



APPLIED INFORMATION SCIENCES



Military Grade Compliance for SharePoint 2007

JANUARY 30, 2007

BY APPLIED INFORMATION SCIENCES STAFF



TABLE OF CONTENTS

WHAT IS A RECORDS CENTER? 4

ADDITIONAL FUNCTIONALITY WHICH SUPPORTS DOD 5015 5

 Content Types and Routing 6

 New Content Type Features Which Support DoD 5015..... 7

E-mail Message Records Management 8

 Additional DoD 5015 E-mail Message Records Management Features..... 8

Setting Policies 8

 Additional Policies Features Which Support Compliance With DoD 5015..... 8

Holds..... 11

 Additional Hold Features Which Support Compliance With DoD 5015 12

APPENDECIES 14

APPENDIX A: ELEMENTS OF A RECORDS MANAGEMENT SYSTEM 15

APPENDIX B: ADDRESSING COMPLIANCE WITH RECORDS MANAGEMENT 17

 Sarbanes-Oxley Act..... 17

 Sarbanes-Oxley Has Global Implications..... 18

 Financial Services..... 18

 GLBA..... 18

 Basel II 18

 SEC and NASD Regulations..... 19

 Healthcare and Life Sciences 19

 HIPPA..... 20

 21 CFR Part 11 20

 Government 21

WHO WE ARE 22

Recent regulatory requirements, such as the Sarbanes-Oxley Act of 2002, make the proper management of official company information both a business priority and a legal obligation that demands the attention of executives and corporate board members. Organizations lacking effective policies and procedures for controlling recorded information risk extensive penalties for non-compliance, a tarnished reputation and possible legal liability.

Regulatory compliance requires companies and organizations to securely manage records for long periods of time in a safe and unalterable state. The appropriate archival of documents is just one component of a larger records management process that also includes the collection, management, and expiration of corporate records (information important for the history, knowledge, or legal defense of a company or organization) in a consistent and uniform manner in accordance with a company's corporate governance policies.

In the past, Microsoft customers using SharePoint Server needed to invest in third-party applications that would allow them to transfer documents out of SharePoint into a separate records-management repository. As a result, Microsoft has introduced a new set of features in Microsoft Office SharePoint Server 2007 (MOSS 2007) for creating and supporting formal records management capabilities: the Records Center.

The addition of the Records Center enables MOSS 2007 to provide these records management capabilities; however some customers - including government organizations - require a records management solution that also includes compliance with the DoD 5015.2 Standard (DoD 5015).

The DoD 5015 is a well-known and widely-adopted industry standard for records management applications in the enterprise content management (ECM) industry. The standard offers guidelines for how records and permissions should be managed, automating the periodic review of vital records, managing e-mail as records, and being able to support multi-phase lifecycle management for documents that require more-complex retention rules. DoD 5015 sets the bar for companies and other organizations in highly-regulated industries when they are choosing a records management solution.

Microsoft selected Applied Information Sciences, Inc. (AIS), a Microsoft Gold Certified Partner, to help develop and extend the records management capabilities of Microsoft Office SharePoint Server 2007 to include the DoD 5015 records management compliance functionality.

The joint Microsoft/AIS-developed additional Records Center capabilities will provide the additional DoD 5015 required functionality to comply with and to complete the certification test against the standard. It will enable customers to collaborate on documents and then manage them within the SharePoint environment to make them official records using a DoD 5015 certified solution.

1. By extending SharePoint 2007 with the additional DoD 5015 records management functionality, customers will realize three key advantages:
2. They will be able to manage their business records effectively without having to make significant additional investments in third-party software;
3. People already familiar with the SharePoint user experience will not have to leave this easy-to-use interface to work with a separate application for managing records;
4. They will be able to manage documents as official business records with military-grade functionality, while taking advantage of SharePoint features such as searching, alerts, collaborative online discussions, and collaboration on new versions of records.

WHAT IS A RECORDS CENTER?

The Records Center SharePoint site template includes the Records Center Web Service and other features which get installed in this special SharePoint Site. The Records Center becomes the hub for all records management processes, including content collection, consistent policy enforcement, item retention management and holds in response to external events, and content expiration. The Records Center site includes the following features:

Enhanced Security: The Records Center site provides several features that help ensure the integrity of the document libraries. Records stored in this site are never automatically modified by the system and records managers can add and maintain metadata on items separately from the record's metadata. This way information can be changed without modifying the underlying record, and these changes can also be audited.

Information Management Policies: Policies provide consistent uniform labeling, auditing, and expiration of records. Policies can be defined for a specific storage location or content type.

Records Collection Interface: The Records Center site provides a set of services that aid in content collection for people and automated systems to easily submit content to a records repository without necessarily having access or permission to any of the contents of the site. The new version of Windows SharePoint Services and Microsoft Exchange Server 2007 provide out-of-the-box functionality to work with these interfaces to send documents to a Records Center site.

Records Routing: When content is submitted to a Records Center site, it can be routed to its proper library based on the corresponding content type. (More about content types shortly)

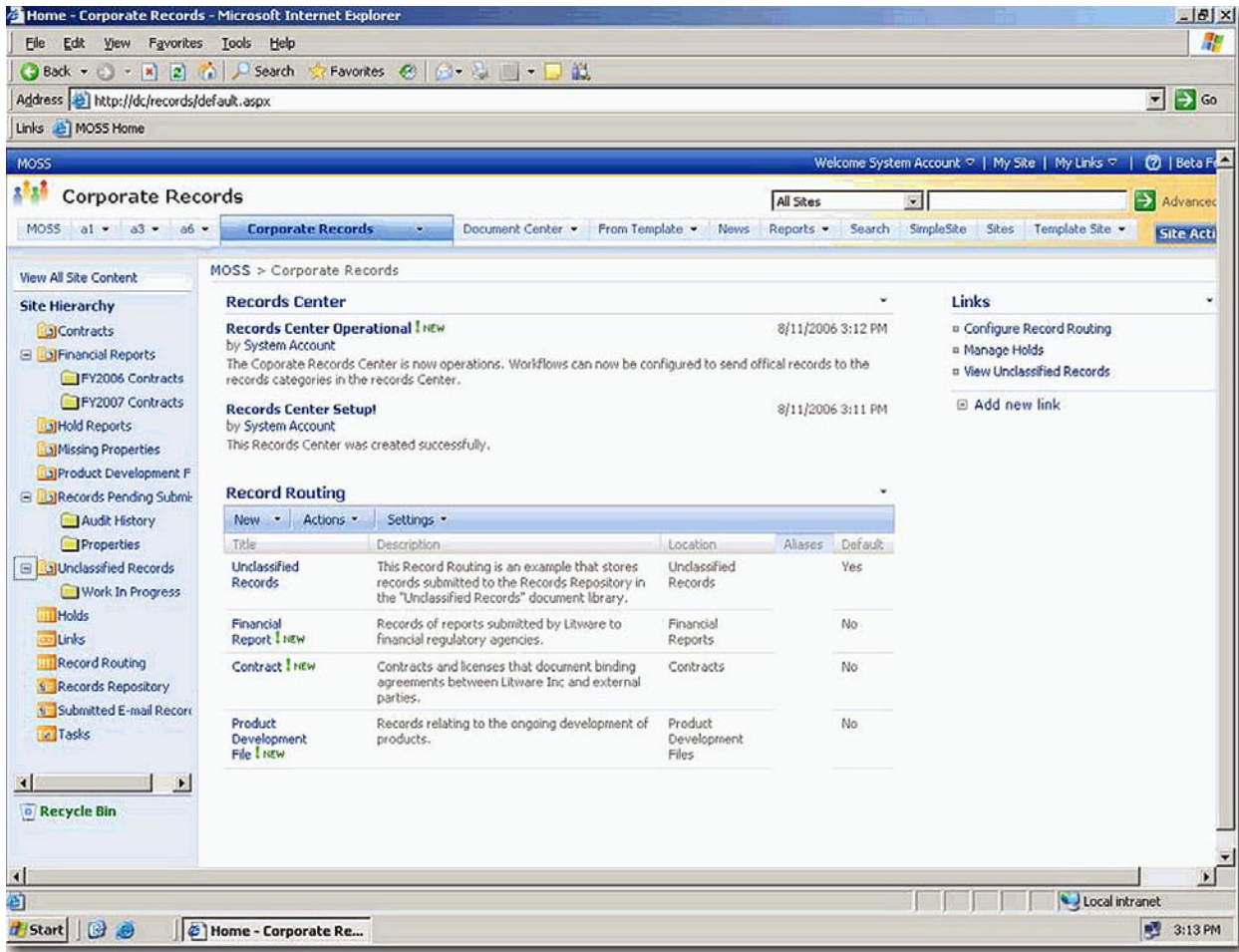


Figure 1: The figure above is what the standard Records Center Site looks like

ADDITIONAL FUNCTIONALITY WHICH SUPPORTS DOD 5015

The additional Records Center capabilities provided by Microsoft include:

File Plan Builder: This feature provides the Records Manager with an updated user interface for configuring a file plan in a DoD compliant SharePoint Records Center. This new user interface supports creating record categories and other file plan-related constructs, like SharePoint folders, which can be closed to new records and can also have their own retention and disposition rules.

Preconfigured DoD Data Structures: New content types, lists, and other data structures are being provided as new features which can be enabled in the Records Center to provide compliance with the DoD 5015. These data structures and lists provide the infrastructure for many of the additional functional capabilities including multiple-phased lifecycle disposition rules and event-based retention calculations.

Metadata Propagation between Categories, Folders, and Records: This feature addresses the propagation of metadata values between categories, folders, and records. Metadata is stored in three separate wells: metadata about categories, metadata about folders within those categories, and metadata about records within those folders. Each well has a separate schema with defined columns. Under some circumstances, metadata needs to be propagated between those wells to ensure consistent processing and lifecycle management of the records managed in the Records Center.

Closing Record Folders: This capability specifically addresses closing a Record Folder within the Records Center so that users no longer can file or add additional records into the closed folder. Users can still view records of closed Folders and policies are still enforced on closed Folders. There is no concept of closing a SharePoint folder in baseline MOSS 2007, so this capability provides new functionality within SharePoint.

CONTENT TYPES AND ROUTING

One of the biggest difficulties in managing content in a large organization is making sure that everyone understands and follows corporate policies, such as managing out-of-date information or requiring labels so that paper copies can be traced back to electronic originals. Office SharePoint Server 2007 supports robust information management policies that let site administrators and list managers control how content is managed. Although this section focuses on document management policies, all of the Office SharePoint Server 2007 policies can be applied to other types of content, such as pictures, list items, and third-party items.

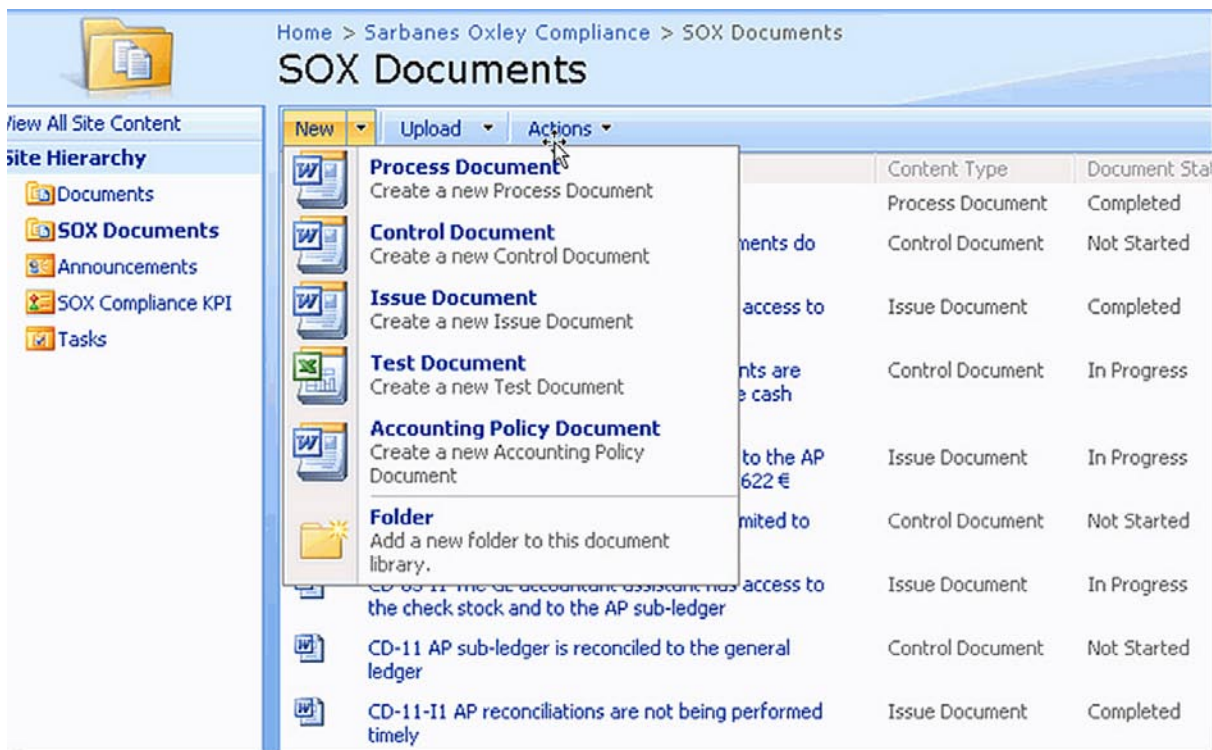



Figure 2: Example Content Types



Content Types, a new addition to Windows SharePoint Services 2007, allows predefined metadata boilerplates so that all newly-created documents automatically have appropriate metadata such as workflow, resulting actions, expiration, and other policies. Content Types address a significant obstacle to automating better compliance: the lack of information classification. If the system regards all content as plain “documents,” then the system can’t enforce policies such as expiration according to the type of content. For example, with the addition of Content Types, Office SharePoint Server 2007 can tell the difference between “contracts” and “memos” and automatically enforce different policies according to those content types.

Content Types are created by the administrator and specify a template that can be used from the document library, as shown in the graphic example in figure 2 on page 5.

When a user clicks New in a document library to create a new file, they can now select a Content Type. Based on the selected Content Type, metadata properties are automatically generated within the new document. For example, if you wanted to create a Sales Proposal, you could select a pre-made Proposal Content Type that captures a sales proposal’s relevant attributes (such as the customer, product type, and salesperson).

Additionally, ensuring metadata inclusion at the time of document creation by using Content Types creates the ability to find documents much easier. For example, if you wanted to review other Sales Proposals, you could easily search and retrieve all Proposals associated with a specific product type, salesperson, or date.

Content submitted to a Records Center site can be routed to the proper location within the records management system based on Content Type. It is important to note that although users can submit content to a Records Center site, they may not have the permissions to view or modify all content because of viewing and security policies.

NEW CONTENT TYPE FEATURES WHICH SUPPORT DOD 5015

New standard Electronic Records and Non-electronic Records Content Types are installed as new features. These new Content Types not only provide a standard set of metadata for records but also provide built-in functionality and workflow to support common records management and compliance business processes. The following new Content Type features are added to the Records Center which support compliance with DoD 5015:

Referencing, Linking, and Renditions: This capability adds a Record Relationships metadata column to every record in a DoD compliant Records Center. Records can be linked to one another according to an administrator defined and managed relationship (e.g. Record A is a rendition of Record B). All links are reciprocal and are automatically updated as items are moved or deleted. A special case of a link relationship is also provided to define a record version which assigns a numeric value to each record version which is a version of the original record.

Enhanced Records Upload: This feature changes the upload experience for a DoD 5015 compliant system to automate some of the data population of the record properties. This relies on the metadata propagation feature mentioned on page 4. This way data which is inherited from the record category (document library) or the folder is pre-populated. Additionally this feature also provides the capability to upload non-electronic records.

Supplemental Markings: This capability addresses advanced access control logic required by the DoD 5015. Access is controlled based upon a record’s Folder metadata values, as well as a special field called the “supplemental markings” list. SharePoint’s prior version of administrator-defined per-item access control lists

(ACLs) has been replaced by examining the values of an item's metadata to dynamically generate a record's unique ACL.

More importantly, business users benefit from the related capability which allows users to be constrained from assigning a value to a metadata column if they do not have access or permissions to that property value. This feature will also limit the edit experience for records to enforce that constraint.

Vital Record Review: In some cases, certain company records are deemed vital and require regular or periodic review. Examples of vital records include "Continuity of Operations Plans", evacuation and severe weather plans, etc. The Vital Record Review capability provides the mechanism to define periodic review cycles for vital records. This new framework provides a way to track when records are due for review and then marking them with a "last reviewed date" during the periodic human-centric review/update process using workflow. The Vital Record Review workflow can be configured to notify the appropriate reviewers when it is time to review the vital records.

E-MAIL MESSAGE RECORDS MANAGEMENT

E-mail messages can be managed as records using the Records Center because of the enhanced integration between Office SharePoint Server 2007 and Exchange Server 2007. The Administrator creates managed e-mail folders in Exchange Server 2007. These special e-mail folders have defined policies that can be used in conjunction with Exchange Server 2007 rules so that these folders send e-mail messages to the Records Center. Users can drag e-mail records from their inbox into the appropriate managed e-mail folder and any required metadata can be entered asynchronously into the Records Center site.

Additional DoD 5015 E-mail Message Records Management Features

While the current Outlook, Exchange, and SharePoint integration provides a robust, unique, and fully-featured user experience for submitting email as records, there are other user scenarios that needed to be addressed to support DoD 5015 compliance. The additional capabilities offer users the choice to file email attachments as separate records or with the email itself, extracting email header information automatically and populating DoD required email record properties.

The user still drags email into the e-folders described above to initiate the process.


SETTING POLICIES

MOSS 2007 includes a set of out-of-the-box policies that can be used for a specific list or Content Type. These policies provide controls that consistently and uniformly enforce the labeling, auditing, and expiration of records. Policies can be configured for a specific storage location or Content Type. For example, to ensure that all company contracts are precise and up-to-date, expiration dates can be based upon contract execution dates.

Although the out-of-the-box policy features of Office SharePoint Server 2007 support many common policies, organizations can have unique needs that require additional policy features. For example, an organization might have a policy that requires files to be saved in a specific format. The policy framework allows organizations to author custom information management policies that will appear on the policy settings page.

Figure 3 on page 9 shows how easy it is to configure auditing and content expiration options.

Additional Policies Features Which Support Compliance With DoD 5015



One of the most significant new features is a new expiration policy framework which provides multi-phased lifecycle management that can be based on date properties, events which may occur in the future, and also can be marked as a permanent record. The following new DoD 5015 features are added to the Records Center:

Category and Folder Cut-off: The DoD 5015 requires the automated calculation of cutoff dates. (From DoD 5015: To cut off records in a file means to break, or end them at regular intervals to permit their disposal or transfer in complete blocks and, for correspondence files, to permit the establishment of new files.) The Cutoff date commences disposition processing on a record. For example, a records disposition policy may call for the record to be held five years after it is cutoff. Cutoff will be approved by a records manager. By using Cutoff as the common denominator for all record dispositions in a folder, Disposition can be batched and multiple records can go through the Disposition pipeline at the same time. Cutoff, like Disposition, requires approval as well. The new features include a process that facilitates management and approval of record Cutoff. Once the Cutoff workflow is approved, the Cutoff date property on the record Content Type is automatically set.

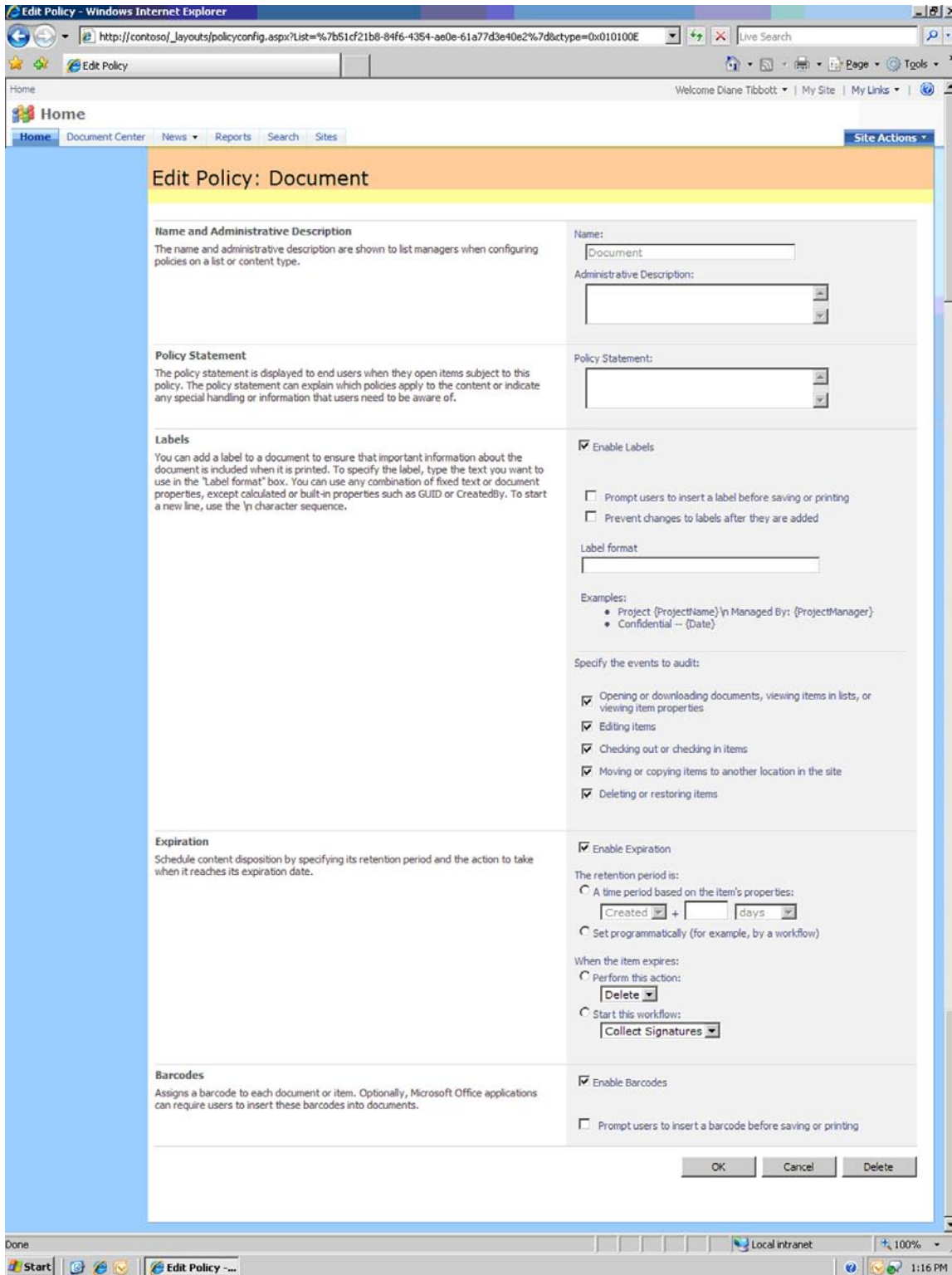


Figure 3: Standard MOSS 2007 Policies

Global Events and Periods: This capability addresses the management of global events and periods for controlling the lifecycle of records. Global events can trigger disposition actions or cutoffs. Unlike a date column on an item, global events are defined once per site but referenced by any record in that site. In addition, this same framework defines global time periods (e.g. the fiscal year) which are used for accurately computing the start of retention rule calculations.

Enhanced Disposition Processing: This new feature extends the existing SharePoint disposition framework to support the more comprehensive DoD 5015 needs. These features allow records managers to define and execute multi-cycle disposition actions. In addition, it allows Records Managers to transfer records and also to leave record metadata inside the repository when the binary content of a record are deleted.

The best way to show how flexible this framework must be is to provide an example. For instance, here is a “disposition instruction” on a record category taken directly from the DoD test cases:

Permanent. Cut off on completion of study, hold 5 years, then transfer by CY block to RHA. Accession to NARA in 5-year blocks 25 years after cutoff.

The enhanced expiration framework can enforce and manage the example rule above. The records manager is notified via e-mail; as the workflow manages the completion of one phase as well as the transition to the next phase of the lifecycle.

HOLDS

A number of compliance regulations mandate that organizations be able to produce records required by investigations and court discovery orders. Failure to fulfill such requests in a timely and complete fashion can expose the company and its officials to significant liability. Even the inadvertent destruction of records can create criminal liability issues.

MOSS 2007 includes a hold feature designed to manage the response to events which would require the suspension of the expiration policy for these affected records. The hold ensures that the records placed on hold cannot be deleted manually or automatically during the lifespan of the hold.

By default, every Records Center site is provisioned with a hold list in which each item corresponds to a single hold order. The list provides tools for finding and holding relevant records, viewing the records currently on a hold, and releasing the hold after the hold order is no longer active. When an event such as a discovery order occurs, a records manager defines a new hold by adding an item to the hold list. The item specifies a name for the hold event, a description, and the person responsible for managing the hold.

The next step is to suspend the expiration policies on all relevant records that may be scattered across different document types and stores. The search function of Office SharePoint Server 2007 makes it easy to find all relevant records thanks to integrated metadata capture and Content Types. The records manager then analyzes the search results and adds the new hold to the relevant records either one at a time or in bulk.

The following screenshot shows a hold in MOSS 2007 that identifies the matter under research and the user managing the hold.

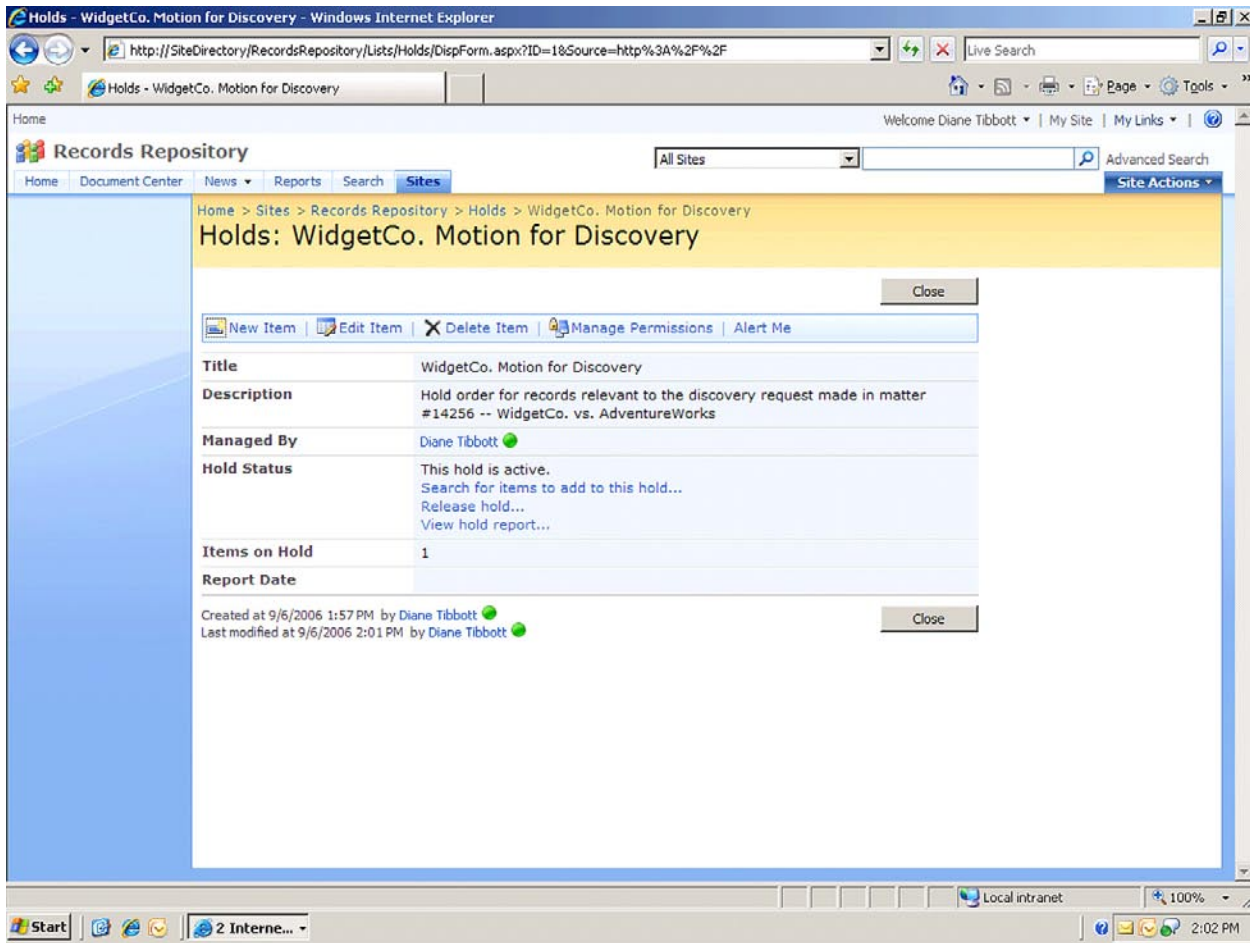



Figure 4: Example Hold Item

ADDITIONAL HOLD FEATURES WHICH SUPPORT COMPLIANCE WITH DOD 5015

The hold framework provided by the Records Center manages holds on individual records only. One of the DoD 5015 requirements includes the need to place a folder on hold and thereby automatically place all child records in the folder on hold. The current SharePoint Records Center concept of a record hold has been extended to an entire folder. When applied to a particular folder, a hold will trickle down to every record in that folder. In addition, any documents added to that folder after a hold is applied are also put on hold. A new folder hold report is also provided so that a list of folders currently placed on hold can be generated.

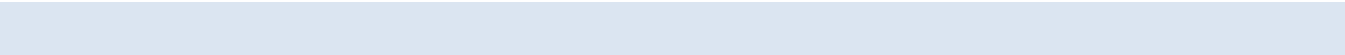
BUILDING BETTER BUSINESS SOLUTIONS

The broad range of new information management capabilities described above enables content that created and managed within SharePoint to be managed in ways that improve compliance and authenticity. By leveraging these new capabilities, companies and organizations can be assured that the SharePoint-based business application will manage the information in accordance with Federal, State, and Local Government regulations.



Additionally, with the enhanced content lifecycle management capabilities, content which should be destroyed is removed from the repository and content which should be maintained is preserved.

All these new capabilities combined, provide a compelling platform for building business applications which require the combination of both structured and unstructured content. We believe a new generation of business solutions based on Microsoft products and technologies are emerging to automate our service economy. With the release of Microsoft Office 2007, Microsoft Office SharePoint Server 2007, and .NET 3.0, Microsoft customers are able to create solutions which support their strategic information management initiatives. These solutions are built on an architectural framework that supports the goals of business flexibility and agility. We are pleased that we are working with Microsoft to make these new features a reality and will be eager to help our clients take advantage of these new capabilities when they become available to Microsoft customers.



APPENDECIES

APPENDIX A: ELEMENTS OF A RECORDS MANAGEMENT SYSTEM


A record is a document or other electronic or physical entity in an organization that serves as evidence of an activity or transaction performed by the organization and that requires preservation and retention for a period of time. Records management is the process by which an organization:

- Determines what types of information should be considered records.
- Determines how active documents that will become records should be handled while they are in use, and determines how they should be collected once they are declared to be records.
- Determines in what manner and for how long each record type should be retained to meet legal, business, or regulatory requirements.
- Researches and implements technological solutions and business processes to help ensure that the organization complies with its records management obligations in a cost-effective and non-intrusive way.
- Performs records-related tasks such as disposing of expired records, or locating and protecting records related to external events such as lawsuits.

Determining which documents and other physical or electronic items in your organization are records is the responsibility of corporate compliance officers, records managers, and lawyers. By carefully categorizing all enterprise content in your organization, they can help you ensure that documents are retained for the appropriate period of time. A well-designed records management system helps protect an organization legally, helps the organization demonstrate compliance with regulatory obligations, and increases organizational efficiency by promoting the disposition of out-of-date items that are no longer records.

A records management system includes the following elements:

- A content analysis overview that describes and categorizes content in the enterprise that may become records, provides source locations, and describes how the content will move to the records management application.
- A file plan that describes each type of record in the enterprise, where they should be retained as records, the policies that apply to them, how they need to be retained, how they should be disposed of, and who is responsible for managing them.
- A compliance requirements document defining the rules that the organization's IT systems must adhere to in order to ensure compliance, along with the methods used to ensure the participation of enterprise team members.
- A method for collecting records that are no longer active from all record sources, such as collaboration servers, file servers, and e-mail systems.
- A method for auditing records while they are active.
- A method for capturing records metadata and audit histories and retaining them.

- 
- A process for holding records (suspending their disposition) when events such as litigations occur.
 - A system for monitoring and reporting on the handling of records to ensure that employees are filing, accessing, and managing them according to defined policies and processes.

Microsoft Office SharePoint Server 2007 includes features that can help organizations implement integrated records management systems and processes. To ensure that information workers can easily participate in your enterprise's records management system, 2007 Microsoft Office system applications, such as Microsoft Office Outlook 2007 and Microsoft Office Word 2007, also include features that support records management practices.

APPENDIX B: ADDRESSING COMPLIANCE WITH RECORDS MANAGEMENT

Interest in company records management strategies and compliance-based solutions has grown as corporate scandals have rocked the public's faith in major corporations. The response - federal legislation such as the Sarbanes-Oxley Act - puts a new focus on corporate accountability. Also, governments all over the world are passing legislation to allow and even require the submission of electronic records to reduce paperwork, open up services to their citizens, and to improve the efficiency of internal processes. Examples of these increased regulations dealing with or requiring the management of content include:

- The Sarbanes-Oxley Act
- The Health Insurance Portability and Accountability Act (HIPPA)
- 21 CFR Part 11
- The Gramm-Leach-Bliley Act (GLBA)
- Basel II
- Securities and Exchange Commission (SEC) and National Association of Securities Dealers, Inc. (NASD) Regulations for Financial Services Customers
- Environmental Protection Agency (EPA) Regulations
- Wide Acceptance of the DoD 5015.2 STD

All publicly traded companies are currently, or will be shortly, subject to the requirements of the Sarbanes-Oxley Act of 2002 (SOX). The following section details some of the records management challenges specifically required by SOX.

SARBANES-OXLEY ACT

The Sarbanes-Oxley Act of 2002 (SOX) was passed into law by the US Congress in response to the Enron, MCI-WorldCom, Global Crossing, et al. corporate scandals that shook investor confidence in the integrity of the nation's public companies. This legislation is directed at publicly traded companies, public accounting firms, and the SEC. It calls for the creation of a Public Company Account Oversight Board with the goal of protecting investors by improving the accuracy and reliability of corporate disclosure required by current securities laws.

From a Records Management perspective several sections of the act specifically address the preservation and retention of certain records. For example, registered public accounting firms must prepare and maintain for a period of not less than seven years audit work papers and other information related to any audit report. Accountants who conduct an audit of a publicly traded company shall maintain all audit or review papers for a period of five years from the end of the fiscal year end that the audit or review was conducted. There are several other references to the preservation of corporate business, audit, and review documents throughout the act.

What is truly unique about SOX is that this piece of legislation has severe penalties for the failure to preserve those records mentioned in the Act. Furthermore, SOX amended Title 18 of US Code to include "destruction, alteration, or falsification of records in federal investigations and bankruptcy", which now makes these activities

obstructions of justice. These tampering provisions are not limited to publicly traded companies and public accounting firms, but to all businesses, public and private alike.

Boards of Directors and corporate managers will have to take SOX seriously since the changes to Title 18 also impose a fine and/or imprisonment of not more than 20 years for “whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence” an investigation or proceeding by a federal department or agency or any case filed in bankruptcy.

Sarbanes-Oxley Has Global Implications

Since SOX governs publicly traded firms, the rules apply only to publicly traded firms that list their stock on any US-based financial exchange. Companies that are not US-based firms but still have their stock traded in the US are still required to comply. Although private firms are not governed by SOX rules many experts expect private companies will eventually abide by the spirit, intent, and letter of the law.

FINANCIAL SERVICES

Financial services is also the term used to describe organizations that deal with the management of money. Banks, investment banks, insurance companies, credit card companies and stock brokerages, are examples of the types of firms comprising the industry, which provides a variety of money and investment related services. Financial services include securities, insurance, banking, and housing industries.

Several regulations govern the compliance and records management requirements for the financial services industry. The following provides a list of the most common compliance requirements.


GLBA

The Gramm-Leach-Bliley Act (GLBA) states that each financial institution “has an affirmative and continuing obligation to protect the privacy of its customers and the security and confidentiality of those customers’ non-public personal information (NPI).” NPI is any “personally identifiable financial information” that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise “publicly available.” Organizations failing to comply with the act face up to \$1 million in fines and could end up in prison. The details of the legislation are codified at 15 U.S.C. § 6801-6810.

Businesses most affected by GLBA are “financial institutions” – companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. The Federal Trade Commission (FTC) has authority to enforce the law with respect to “financial institutions” that are not covered by the federal banking agencies, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and state insurance authorities. Among the institutions that fall under FTC jurisdiction for purposes of the GLBA are non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors.

Basel II

The Basel II Capital Accord imposes strict and onerous capital requirements upon banks to support operational risk. The new Accord consists of three pillars: (1) minimum capital requirements, which seek to refine the standardized rules set forth in the 1988 Accord; (2) supervisory review of an institution’s internal assessment process and capital adequacy; (3) effective use of disclosure to strengthen market discipline as a complement to



supervisory efforts. Introduced in 2001, the Accord was scheduled for implementation in 2006 and is currently endorsed by 135 countries.

To comply with the tenets of the Accord, financial institutions which rely very heavily on information to make their decisions and mitigate credit risk will need to ensure that the information is delivered accurately and in real time. Accomplishing this goal of compliance with the Accord will have a profound effect on how information technology is delivered in all financial services sectors. There will be large competitive advantage for financial services firms that successfully change their IT infrastructure to comply with Basel II. Firms that fail to do so will operate at a significant competitive disadvantage.

Businesses most affected by Basel II are also “financial institutions” – companies that offer financial products or services to individuals, like loans, financial instruments, investment products, etc. Under the umbrella of “financial institutions” are included savings and loan banks, investment banks, commercial mortgage institutions, and some global investment firms.

SEC and NASD Regulations


The SEC has long mandated specific record keeping requirements. The SEC said as early as 1997 that emails should be kept, and issued a clarification of the rules in November 2001 explaining that emails relating to the firms’ business were subject to the same retention requirements as other books and records. Specifically, those regulations include Rule 17a-3 (Records to Be Made by Certain Exchange Members, Brokers and Dealers) which defines what records must be maintained, Rule 17a-4 (Records to Be Preserved by Certain Exchange Members, Brokers and Dealers) which defines how long and how those records must be kept, and NASD Conduct Rule 3010 and 3110 which outline specific records requirements for NASD members and the records of business with their customers. Now as recent as June 18, 2003, the NASD issued guidance on the retention and preservation handling of Instant Messages (IMs). Firms must now keep IMs for three years.

The penalty for not complying with SEC and NASD rules can be financially harsh. For instance, five securities firms have tentatively agreed to pay fines totaling \$8.3 million for allegedly failing to keep emails and to produce them in regulatory investigations. Each of the five firms will pay approximately \$1.65 million to settle the expected civil charges without admitting or denying wrongdoing. Another more spectacular example involves the major investment banks of Citigroup, Credit Suisse First Boston, Merrill Lynch, Morgan Stanley, and Goldman Sachs. SEC and NASD regulators looking into the supervision of analysts who were credited with contributing to the loss of millions of dollars by large and small investors alike are seeking email messages about analysts and their ratings on companies, as well as any evaluations of the analysts written by their superiors. The firms agreed in April to pay a total of \$1.4 billion to end investigations into whether their investment advice in the late 1990’s was tainted by their desire for investment banking fees. Here again the management, preservation, and retention of email records plays notably in the settlement of these charges and the large fines and settlement amounts.

The financial services sector, which includes investment banks, brokers, and dealers are most affected by SEC and NASD regulations. Global investment banks that trade on US exchanges and do business in the US are also subject to these regulations.

HEALTHCARE AND LIFE SCIENCES

The healthcare and life sciences industry is comprised of hospitals, clinicians, health insurers, and manufacturers of pharmaceuticals, biotechnology, and medical devices. Rising costs and increases in competition and



regulation have created unprecedented challenges across the entire spectrum of healthcare and life sciences organizations.

The challenges that people in these industries face include:

- Medical clinicians and administrators strive to deliver high-quality, cost efficient care. At the same time, they juggle demands on their time and attention from government regulators, health insurers, colleagues, and patients.
- Health plans are under unprecedented market pressures to improve the health of their members, improve quality of care and customer experience, and control rising medical costs.
- Life sciences companies—such as manufacturers of pharmaceuticals, biotechnology, and medical devices—are being pinched by higher research and development costs and more stringent regulations.
- In such hypercompetitive marketplaces, quick and effortless access to relevant information, people, and insights is a critical component of success.


HIPPA

The Health Insurance Portability & Accountability Act (HIPAA) regulations require all individually identifiable health care information be protected to ensure privacy and confidentiality when electronically stored, maintained, or transmitted. Further, HIPPA regulations require personal health information (PHI) be stored and handled (transmitted, printed, etc.) in a secure manner clearly stating that the organization must ensure the confidentiality, integrity and availability of protected health information and safeguard it from threats, hazards and unauthorized disclosure. Included are the requirements to secure the information from unauthorized access through user access control, audit logs of access to PHI, integrity controls to corroborate that PHI has not been altered, and to maintain documentation required by the regulations for six years from the date of its creation or the date when it last was in effect, whichever is later.

The penalties for violating HIPAA regulations range from \$100 per person per incident for run-of-the-mill improper disclosures of health information to \$250,000 and 10 years in prison for intentional violations. There is also a risk of class action lawsuits and, of course, damage to the organization's reputation.

21 CFR Part 11

The US Food and Drug Administration (FDA) regulation first introduced Part 11 of Title 21 of the Code of Federal Regulations (21 CFR Part 11) in August 1997, which contains “specific controls on the use of electronic records and includes strict administrative controls on electronic signatures.” A key feature of the regulation is that it makes electronic signatures as valid as handwritten signatures in the pharmaceutical industry. This regulation applies to all aspects of research, clinical activities, and the manufacturing and distribution of compounds, devices or software, including maintenance that is regulated by the FDA and covers aspects that may also be regulated by the Public Health Service, another division of the US Department of Health and Human Services. The far reaching implications of this regulation mean anything the FDA has jurisdiction over and some items within Public Health Services' purview is covered by the terms of Part 11. The FDA expects life sciences companies to identify all applications covered by the regulation, develop a plan for bringing the application into



compliance, and demonstrate what they have accomplished to bring their applications into compliance. Part 11 also applies to new systems, current applications, and legacy systems that are directly involved with research, clinical activities, product manufacturing, and distribution – all must comply.

The implications for non-compliance can be devastating for a pharmaceutical or health sciences company and can range from fines to having the FDA order the facility closed. An example of the potential severity of non-compliance is highlighted by a recent case. In May 2003 drug maker Schering-Plough Corp. agreed to pay the FDA \$500 million as part of a settlement to resolve quality-control problems at four of its factories.

Part 11 affects the following vertical industries: pharmaceutical, clinical trials management, medical device manufacturing, and companies that maintain medical devices, to name a few. There is also opportunity within the Federal government at FDA, the Centers for Disease Control and Prevention (CDC), and government hospitals and medical research facilities.

GOVERNMENT

Every Federal agency is legally required to manage its records. Records are the evidence of the agency's actions. Therefore, they must be managed properly for the agency to function effectively and to comply with Federal laws and regulations.

Agency heads have specific legal requirements for records management which include:

- Making and preserving records that contain adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities ([44 U.S.C. 3101](#)).
- Establishing and maintaining an active, continuing program for the economical and efficient management of the records of the agency ([44 U.S.C. 3102](#)).
- Establishing safeguards against the removal or loss of records and making requirements and penalties known to agency officials and employees ([44 U.S.C. 3105](#))
- Notifying the Archivist of any actual, impending, or threatened unlawful destruction of records and assisting in their recovery ([44 U.S.C. 3106](#))

WHO WE ARE

For 25 years, Applied Information Sciences (AIS) has provided software and systems engineering services to government agencies and businesses around the world. Our analysis-driven approach to business problems combined with our commitment to deadlines and budgets results in successful projects and long-term relationships with our customers, employees and partners.

For 13 years AIS has been a Microsoft Managed Gold Partner, the highest partner relationship offered by Microsoft. Additionally, several key AIS employees have been selected to be members of Microsoft Partner Advisory Councils. Joining a select few from around the world, these council members have the opportunity to review and provide feedback for Microsoft technologies and products. This unique partner status results in special product trainings and technical readiness programs years ahead of their market release, enabling AIS to help our clients prepare with the long-term planning of their technology evolution.

AIS, Inc. is headquartered in Reston, Virginia with additional offices in Columbia, Maryland and Austin, Texas.



APPLIEDINFORMATIONSCIENCES

Corporate Headquarters

11400 Commerce Park Drive
Suite 600
Reston, VA 20191
Phone: 703.860.7800
Fax: 703.860.7820

Central Regional Office

7718 Wood Hollow Drive
Suite 150
Austin, TX 78731
Phone: 512.651.5220
Fax: 512.651.5241

Contact Information by Department Sales

Phone: 703.860.7815

WWW.APPLIEDIS.COM

800-AIS-4553