.
- ✓ Protects backup transmissions further by using integrity controls, mutual authentication, access controls, alarms for abnormalities, auditing of failed logins, and event reporting.
- ✓ Simplifies disaster recovery with tools to restore lost data quickly.
- ✓ Reduces media control risks, compared to traditional disk or tape backup techniques, by eliminating insecure methods of data handling, especially transporting physical media offsite.
- ✓ Offers multiple point-in-time backups per day — as often as every 15 minutes — to ensure that recovery is possible with minimal data loss.
- ✓ Allows long retention periods — as long as seven years — to meet HIPAA requirements.

RDB Solutions Meet Privacy Requirements

Under the HIPAA rules for the privacy of personal data, health care providers that engage in electronic transactions must observe privacy safeguards to restrict the use and disclosure of individually identifiable health information. As independent third-party service providers, Remote Data Backups and its subcontractors are "business associates" under the HIPAA security and privacy rules. If needed, Remote Data Backups will provide and sign a business associates agreement in conjunction with use of the FortBackup service. The FortBackup service and its agents do not receive data for any purpose except to provide data restoration after data loss. Because the data is encrypted before it leaves the customer's server and only the customer has access to the password, the FortBackup service and its agents cannot access the data.

RDB solutions are important parts of a HIPAA-compliant solution for preventing unauthorized access:

- ✓ **Secure Transmission and Storage:** Customer data is encrypted with 128-bit AES encryption, and then transmitted and stored as encrypted data at vaults that reside offsite at a secure remote facility. With the FortBackup solution, customer encrypted data may also optionally reside on an appliance at the customer's site to facilitate rapid recovery.
- ✓ **Logical Access:** Strict controls limit logical access to the data; for example, a secure user interface prevents viewing the contents of data files. In addition, customers can restore data only to the computer where the data originated, or to a computer where the customer has installed the data encryption key. The user interface cannot specify, change, transport, or access data encryption keys. By preventing loss of data, RDB solutions are also important for HIPAA-compliant strategies:
- ✓ **Physical Controls:** The data center is a hardened underground facility, meeting numerous physical criteria. The facility controls access through administrative procedures, physical safeguards, and technical security measures.
- ✓ **Redundant Vaults:** All backed-up data resides on two separate, redundant vaults. The data center has redundant bandwidth providers, power, and HVAC.
- ✓ **Retention for up to Seven Years:** Customers can retain historical backups for up to seven years.

RDB solutions complement physical safeguards to ensure that recent and vulnerable data receive protection automatically and regularly. This protection is critical, because sources of data are often distributed throughout an enterprise. Many of these sources rarely receive protection because of their remote location or poor resources for manual backup. RDB solutions can ensure that backup and protection extend to all areas of the business and their sensitive data.

This automated, regular approach provides auditors with proof of a good-faith attempt on the part of enterprises to protect their vital business information for the purposes of disaster recovery and business continuity. It also ensures data recovery for operations.

Remote Data Backups' DataRevoke solution deletes specified data — and can overwrite data locations to prevent recovery of deleted data — under conditions that administrators define. These conditions include a lost notebook computer, password tampering, and other evidence of unauthorized system access. The DataRevoke solution can prevent potentially disastrous and embarrassing disclosure of data, for example, when notebook computers are lost or stolen.

Proactive Effort

In addition to meeting the challenges of externally imposed regulations, enterprises must also work proactively to improve their IT processes for security, confidentiality, and robustness. Such proactive enterprises choose business partners and vendors that can assist them to meet these internal goals. SysTrust™ Certification demonstrate a partner's commitment to best practices.

Sarbanes-Oxley Act (SOX)

This Act implements multiple reforms to increase integrity in financial reporting. It prescribes:

- ✓ Federal oversight of public auditors
- ✓ A new set of auditor independence rules
- ✓ Protection for “whistleblowers” at publicly traded companies
- ✓ New disclosure and reporting requirements applicable to public companies and insiders
- ✓ Signed certifications of the integrity of financial reports from CEOs and CFOs. Severe civil and criminal penalties punish persons who are responsible for accounting or reporting violations.
- ✓ Who must comply: All U.S. and non-U.S. public companies that issue securities in the U.S. public markets, including their auditors, board members and lawyers.
- ✓ What it covers: Includes financial data and records, and related records and communications.
- ✓ Pertinent requirements: An infrastructure designed to protect and preserve records and data from destruction, loss, unauthorized alterations, or other misuse.
- ✓ Penalties for non-compliance: Up to a 10-year prison sentence and potential \$15 million fine.



How Remote Data Backups Can Help

RDB solutions help establish the required infrastructure and controls to protect and store vital company financial records, satisfying key requirements for privacy, security, and confidentiality:

- ✓ Getting data off-site and off-line protects and preserves the records from destruction, loss, and viruses. It also maintains a duplicate copy stored separately from the original.
- ✓ Storing information at an off-site vaulting facility ensures that data is protected and available for business continuity and disaster recovery.
- ✓ Using a trusted third-party vendor with a global footprint ensures consistent execution and monitoring of best practices, as determined by internal control frameworks, across the entire enterprise.
- ✓ Encrypting backup data prevents unauthorized access.

The Committee of Sponsoring Organizations (COSO, a private sector trade group supporting SOX) Internal Controls Integrated Framework divides the overall problem of IT risk assessment and control into two parts. One part includes general IT processes, such as data management, disaster recovery, and data center operations. The RDB services fall into this category. They comply with SOX requirements and provide strong controls for the data management functions. They also preserve the completeness and accuracy of backup data, so that processing following restoration is reliable. Access is restricted properly, assuring that data is not altered or deleted through the backup process. Only the Fort Backup solution provides guaranteed data recoverability through its limited warranty.

RDB solutions ensure that data protection for distributed data is automated and regular. This automated, consistent approach provides proof of a good-faith attempt on the part of enterprises to protect their vital business information for disaster recovery, business continuity, and general records compliance.

For more information on Sarbanes-Oxley compliance, please see the “SysTrust” section later in this document.

FACTA

The Fair and Accurate Credit Transaction Act (FACTA) makes permanent the national standards originally set by the Fair Credit Reporting Act (FCRA) of 1996. Originally, these consumer protections were to expire in 2003. FACTA also creates new provisions to combat identity theft and help its victims.



- ✓ **Who must comply:** Broker-dealers and those individuals who trade securities or act as brokers for traders, including enterprises such as banks, securities firms, stock brokerage firms, any financial institutions that trade any type of security governed by the SEC, and any entities under the jurisdiction of the National Association of Securities Dealers (NASD).
- ✓ **What it covers:** Information from creditors regarding fraudulent applications and transactions. It also covers any record about an individual, whether in paper, electronic, or other form, which is in a consumer report or is derived from a consumer report.
- ✓ **Pertinent requirements:** Victims of identity fraud may now request and obtain information from creditors, which creditors must supply.
- ✓ **Penalties for non-compliance:** Statutory damages, actual damages, punitive damages, and attorney's fees.

How Remote Data Backups Can Help

RDB solutions supply creditors with a reliable way to get their transaction and application information off-site, off-line, and out-of-reach to protect such data from loss or inadvertent destruction. If people suspect they might be a victim of identity theft and rightfully request their transaction and application information, such safeguards protect the necessary data from unauthorized access, but allow ready access to appropriate parties.

Enterprises should encrypt backup data containing consumer information as a precaution against disclosure. RDB uses 128-bit AES digital encryption in data transmission and storage, supplemented by strong physical security that includes hardened underground vault locations.

The DataRevoke solution can prevent potentially disastrous and embarrassing disclosure of data due to a lost or stolen notebook computer, tampering with passwords, or other unauthorized access. The solution can automatically delete and overwrite data that administrators specify.

Gramm-Leach-Bliley (GLB) Act

The Gramm-Leach-Bliley (GLB) Act requires that financial institutions ensure the security and confidentiality of their customers' non-public personal information. Identity theft has led the Federal government to create mandates to prevent even accidental disclosure of private information.

- ✓ Who must comply: Financial institutions have a continuing obligation to respect customers' privacy.
- ✓ What it covers: Customers' non-public personal information, such as Social Security numbers, credit records, and payment history.
- ✓ Pertinent requirements: Administrative, technical, and physical safeguards:
 - Ensure the security and confidentiality of customer records and information
 - Protect against any anticipated threats or hazards to those records.
 - Protect records against unauthorized access or use, which could result in substantial harm or inconvenience to any customer. -Ensure data recovery for operations.
- ✓ Penalties for non-compliance: Up to 10-year prison sentences and/or a maximum \$1 million fine. In addition, the Treasury Department, the Office of the Comptroller, the Office of Thrift Supervision, the Federal Reserve Board, and the FDIC have issued a joint final rule, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (the Guidelines). The Guidelines require an enterprise to involve its board of directors in assessing the risk, managing and controlling risk, and overseeing service provider arrangements. The Guidelines include the following Objectives:
 - ✓ Ensure the security and confidentiality of customer information.
 - ✓ Protect against any anticipated threats or hazards to the security or integrity of such information.
 - ✓ Protect information against unauthorized use or access, which could result in substantial harm or inconvenience to any customer. The Guidelines for management and control of risk include:
 - ✓ Access restrictions at physical locations.
 - ✓ Encryption, including while in transit or in storage on networks or systems to which unauthorized individuals might have access.
 - ✓ Dual control procedures.
 - ✓ Monitoring to detect actual or attempted attacks.
 - ✓ Measures to protect against destruction, loss, or damage due to hazards such as fire, water damage, or technological failure. The section on oversight of service provider arrangements requires:
 - ✓ Due diligence in selecting service providers.
 - ✓ Service providers by contract to implement appropriate measures designed to meet the Objectives of the Guidelines.
 - ✓ Where indicated, monitoring service providers, including review audits and test results.

How Remote Data Backups Can Help

Remote Data Backups, used together with best practices, protect sensitive customer information by getting the data off-site, off-line, and out-of-reach. Storing backup data off-site in secure, state-of-the-art vaulting facilities ensures security and protects data against threats or hazards including natural disasters, human error, or sabotage. Both solutions eliminate unnecessary exposure of information to human threats and natural disasters, while ensuring data security and privacy.

Encrypting backup data containing sensitive customer information is an advisable precaution to prevent unauthorized access. For these protection requirements, RDB solutions offer unmatched capabilities, including 128-bit AES encryption of all data in transit or at rest in storage. Only the customer has the password.

RDB ensure that data protection happens regularly and automatically, which is critical for the many sources of sensitive data distributed throughout an enterprise. Many go unprotected because of their remote location or poor resources for manual backup.

RDB can ensure that secure backup and protection extend to the sensitive data from all areas of the business. RDB best practices offer increased security using strong physical security in the form of hardened vault locations. Because they can back up and safeguard distributed data, RDB solutions meet requirements for operational data recovery. In the event of small-scale data losses, users can quickly recover data over the Internet. Remote Data Backups' DataRevoke solution can automatically delete and overwrite data that administrators specify. It can prevent potentially disastrous and embarrassing disclosure of data because of a lost or stolen notebook computer, tampering with passwords, and unauthorized access.



SEC Rule 17a

In 1934, to protect investors from fraudulent or misleading claims, the SEC enacted the Securities Exchange Act, a set of laws that required keeping records for reviewing and auditing securities transactions. SEC Rule 17a amends that law to allow broker-dealers to store records electronically, including electronic communications such as email and instant messages.

- ✓ Who must comply: Broker-dealers and those individuals who trade securities or act as brokers for traders, including enterprises such as banks, securities firms, stock brokerage firms, any financial institutions that trade any type of security governed by the SEC, and any entities under the jurisdiction of the National Association of Securities Dealers (NASD).
- ✓ What it covers: Electronic records and communications relating to traded securities governed by the SEC.
- ✓ Pertinent requirements:
 - Records retention on compliant media from the time of creation to final disposition.
 - Written and enforceable retention policies.
 - Storage of data on indelible, non-rewriteable media.
 - Readily retrievable and viewable data.
- ✓ Penalties for non-compliance: Suspension and potential fines up to \$1 million.

How Remote Data Backups Can Help

Although SEC Rule 17a does not explicitly require storing data off-site, off-site storage complies with the rule, and makes good business sense because it ensures that both copies of a record cannot be destroyed in the same disaster.

RDB solutions provide effective, efficient solutions for keeping critical information off-site and protected. The data is encrypted, making it unreadable to unauthorized people, yet easily accessible when needed.

Protection of data should continue as long as regulations or litigation requires, or until deliberate destruction as part of an end-of-life cycle. FortBackup can retain stored data for as long as the customer requires (typically seven years).

Backup and archiving are different processes and should remain distinct. Digital archiving solutions address the necessity for quick retrieval and provide audit trails of inactive data stored for specified retention periods for regulations and litigation.

RDB solutions ensure that the task of data protection happens automatically. It is critical to deal with the many sources of sensitive data distributed throughout an enterprise. Otherwise, this data might be unprotected because of its remote location or lack of manual backup resources. RDB solutions ensure that secure backup and protection include all areas of the business and all sensitive data.

SysTrust™ Certification

Our online backup system has been examined and SysTrust Certified by the independent accounting firm PriceWaterhouseCoopers.



SysTrust, an assurance service developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), tests system reliability according to four essential principles:

- 1. Availability**
The system is available for operation and use at times set forth in service-level agreements.
Our data centers have over 99.99% availability for the past 8 years.
- 2. Security**
The system is protected against unauthorized physical and logical access.
Restricted data center access, bank-level encryption, private key.
- 3. Processing Integrity**
System processing is complete, accurate, timely, and authorized.
Data is encrypted before it leaves the host, then transferred and stored in encrypted format.
- 4. Maintainability**
The system can be updated when required in a manner that continues to provide for system availability, security, and integrity.
Software and data center updates don't interfere with client backups and restores.

This certification process encompasses our general IT infrastructure, including:

- ✓ Production data center and network operations
- ✓ Server configuration and database administration
- ✓ Storage management systems
- ✓ Disaster recovery processes
- ✓ System monitoring tools and processes
- ✓ System security (both logical and physical)
- ✓ Change management and common support processes.

SysTrust vs. SAS#70 Compliance

SysTrust is a more stringent certification standard than SAS#70, and a more applicable compliance standard for online backup solutions.

Contrary to popular misconception, SAS 70 pertains to internal controls and practices within the company to deliver accurate and truthful financial information to its clients, and does not specifically address the backup company that handles their data.

The Sarbanes/Oxley Act of 2002 requires financial institutions to furnish SAS-70 Reports to its customers as a way of assert the level of controls over their financial statements and assertions.

Differences between SAS 70 and SysTrust audit engagements

Criteria	SAS 70	SysTrust
Nature of audit	Provides a report on a service organization's controls related to financial statement assertions of user organizations.	Provides a report on system reliability using standard principles and criteria for all engagements.
Pre-established control objectives or criteria?	No.	Yes.
Objective of audit	Information sharing and assurance. Provides detailed information on the design of the system and controls, an opinion on the system description and controls, and the results of the auditor's procedures.	Assurance on a system. No detail on the underlying control procedures is provided.
Types of systems addressed	Systems that process transactions or data for the user organization	Any system.
Distribution of report	Generally restricted to the service organization, user organizations, and prospective user organizations.	No restrictions.
Audience for the report	Service organizations, user organizations (i.e. customers), and auditors of the user organizations.	Stakeholders of the system - for example, management, customers, and business partners.

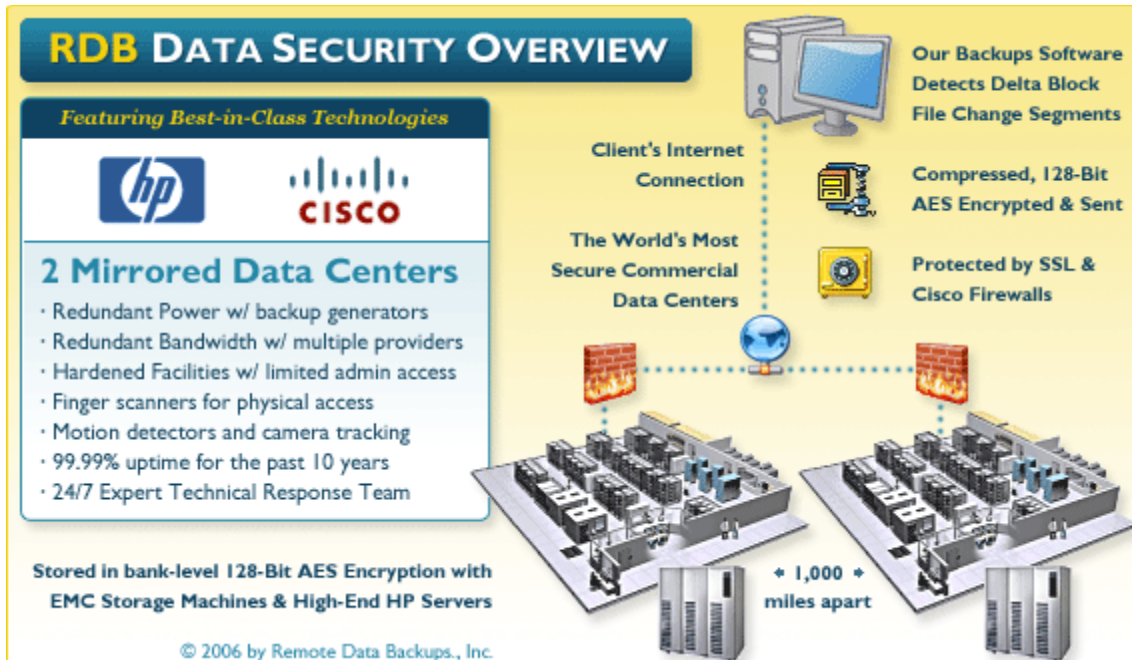
*From v.2.0 of "AICPA/CICA SysTrust Principles & Criteria for Systems Reliability".

Backup Data Security Overview

We've layered state-of-the-art technology to deliver industry-leading security and performance.

Your data is bank-level AES encrypted before it leaves your computer, then transmitted and stored encrypted at our two world-class, underground, mirrored Data Centers.

No one can access your data without your Personal Encryption Key. Redundant fiber optic bandwidth via multiple providers ensures extremely fast and reliable data transfers.



Superior Backup Data Center Technology & Service

Our mirrored data centers employ the industry's leading enterprise technologies to provide our clients with the best security, reliability and performance on the market.



Enterprise HP Servers

Deploying servers from Hewlett-Packard, the world's largest consumer and SMB IT company, helps our data centers maintain over 99.99% historical uptime.



Cisco Hardware Firewalls

Sophisticated hardware firewalls from Cisco, the leader in Network security, securely protect your backup files from hackers, viruses, spybots, etc.



Redundant Bandwidth

We use multiple enterprise bandwidth providers on multiple fiber optic backbones to ensure consistently fast and reliable file transmission.



Physical Security, Power Backup & Support

Both data centers are hardened facilities with finger scanners, motion detectors and camera tracking, redundant power generators and 24/7 Expert Response.



Two Mirrored Data Centers

We store your data at two world-class, geographically separate, mirrored underground backup centers with redundant bandwidth, redundant power and an unparalleled level of data security and performance.

Level 4 Data Center Security

Our two underground data centers are the world's most secure commercial data storage facilities. Features include:

- a. Separated by 1,100 miles, in ultra-secure private limestone mines located 100-200 feet below ground
- b. All data received by either hardened Data Center is immediately replicated to its mirror — connected by point-to-point, high-speed WAN links
- c. Traffic is load-balanced between the two sites, eliminating degraded system performance
- d. Redundant bandwidth with multiple fiber optic telecom providers to ensure consistently fast and reliable transfers
- e. Each server platform has fail over and redundancy, continuous server monitoring and performance tuning, assuring that storage capacity is never exceeded.

Enterprise Network Infrastructure

- a. Redundant power supply using backup generators, full power for 7 days
- b. High performance HP Servers & Cisco / Nokia firewall security
- c. Redundant completely independent electrical systems, power train, commercial power feeds, cooling system, UPS systems, dedicated A/C units, generator systems and fuel system
- d. Environment and climate controlled facilities, resistant to seismic activity and other natural disasters, with Class A vaults with OSHA certified fire suppression and EPA certified water treatment plants and clean air fire extinguishing systems (CAFES)
- e. Best practices networking and best-of-breed routers, switches, firewalls, servers, facilities infrastructure, power grids and telecommunications circuits are all deployed with backup components to maximize fail over and redundancy
- f. Failed account access attempts are logged and reviewed to prevent unauthorized access

Impenetrable Physical Security

- a. Level 4 (highest) security rating, 24/7 armed security, maintenance & service operation
- b. Finger scanners for physical access, motion detectors, CCTV monitoring & camera tracking
- c. Co-location equipment is locked in cage with sensors and alarm system
- d. Visitors require pre-authorization and photographic identification
- e. All access to computer equipment is logged

Data received by either Data Center is immediately replicated to the other, so an unlikely outage or disaster at one location will not affect your data availability or service performance.

This is a comforting fact in light of the frequency of recent natural disasters (hurricanes, floods, earthquakes, tornados, etc.) that can easily destroy a single, less fortified data center.



128-Bit AES Encryption

Your files are securely transmitted, stored and retrieved using government-level AES encryption.

If someone were to somehow intercept your data during a backup or restore, or gain access to our servers (which, of course, has never happened), it still take multiple supercomputers decades to decipher any of your data.

Advantages of encrypted backups

- It would be far easier for someone to steal your local backups (*tape*, *CD-DVD*, *Zip/Jaz*) than to intercept and decrypt your encrypted offsite data.
- Local backups containing your sensitive data are rarely encrypted or even protected by a simple password.
- Disgruntled employees, competitors, hackers, thieves, curious people who find lost tapes, etc. all jeopardize the safety of unencrypted backups. Backup tapes are pocket-size, so you might not even notice they are gone.

How Secure is 128-Bit AES Encryption?

If a super-computer could break the DES code in one second, it would take the same supercomputer 149 trillion years to decode a 128-bit AES key - longer than the existence of our universe. It is safe to say no supercomputer in the foreseeable future will be able to brute-force AES 128 bit. As long as no one finds your encryption phrase, your encrypted data can never be deciphered.

Secure Socket Layer (SSL)

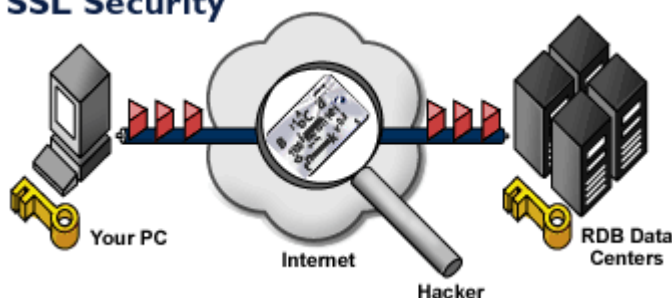
Digital certificates encrypt your backup data in transit using Secure Socket Layer (SSL) technology, the industry-standard for protecting Internet communications from hackers.

SSL negates packet sniffing

SSL encrypts each packet of data using complex digital keys by both your Internet Connection and our data centers.

Any data a hacker could possibly access appears as random, nonsensical characters, only decipherable by our servers which possess the digital key to decrypt, or unscramble, the data.

SSL Security



Without SSL, hackers can easily view your data transmitted through the Internet essentially as plain text.

Any sensitive information such as credit card numbers, contacts, etc., could easily be stolen or compromised.



Did You Know...

NIST (National Institute of Standards and Technology) determined that 128-bit AES is secure enough to protect U.S. Government classified information up to the TOP SECRET level.

AES is the government *and* commercial standard for encrypting sensitive digital information, including financial and telecommunications data.

Conclusion

With the new regulations, the roles and values of Remote Data Backups have expanded. The primary functions of these solutions are to provide disaster recovery and business continuity as part of a comprehensive data protection strategy. These functions, as well as privacy and security safeguards, are now an important component of a Compliant Records Management program.

However, the regulations also require fast recovery of specific data for compliance audits and litigation. Digital archiving of electronic records for audits and litigation requests helps enterprises subject to the regulations reviewed previously. By using the information in this white paper, enterprises can avoid the risk of noncompliance by employing the protections afforded by Remote Data Backups to meet audit and litigation requests for specific records. Remote Data Backups services support enterprises in their efforts to become compliant corporate citizens.

For more information on how Remote Data Backups can help you comply with various regulations, please visit our website, call or email us today.