

HiSoftware Policy Sheriff™ SP
HiSoftware Security Sheriff™ SP



Content-aware
Compliance
and Security Solutions for
Microsoft SharePoint®



SharePoint and the ECM Challenge

The numbers tell the story. According to the consulting firm Doculabs, 80 percent of the information within organizations is unstructured (word processing files, e-mails, spreadsheets, Web content, blogs, wikis, etc.), with growth predicted at a rate of 36 percent per year. So how are businesses managing this explosion of content?

Many organizations are turning to SharePoint as the solution to their content management challenges. Microsoft recently stated that 20,000 new SharePoint users come online every day. The research firm AIIM has also reported on the rapid adoption of SharePoint, stating that 70 percent of the largest global

organizations are already using it today. AIIM further reports that in organizations using SharePoint, more than half consider it their primary ECM system.

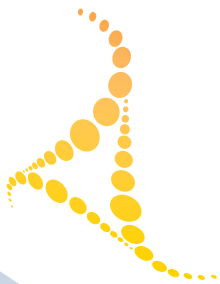
But gaps in SharePoint adoption and business-readiness remain, particularly when it comes to data compliance and the management of private or otherwise sensitive content. In fact, only 20 percent of the respondents to AIIM's 2011 survey indicated they had sufficient confidence in SharePoint security to store sensitive information. And more than 60 percent of organizations have yet to bring SharePoint in line with their existing compliance policies.

SharePoint: Not a Compliance and Security Silver Bullet

As this data shows, many organizations are deploying SharePoint to manage their enterprise content and streamline business processes while enhancing "enterprise 2.0." However, compliance and security concerns — and their associated risks — remain top of mind.

As the amount of content and user interaction increases, particularly given the enhanced collaborative capabilities of SharePoint 2010, the chance for a security breach or a compliance violation increases as well. Without effective

compliance and security controls, SharePoint will never realize its potential as a comprehensive, widely adopted Enterprise Content Management platform. A solution that automatically scans, classifies, applies permissions, tracks, encrypts and prevents the inappropriate storage, access and distribution of sensitive content stored in SharePoint is clearly necessary to overcome this confidence gap.



“Without effective compliance and security controls, SharePoint will never realize its potential as a comprehensive, widely adopted Enterprise Content Management platform.”



Ensure Data Compliance, Enforce Information Security Controls

Fully integrated with SharePoint, HiSoftware's content-aware compliance and security solutions, including HiSoftware Policy Sheriff SP and HiSoftware Security Sheriff SP, complement the platform's powerful content publishing and collaboration features by continuously auditing data and documents for compliance requirements such as privacy, information security, accessibility, site quality and brand integrity. Along with the hundreds of checkpoints built-into HiSoftware's proprietary rules engine including pre-defined checkpoint groups for Section 508, HIPAA, FISMA and other regulatory mandates, HiSoftware's solutions

allow users to easily define and configure tests for their own unique privacy and security policies without costly consulting and/or programming resources. As the checkpoint scans identify areas of risk or detect specific policy violations, the item is classified via the addition of metadata. Once classified based on these policy controls, pre-defined business rules can automatically restrict access to the item, encrypt it, track the document's chain of custody, and prevent it from leaving SharePoint.

HiSoftware Policy Sheriff™ SP

Policy Sheriff SP is HiSoftware's content-aware compliance solution for SharePoint. Fully integrated with SharePoint 2010, Policy Sheriff SP allows organizations to realize the full ECM potential of SharePoint by ensuring compliance with specific regulations and internal policies using the following functionality:

SCAN: Organizations scan information at rest within their SharePoint sites against the HiSoftware rules engine to assess the current level of sensitive information present and identify compliance issues. In addition to information at rest, Policy Sheriff SP also scans data in motion against these corporate policies.

REPORT: Through the Policy Dashboard, Policy Sheriff SP provides executive visibility into compliance and security status. Via standard reports, compliance and privacy officers can get real-time insight into the compliance status of the SharePoint environment, identify teams or departments where issues are recurring, and measure progress against compliance objectives over time.

CLASSIFY: As Policy Sheriff SP scans your SharePoint content, the content is classified via the addition of a metadata field:

- By the HiSoftware rules engine while it scans data at rest within a specific SharePoint site or library
- Automatically as new documents and items are added to SharePoint
- By authorized users when they create and/or edit an individual document or content item

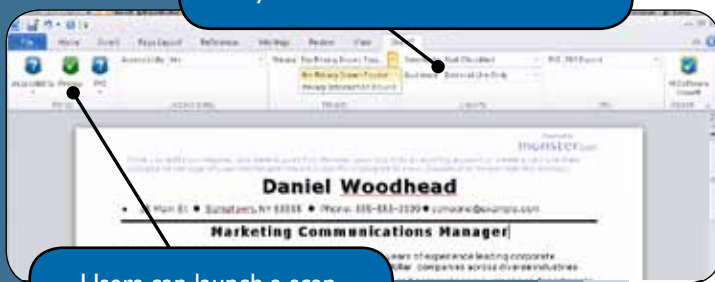
A number of basic classification categories come standard with the solution, however, an organization may easily customize any number of new classification categories for their specific needs.

Once an item is classified by Policy Sheriff SP, the classification values can then be utilized by Security Sheriff SP to encrypt and/or apply permissions that restrict access to the item, regardless of the permissions applied to the larger SharePoint site, library or list in which the item physically resides. Classification can also aid in e-discovery, search and retrieval, and provide a persistent form of identification for sensitive content as your SharePoint environment grows and evolves.

Sheriff Office Connectors and Sheriff Outlook Connectors

By deploying the Sheriff Office Connectors and Sheriff Outlook Connectors for Microsoft's Office and Outlook applications, organizations can add further controls to prevent sensitive content from being viewed by unauthorized users. Security Sheriff SP, working in concert with the Connectors, allows individual content contributors to scan and classify content on its way into and out of SharePoint from within the familiar Microsoft ribbon interface. Once classified, credentialed privacy or other policy officers may choose to upgrade, downgrade or override a user classification, as needed, to ensure that a specific document is tagged with the proper level of sensitivity. Both Connectors are optional add-ons and are sold separately.

Sensitivity and audience can be set by content authors. Policy officers can use the Connectors to override system or user classifications.



Users can launch a scan from directly within the client applications.

The Sheriff Office Connectors and Sheriff Outlook Connectors appear right in the ribbon, allowing users to scan and classify documents as they are being worked on.

HiSoftware Security Sheriff™ SP

Security Sheriff SP builds upon the policy scanning and classification features of Policy Sheriff SP to deliver content-aware security within SharePoint. Security Sheriff SP includes all the functionality of Policy Sheriff SP with the added ability to restrict access to and encrypt content based upon the presence of Protected Health Information (PHI), Personally Identifiable Information (PII) or other sensitive corporate information using the functionality outlined below:

RESTRICT: Based upon the business rules associated with its classification, access to a document or content item within SharePoint can be restricted to a specific individual or group, even if a wider audience has access to the site or library where the item physically resides in SharePoint.

ENCRYPT: When Security Sheriff SP identifies sensitive content, it can encrypt the information immediately. This means only properly credentialed users will be able to access the content — whether inside or outside of SharePoint — even if they have SharePoint administrator privileges.

PREVENT: Security Sheriff SP can prevent sensitive information from leaving SharePoint. For example, if a document is going to be emailed to a group and a listed recipient does not have proper access to that category of document, the email cannot be sent until that individual is removed from the distribution list.

TRACK: Security Sheriff SP tracks the entire lifecycle of SharePoint content and documents. This means that a policy officer can see if and when a document has been accessed, emailed, printed or edited, and by whom. A document's entire "chain of custody" is recorded and easily available in the event of a breach or a regulatory audit.

WORKFLOW: As specific areas of content risk are identified in SharePoint, Security Sheriff SP triggers workflow to remediate compliance issues and/or task the proper individual(s) in the organization to review and potentially classify, re-classify and encrypt the content. Workflow can also be used to prevent the publication of non-compliant content (e.g. in a discussion forum or blog) based upon the policies managed within the HiSoftware rules engine.

Flexible Rules Engine

HiSoftware allows organizations to automate the monitoring of SharePoint content both at rest and in motion. The flexible rules engine within Policy Sheriff SP ensures information moves in and out of your systems in accordance with your privacy policy, Written Information Security Program (WISP), and brand standards while preventing a damaging breach of private or other confidential information that could impact your bottom-line and your corporate reputation. Specific rule sets are pre-defined to address compliance with HIPAA/HITECH, MA 201 CMR, FISMA, COPPA, Section 508 and WCAG 2.0, OMB 10-22 and many other government regulations. These rules are available for use in both Policy Sheriff SP and Security Sheriff SP and are broken out into four modules, each sold separately.

PRIVACY: HiSoftware's Privacy Module automatically scans SharePoint sites to detect the presence of PII and PHI and notify policy officers and privacy managers. Depending on your organization's unique compliance approach and risk threshold, HiSoftware's solutions for SharePoint can confirm the use of secure methods to collect private information with the proper consents, and that whenever information is stored, accessed or moved, it is only by credentialed users and only to appropriate locations. Specific privacy checkpoints which come standard with the privacy module include: HIPAA, FISMA, COPPA, OMB 10-22 cookie guidance and MA 201 CMR 17.

ACCESSIBILITY: HiSoftware's Accessibility Module establishes ongoing, automated checks to ensure SharePoint accessibility concerns are seamlessly managed and that compliance issues are flagged and prioritized for swift remediation. The Accessibility module checkpoints map to all common Web accessibility standards, including Section 508, WCAG 1.0 and WCAG 2.0, Canadian Common Look and Feel (CLF) and XML Accessibility Guidelines (XAG).

BRAND INTEGRITY AND SITE QUALITY:

HiSoftware's Brand Integrity and Site Quality Module consistently scans and analyzes SharePoint content for broken links, brand conformance issues such as logo consistency and integrity, correct legal name usage, copyrights and more. This module also includes checkpoints to monitor for offensive or inappropriate language that may be included in collaborative environments such as blogs, discussion lists or other user-generated content. Detailed reports help development and quality assurance managers quickly pinpoint and fix issues as identified.

OPSEC INFORMATION ASSURANCE:

The OPSEC Module monitors and verifies that SharePoint content complies with federal risk assessment practices and the U.S. government's OPSEC guidelines. This includes operational military information and helps to determine if published SharePoint content references any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel. These safeguards help protect against the accidental disclosure of confidential information and fully integrates OPSEC testing into quality assurance and content delivery processes for your SharePoint farm.

HiSoftware is committed to ensuring that its rules engine delivers the best of both worlds. By taking advantage of pre-defined checkpoint groups to address specific regulatory mandates your organization can quickly deploy a proven content compliance solution and begin protecting sensitive information immediately. However, as you refine your compliance approach to meet the unique needs of your organization, the flexibility of the rules engine allows you to customize monitoring, enforcement and reporting protocols to deliver the most secure, compliant SharePoint environment possible.



Compliance and Security That Works the Way You Do

By default, SharePoint mirrors the traditional “IT” approach to permissions and access management. SharePoint secures access by applying permissions to specific libraries or lists based on Active Directory groups defined by the SharePoint Administrator. The Active Directory groups are often tied tightly to the organizational structure, yet frequently this approach does not reflect the cross-functional reality of how business gets done, and is often at odds with the use of SharePoint as an enterprise collaboration platform. This approach is also an underlying cause of the many governance headaches associated with SharePoint, including proliferation of sites and document libraries.

Both Security Sheriff SP and Policy Sheriff SP look at an entire library or list of content to identify individual documents and files which should be secured based on specific policies. These policies are applied by scanning the content against the defined checkpoints resident within the HiSoftware rules engine. This approach is possible because HiSoftware’s solutions for SharePoint are content-aware, and are able to read the actual data contained in a specific document or item. HiSoftware then classifies, and if desired, restricts access to, and encrypts the item(s).

Because permissions are applied at the individual file level (using classification), as compared with solutions that secure or encrypt documents at the library level, sensitive content can be stored, shared and collaborated on from any site, library or list in the SharePoint farm, and the access to that content restricted only to those who have permissions to the file as defined by its classification.

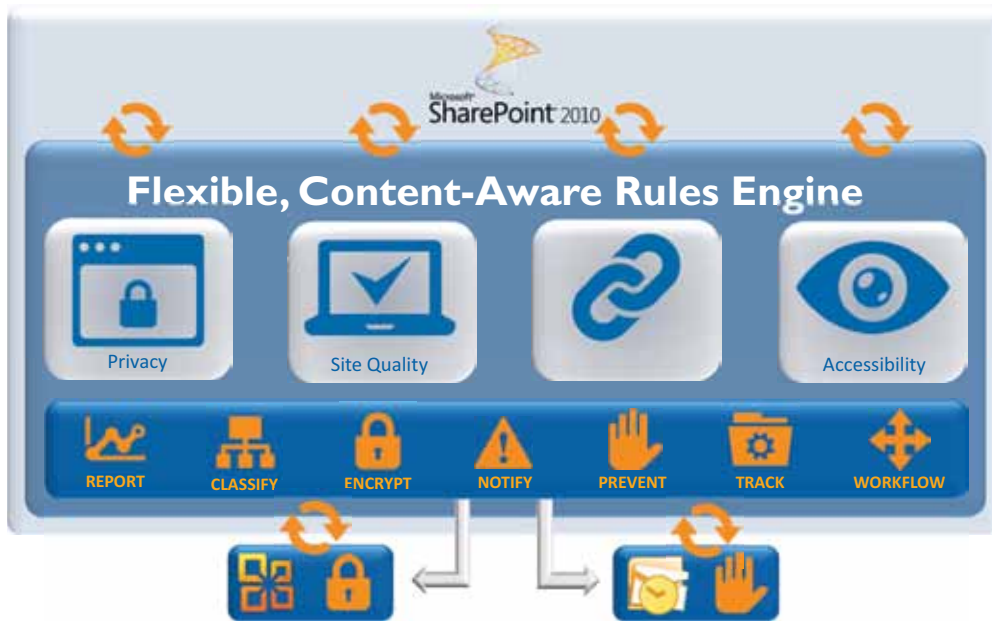
HiSoftware is the only solution which limits access at the item-level. In addition to protecting your organization from an accidental breach, this approach also controls the proliferation of sites, lists and libraries in SharePoint. For example, if a company’s board of directors is considering a potential merger, the documents generated prior to the merger becoming public can be stored anywhere in SharePoint and classified as “Board Only,” making the sensitive content visible only to relevant Directors. Other solutions would require the provision of a new site every time such a restricted project was undertaken. Most importantly, without item-level security, the end user has to remember the proper location for every sensitive item they create or edit to ensure appropriate access – a certain recipe for a breach.

Making SharePoint Safe for Sensitive Data

HiSoftware delivers comprehensive content-aware compliance and security solutions optimized for SharePoint. Unlike competitive solutions for classification, or enterprise data loss prevention (DLP) solutions that are significantly more expensive to deploy and maintain, HiSoftware has created a highly configurable, compliance and business-centric approach to managing sensitive data in SharePoint, tightly integrated to the way your organization already uses SharePoint and its complementary Microsoft applications today. And because of our content-aware approach to compliance and security, HiSoftware is the only vendor that offers this functionality at the file level, helping to simplify SharePoint governance while minimizing the creation of new sites expressly for the purpose of storing and sharing sensitive information.



HiSoftware Security Sheriff SP



HiSoftware Security Sheriff SP **scans** and **classifies** SharePoint data both at rest and in motion. Based upon classification, Security Sheriff SP restricts access to the item, **prevents** the item from being removed from SharePoint, and **tracks** its entire chain of custody. Any SharePoint item can then be **encrypted** to safeguard against a breach inside or outside of SharePoint. The solution also includes a complete set of policy **notifications** and **workflow** capabilities to alert privacy and information security officers of a potential risk. Using the Sheriff Office and Sheriff Outlook Connectors, individual content contributors can further manage compliance and privacy settings by applying classification from within the familiar Microsoft ribbon interface.

Key Features and Benefits

Maintain Compliance with Regulatory Mandates –

Leverage pre-defined checkpoints for HIPAA/HITECH, MA 201 CMR, FISMA, COPPA, Section 508 and WCAG 2.0, OMB 10-22 and many other regulatory requirements.

Leverage the Full Business Value of SharePoint –

Security and permissions functionality expands the community that can now safely use and have access to your SharePoint environment: internal employees, partners, vendors, customers and prospects.

Secure Sensitive Information – Implement content-aware controls that ensure the right users access the right information, every time.

Apply Unique Classification Parameters Using Metadata –

whether system-applied based on policies, or user-applied, classification can control access to content and aid in e-discovery, search and retrieval, and any audits which may be required in the event of a breach.

Simplify SharePoint Governance and Reduce Administration Costs –

Automate SharePoint compliance and security to reduce site proliferation and allow administrators to focus on higher value projects for training, business process management and user adoption.

About HiSoftware

HiSoftware provides content-aware compliance and security solutions for the monitoring and enforcement of risk management and privacy guidelines across digital environments. The company's solutions provide a data governance and compliance platform for content management and collaboration processes that support corporate and brand integrity, site quality, accessibility and confidentiality for public websites and portals, as well as internal intranets and SharePoint sites. HiSoftware's customers include some of the largest US and international government agencies, as well as Global 2000 companies. The company is headquartered in the United States in Nashua, New Hampshire and has international offices in Melbourne, Australia. For more information, visit www.hisoftware.com.



Corporate Headquarters

One Tara Boulevard, Suite 104

Nashua, NH 03062 USA

T: +888.272.2484 (U.S. & Canada)

+1.603.578.1870

F: +1.603.578.1876

E: info@hisoftware.com

 [@HiSoftware](https://twitter.com/HiSoftware)

www.hisoftware.com