dock
Simply Productive

4 Steps to Manage Compliance & Security

SHAREPOINT

Step 1

UTILIZING AUTOMATION TO PROTECT CLASSIFIED DATA

Plan and document governance strategies along with protecting your content and infrastructure by automating as much as possible. Protect your classified data by applying automation in a consistent, measurable and enforceable standard within the SharePoint environment. By doing so, you'll be able to see a reduction of opportunities for data breaches because of being proactive in scanning all sensitive information.

Automation starts with metadata that's embedded into your content assets to be used for discovery, classification and security best practices. Content can be identified with SharePoint managed metadata capabilities to the identification, tagging and appropriately classified. Automation should include data of your private customer and employee information, intellectual property, and confidential company documents such as contracts and reputations. We advise you to scan and report on SharePoint content to identify and afterward delete, tag or isolation of sensitive, harmful or non-compliant content.

Step 2

UTILIZE OFFICE 365 SECURITY & COMPLIANCE CENTER ALERTS

Once your alerts have been generated and displayed on the View alerts page in the Security & Compliance Center, you can triage, investigate, and resolve them. Your team can use the new alert policy and alert dashboard tools in the Office 365 Security & Compliance Center to create alert policies. Then view the alerts that are generated when users perform activities that match the conditions of an alert policy. Next, create alert policies to track malware activity and data loss incidents. In addition, many default alert policies are already included, which help you monitor assigning admin privileges in Exchange Online, malware attacks, and rare levels of file deletions and external sharing.

Step 3

SETUP AUDIT TRAILS FOR SHAREPOINT USAGE & ADMIN ACCESS

Auditing is key to efficiently managing your company's infrastructure even with using SharePoint. Start by enabling auditing for systems and file access, as well as all administrative changes to SharePoint. Audit any existing SharePoint permissions to review or create corporate access control policies that enable compliance and security structures. When you align SharePoint permissions with your corporate directory services, admins can understand inheritance and unmanaged item-level permissions. Auditing has the option to be configured for a site collection, a list or library, or based on a content type as part of an organizations information management policy.

Step 4

REGULARLY PERFORM BACKUPS & PROVIDE TESTING OF SYSTEM

We recommend your company performs regular backups as well as test and restore them on a consistent basis, at the very least annually. When testing your backup systems, consider how to recover from disasters using SharePoint services. By placing your SharePoint environment on a solid security traction, it frees up your time to broaden the use of SharePoint in your business for additional active collaboration and communication. Start by identifying and quantifying your Recover Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for your business. An RTO is a time that's required to recover from a disaster such as a security breach. It provides key metrics for disaster recovery planning. An RPO provides data measured in time that you can lose from the same disaster, which are key metrics for disaster recovery planning.