California Code of Regulations

Trustworthy Electronic Document or Record Preservation: sections 22620.1-8

July 4, 2017

Overview

The Secretary of State of California has proposed to add sections 22620.1 through 22620.8 to Chapter 15 of Division 7 of Title 2 of the California Code of Regulations. These regulations create uniform statewide standards established by the American National Standards Institute (ANSI) or the Association for Information and Image Management (AIIM) for the purpose of storing and recording permanent and nonpermanent records in electronic media. This document describes how DataTrust Solutions' Secure Archive Manager helps organizations meet the proposed regulations.

Regulations

Sections 22620.1 through 22620.8 indicate that electronic content management systems shall be designed in accordance with the following:

- section 6.2 Recommended Project Steps and Activities of AIIM ARP1-2009
- section 6.17 Business practices documentation of AIIM ARP1-2009
- use of compression technologies specified in section 5.4.2.4. Document image compression of AIIM ARP1-2009
- creation of two copies of each document as identified in section 5.3.3 Trusted system and legal considerations of AIIM ARP1-2009
- section 5.4.1.4 Image formats of AIIM ARP1-2009

The follow section discusses the relevant sections of AIIM and related features of InfiniVault.

AIIM ARP1-2009 Compliance

Section 6.2 Recommended Project Steps and Activities

This section describes a framework for planning of a project to implement EDMS technologies. This section does not apply to the storage equipment used for the document management system.

Section 6.17 Business practices documentation

This section recommends that an organization prepare a document describing business practices and policies. While this does not inherent apply to the digital storage system, it is helpful to keep in mind that Secure Archive Manager provides the following features relevant to records management:

- compatibility with most document management applications
- content indexing
- industry-standard security model to prevent unauthorized access, including Active Directory integration
- immutable storage to prevent tampering
- audit trail for each file under management
- retention management based on policy

Section 5.4.2.4. Document image compression

Secure Archive Manager provides LZW compression, as specified in this section.

Section 5.3.3 Trusted system and legal considerations

This section describes the following requirements that apply to the digital storage system:

- Two copies of each document – Secure Archive Manager can automatically create multiple copies of each file, based on a configurable policy. The copies can be written to different storage locations and to different storage technologies.
- Prevent unauthorized modification – First, Secure Archive Manger prevents unauthorized users from accessing data it manages. Second, Secure Archive manager encrypts every file with a unique encryption key, thus the file cannot be opened or modified without the encryption key. Third, Secure Archive Manager uses content based cryptographic hashes to create a digital fingerprint of each file and this can be used to verify the contents of a file were not modified. Forth, Secure Archive Manger can enforce WORM (write-once-read-many) or retention for a specified period of time, preventing any modification. Fifth, Secure Archive Manager audits every user action and generates alerts if a user is attempting to modify content in WORM mode or under retention.
- Audit processes to verify immutability – Secure Archive Manger uses content based cryptographic hashes to creates a digital signature for each file under management. Secure Archive Manager supports MD5, SHA-1 and SHA-256 content based cryptographic hash options. Secure Archive Manger provides file write verification. When a file is written to Secure Archive Manager lands in a cache, where the file is hashed. Then the file or object is committed to the permanent storage location. After the commit process is complete Secure Archive Manager reads the file and re-hashes it to verify it matches the previous hash and then records this info in an audit log. This process confirms that the file was correctly written to the primary storage location and additional storage locations too. Secure Archive manager also has a periodic audit process using hashes that runs in the background and checks the integrity of files. If a checked file hash does not match the original file then the file is corrupt and this is logged in an audit trail. In systems with more than one copy Secure Archive Manger will copy back the file to the original file location. Optional Read Verification prevents retrieval of any file that has been altered or become corrupt. If the calculated and saved digital fingerprints do not match then this event is logged in an audit trail. The identification of any user who has accessed the file is also logged.
- One copy must be written to immutable media; this copy must be taken offsite – Secure Archive Manger can write multiple copies of each file in an immutable format to one or more storage locations. One or more copies can be written offsite to another Secure Archive Manger system or to a Cloud or Object storage system with WORM storage.
- Storage medium must be considered appropriate for evidence – The WORM format on electronic media is trusted by many law enforcement organizations and administrative oversite organizations such as the Securities and Exchange Commission to retain electronic evidence. An

additional layer of verification is provided by using the content based cryptographic hashes. The use of individual encryption keys for each file provides for iron clad verification.

- Retention policy – Secure Archive Manager provides Policy based retention management of all content. The Policies are preconfigured and specified by the archive administrator. Secure Archive Manger will not allow any files under retention to be modified or deleted by any user or system administrator. If desired a Policy can be specified for each archive that at the end of a retention period to automatic delete the files.

Section 5.4.1.4 Image formats

Secure Archive Manager is compatible with any file format for electronic storage.

Conclusion

By meeting all the requirements for electronic storage of documents, Secure Archive Manager helps government organizations to comply with sections 22620.1 through 22620.8 to Chapter 15 of Division 7 of Title 2 of the California Code of Regulations.