



# ASSUREON<sup>TM</sup>

## Electronic Discovery & Assureon

### Compliance by Nexsan

#### Cost of Electronic Discovery

Electronic Discovery can easily cost a corporation hundreds of thousands of dollars. Traditionally, corporate attorneys have advised their clients to maintain business records for lengthy periods of time. Their position was that the documents might be needed in case of a litigation or government investigation. As a result, most companies elected to keep rather than destroy business records.

#### Less May be Best

In the past decade the amount of litigation has grown at a substantial rate. With the changes and the relaxation of pre-trial discovery rules, records are frequently subpoenaed during litigation and used to the advantage of the opposing party. Very often a plaintiff's attorneys request appears to be a fishing expedition looking for a "smoking gun" amongst the millions of documents, emails, and reports accumulated over a period of years. The very documents that the attorney recommended saving are now causing companies to pay thousands of dollars to find and turn over to the plaintiff. These documents may also contain evidence that will be detrimental in court. Many of these records would not have been available if they had been destroyed under a records retention program.

#### Laws & Judgments

Rule 26, General Provisions Governing Discovery: Duty of Disclosure, states in relevant part that all parties in litigation must disclose "a copy of, or description by category and location of, all documents, data compilations, and tangible things in possession, custody, or control of the party that are relevant to disputed facts alleged with particularity in the pleadings." In the case of *Armstrong v. Executive Office of the President*, 821 F. Supp. 761,773 (D.D.C. 1993), the court ordered the restoration of backup tapes.

#### Integrated Retention Management System

In order to minimize a risk of electronic discovery, a company needs to establish retention policies based on industry, federal, state and local laws. Equally important is a systematic process that manages, authenticates and disposes of the records based on the company's retention policies.

Assureon has an integrated retention management system which allows a company to apply their retention policies to any document within their organization. Assureon can also be used with an existing document or email management system.

Procedures must also be provided for the suspension of records destruction in case of foreseeable pending, or actual, litigation or government investigation. If not, the company could be liable for obstruction of justice, or contempt of court.

# Disposition is Critical to an Effective Record Retention System

## Suspend Disposition

---

Assureon has the ability to place "On hold" any deletion. The disposition process requires a conscious action on the part of the administrator. At the end of their retention period, the files are automatically presented to the administrator in order to confirm their deletion.

Problem #1: IT departments have faithfully implemented backup solutions in order to protect data. It is not uncommon for a document to be stored multiple times on different media in different (often offsite) locations. How does one locate all copies of a specific document when it is time to dispose of it?

## Historical Problems

---

Problem #2: Record retention policies dictate different retention periods for different documents based on the document type, industry, and regulation. Long term storage typically uses tape or magnetic optical media for its cost benefits and WORM media for compliance reasons. The only way to delete a specific record is to destroy the entire disc or tape. This solution is not feasible, as the tape or disc may have a variety of documents on them with different retention periods.

## Disposition at the File Level on Disk, Tape, Optical, DVD or WORM Media

Assureon addresses both problems. When setting up retention policies a file can optionally be encrypted. Assureon uses encryption as a means to dispose of files and to keep their content secure. Each file is encrypted with a unique encryption key. When a file is no longer needed and has past its predefined retention period, the key is removed from the system. By destroying the key, the contents of the file become unusable and are effectively destroyed; the file is "virtually deleted". All copies of the file, whether off line and/or on tape, optical media or in an offsite location, are also unreadable. Assureon takes care of key management (safeguarding the cryptographic keys) and if the file is physically accessible, the scrubbing of the file.

Assureon uses the Advanced Encryption Standard (AES) with 256 bit keys, which is currently unbreakable, guaranteeing the non-readability of the disposed records once the keys are scrubbed.



This brochure is not a legal opinion or intended to be legal advice.  
Please seek legal counsel for questions on compliance.

© 2006 Nexsan Technologies Inc. All rights reserved.  
Tel: USA 886 4 NEXSAN (International) Tel: +1 818 715 9111  
E-Mail: [sales@nexsan.com](mailto:sales@nexsan.com) or visit our Web site: [www.nexsan.com](http://www.nexsan.com)