WHITE PAPER

Meeting the Requirements for

Compliant Data Storage

&

Best Practices for Business Continuity

With

PoINT ARCHIVER VERSION 2.0

Prepared by Euroson America Inc
June 2007

TABLE OF CONTENTS

1. INTRODUCTION AND CONCEPT

Data availability and authenticity are critical tasks with major impact on the economic success of today's business organizations. Rapid recoveries after a system failure and data authentication are essential components to ensure business continuity. Within this scope, the responsible management must be able to reduce the risk of liability by choosing appropriate solutions. The growing volume of data requires solutions which can reduce storage costs at the same time.

Throughout the numerous statutes and regulations that have promulgated electronic record legislation there is a common set of foundational requirements regarding the use and acceptance of electronic records

- The records must be authentic and there should be proof that they are what they purport to be.
- The integrity of the records must be protected from alteration or deletion for as long as the records are retained.
- Records may not be distributed, copied or viewed without proper consent.
- The records must be readily accessible when required.
- When retrieved, the records must be capable of being processed (by available hardware and software) and reproduced in a format that can be read by a person.

In selected regulations, and in all Best Practices related to electronic records storage, a duplicate "recovery" copy of the original electronic record is often required and in specific cases it must be kept at a separate geographical location. In accordance with good recordkeeping practices, an increasing number of laws and regulations require an audit trail (i.e., the process and management evidence) be produced and retained as a means of tracking any possible alterations to, or unauthorized distributions of, the record as well as other events such as the migration of the record. (i.e., the transfer of records from one media to another)

Best Practice policies require Data storage systems which provide these capabilities;

- Physical and logical security over information systems, processes, and communications
- Monitoring, auditing, and reporting
- Business continuity & disaster recovery
- Encryption
- Access and restriction controls

Organizations need to re-evaluate their current policies and practices for meeting these compliance and best practices requirements. In addition, companies also need to implement long-term data protection strategies that integrate with their existing infrastructure, create minimal disruption to organization and workflow, and integrate standardized devices and file systems.

2. POINT ARCHIVER PRODUCT DESCRIPTION

PoINT Archiver 2.0 is a Windows server application for centralized administration of the complete data archival process. Using an intuitive user interface, PoINT Archiver provides a secure, cost effective, network-wide process of Filter Based Data Archiving. Two types of Archive Jobs can be created; Standard Archives and Tiered Archives, using PoINT's "Tiered Archive File System".

Additional modules provide Retrieval, Data Protection, and Authentication features. Retrieval allows selected archive data to be restored to its original location, or to a new location. Data Protection applies encryption of Archive Volumes, which prevents unauthorized access. Data Authentication monitors Archive Volumes for changes and alterations to data, and creates a series of reports to assure the accuracy and authenticity of data. With PoINT Archiver, virtually every compliance and business continuity issue can be addressed and satisfied.

FILTER BASED DATA ARCHIVING

PoINT Archiver has an intuitive user interface to create Archive Jobs, which are configured to "Monitor" specified folders. Monitored folders can be locally attached devices as well as any accessible network share. According to user defined Conditions (time, size, age, attributes), files contained within these monitored folders are either copied or moved into Archive Volumes. Archiver can store the Archive Volumes on multiple Devices, in multiple locations. These Devices can be "On Line" magnetic storage such as a NAS hard disk, or "Off Line" optical media which are produced using automated CD/DVD/BD disc production systems. Secondary storage devices such as optical and tape libraries may also be used as Archive Volume storage Devices. (Additional Library management software is required)

Data Retrieval, Data Protection and Data Authentication modules provide all of the necessary features for retrieval, access control and protection of the archived data. With Archiver 2.0, the user has a wide assortment of options to define the level of data security. An audit trail of all files archived is provided by detailed logging and messaging. For additional security, multiple discs may be produced automatically, and several CD/DVD/BD disc production systems can be used in parallel. A database of all archived files is presented in an Explorer like view where individual files, directories and the entire Archive Job can be searched and retrieved as needed. Files can be retrieved to their original location, or to a new location.

STANDARD ARCHIVE - Automated collection of data from Network shares

Standard Archive Jobs are configured to monitor local and/or network directories. Based upon user defined Conditions such as time/date, size, attributes or access date, The PoINT Archiver Agent periodically monitors folders and copies or moves files and folders to be archived into a specified Archive Volume, which is stored on the specified Archive Device(s). Additional filters provide inclusion or exclusion of files by name and type. In configurations where files are copied and therefore not deleted from the original folder, configurable criteria can be defined (e. g. date, archive bit, file contents) to identify and archive different versions of the same named file.

The Archive Volume may be written to optical media using a CD/DVD/BD disc production system for off-line and off sight storage as well as to any UNC accessible storage device. Optionally, archive media may be encrypted using the PoINT Secure File System to prevent unauthorized access to sensitive information. Archive Volume storage devices range from a simple hard disk, NAS or SAN to a mirrored volume set in an optical library.

TIERED ARCHIVE - Automated migration of data from folders located on the Archiver Server

Tiered Archives specifically monitor folders and files located on storage devices locally attached to the PoINT Archiver Server. In addition to most of the features of a Standard Archive, PoINT's *Tiered Archive File System* provides additional functions such as attribute management of the monitored folders, migration of data by age and/or file size and transparent read access to the Archive Volumes.

The PoINT *Tiered Archive File System* (TAFS) is applied to the monitored folders and provides specified settings for attribute management of files within these directories, allowing new or existing data shares to be secured as Write Once compliant volumes. Files which are copied into Archive Volumes located on secondary storage devices can be replaced by links at their original location, allowing transparent read access to the archived data via the file system. The result is a reduction in used storage capacity on the server and the minimization of backup and recovery times. Significant savings can be achieved without changing existing applications or workflows.

The PoINT *Tiered Archive File System* provides a storage hierarchy which permits the use of a variety of storage devices to provide a solution which overcomes the limitations of any individual technology. The user has a wide assortment of options to define the level of security and select the combination of hardware and technologies used. The possible configurations of Archive Volume storage devices vary from a simple USB hard disk to a mirrored volume set in an optical library. For compliance and long term retention an additional replication copy can be produced using a CD/DVD/BD disc production system. Archive Volume contents are written to optical media using a standard UDF file system to assure that they may be read on any system worldwide. Optionally, archive media may be encrypted using the PoINT Secure File System to provide access security.

The replication to an additional file system and to optical media improves the data reliability and availability. The selection of archive-storage device hardware depends on the individual requirements. These features provide benefits such as additional security and compliance, redundancy and disaster recovery, and automated file server consolidation.

OPTIONAL MODULES

PoINT Archiver offers numerous options to provide additional features for automation of the data retrieval process and to provide additional levels of data security and authenticity.

Retrieval Module for restoring data in Archive Volumes

PoINT Archiver displays the structure of the archived data in a “Directory Tree” view similar to the Windows Explorer. The file information (e. g. name, size, date of preparation) along with the name of the corresponding archive medium or image can be queried for each stored file version. During retrieval from optical media of any file, directory or a complete archive volume, PoINT Archiver generates a list of all required media and prompts the user to insert these into the disc production system. Only the requested files are then automatically copied into the selected target directory. Retrieval from on line Volumes (on NAS or in an optical library) is completely transparent with no additional user intervention.

Data Protection Module for Access control

An optional Data Protection module uses encryption which further protects the entire contents of the Archive Volumes, preventing unauthorized access to archived data. The combination of a system key and different archive keys makes the files illegible outside of the specific PoINT Archiver installation. The PoINT Secure File System secures data written to any Archive Volume and when used with disc publishing systems combines the advantages of removable media with the security of closed systems.

Authentication Module for Data security

In order to recognize possible manipulation of the archived data, digital fingerprints of the files and of the complete medium are encoded and stored on the media itself and also in the database. Thus any individual archive medium can be examined for consistency and compared with the database records. Additionally the files in the origin folder can be compared with the database or with the archived files. Documents which have been deleted or changed are identified and reported to the administrator.

POINT ARCHIVER HIGHLIGHTS

- Network wide filter based file archiving
- Tiered Archive File System ‘PoINT TAFS‘
- File versioning
- Database-driven file browsing
- Standardized UDF or PoINT Secure File System
- Monitoring and long term availability for archived data
- Utilization of standard hardware
- Parallel use of multiple CD/DVD/BD disc production systems

SUPPORTED DEVICES AND OPERATING SYSTEMS

Euroson America Inc. believes the information in this section to be accurate as of its publication date. Such information is subject to change without notice.

Supported Archive and Replication-Devices

Hard Disks (File System)
Jukeboxes: CD/DVD/BD, MO/UDO. (PoINT Jukebox Manager license required)
CD/DVD/BD Disc production systems; (LSK, Primera, Rimage)

The list of supported devices is extended on a continuous basis.

Supported Server operating systems

Windows 2000
Windows XP Professional
Windows 2003 Server
Windows Vista

More information on supported devices and specific requirements for drive and server configurations is available at www.point.de.

GLOSSARY OF TERMS

Archive Job ; An Administrator process to identify monitored folders and define filters for files in order to initiate the migration of data contained within the monitored folders into Archive Volumes.

Archive Volume; UDF image file(s) containing the content of an Archive Job, written to a storage device and/or on to a physical optical disc.

Archive Job Trigger; A condition which results in the filtered contents of monitored folders to be written to an Archive Volume

Filter Based Data Archiving; The process of creating multiple Archive Jobs for the purpose of managing the data archival process throughout a network.

Tiered Archive File System; Storage Management of, and file system access to, the Archive Volumes which may be distributed across multiple devices and storage technologies.

3. MEETING THE REQUIREMENTS FOR COMPLIANT DATA STORAGE WITH POINT ARCHIVER

PoINT Archiver provides a process for meeting all of the numerous statutes regulations and requirements regarding the use and acceptance of electronic records

- The records must be authentic and there should be proof that they are what they purport to be.

PoINT Archiver allows files and folders stored on hard disc to be controlled as WORM volumes. It also migrates files to optical media or optical disc images which further assures the accuracy of the information. Detailed logging of Archive Jobs documents the origin of the file, and the optional Authentication module provides the highest possible level of data authentication.

- The integrity of the records must be protected from alteration or deletion for as long as the records are retained.

PoINT Archiver allows the user to define the storage devices necessary for long term retention. Optical media provides the best long term retention/authentication model due to its inherent Write Once properties. Archiver provides the functionality to produce Write Once optical media using both Off Line (CD/DVD/BD disc production system) and On Line (Library) storage devices.

- Records may not be distributed, copied or viewed without proper consent

PoINT Archiver works with the sharing and permissions mechanism of the Windows operating system, so access control is secure. Archiver has an optional Data Protection module which uses encryption to control access to data written to Archive Volumes, whether located on hard disc or removable optical media. With Data Protection, these Archive Volumes cannot be read outside of the specific Archiver installation, preventing unauthorized access.

- The records must be readily accessible when required.

PoINT Archiver allows the Administrator to define and use multiple storage devices, and to manage the retention periods for the Archive Volumes individually, so that data is available as long as required. Data which has been written to off line optical discs can be easily retrieved using a database driven inquiry. With the available Retrieval Module, individual files, folders and complete Archive Jobs can be automatically restored using the CD/DVD/BD disc production system.

- When retrieved, the records must be capable of being processed (by available hardware and software) and reproduced in a format that can be read by a person.

PoINT Archiver stores and represents all file contents in their native formats. Data which has been migrated to optical media is written using the Universal Disc Format (UDF), assuring it can be read on any authorized system world wide.

4. MEETING THE REQUIREMENTS AND BEST PRACTICES FOR BUSINESS CONTINUITY

- Provide Physical and logical security over information systems

PoINT Archiver allows the use of multiple storage devices while providing the Administrator with secure control of the logical display of the data contents. Data stored in multiple locations can be represented as a single logical file structure.

- Monitoring, auditing, and reporting

PoINT Archiver maintains detailed log files of all data migrations including file information, time and date. The Authentication module extends the reporting to include recognition of any possible manipulation of the archived data.

- Business continuity & disaster recovery

PoINT Archiver uses multiple storage devices and technologies in order to allow the Administrator to specify which is most appropriate, based upon retention and access requirements. These devices can be located in multiple locations so that physical copies of records are retained, and can be easily restored in case of catastrophic events.

- Encryption

PoINT Archiver offers a Data Protection module which uses encryption to control access to information stored in Archive Volumes independent of the media or device used. Individual files within encrypted Archive Volumes are not visible by connection to their storage device and cannot be accessed outside of the specified Archiver installation.

- Access and restriction controls

PoINT Archiver works with the sharing and permissions mechanism of the Windows operating system, so access control is secure. It also monitors specific folders and secures their contents with a Write Once file system. The storage of individual data files within Archive Volumes limits access to these data files to users with permissions to the Archiver installation.

5. SUMMARY AND CONCLUSIONS

Data availability and authenticity are critical tasks with major impact on the economic success of today's business organizations. Numerous Compliance regulations as well as Best Practice procedures create a common set of foundational requirements regarding the use and acceptance of electronic records.

PoINT Archiver 2.0 is a Windows server application for centralized administration of the complete data archival process. Archiver provides an integrated, flexible solution allowing the user to specify the appropriate devices to meet any of these Compliance and Best Practice requirements.

Using multiple devices and technologies in multiple physical locations, PoINT Archiver uniquely solves this complex set of requirements from a centralized Administrative console, using a Network-wide process of Filter Based Data Archiving