Managing Information Policy

An information management policy clearly lays out what kind of data should be kept, what kind should be deleted and establishes a sound, objective method to apply to company-wide data. So, how do you get started? The following steps can provide a basic guide for setting up your information management policy.

1. Take Inventory.
To establish a baseline, find out how much disk space is being used to back up and archive data, how many backup tapes are stored off-site, how much data each tape contains and how many paper files are stored on- and off-site. Once you've accounted for the amount of data your company has, take a sample of the files to get a rough idea of how much qualifies for transfer to a Safe Harbor folder—the area to keep electronic documents that meet the company's criteria for retention—and how much can be deleted.

2. Identify the types of records that must be retained.
This will vary by industry, so you will need to determine what rules apply to your company. In general, however, records that should be retained fall within one of these four categories:

- Marketing plans and materials
- Customer service records
- Purchasing records
- Financial records

Another method for determining retention criteria is to convene a committee of people throughout the organization. The criteria decided by this committee are then subject to final review by company leadership. Depending on your industry and company size, you should consider involving attorneys to assist with this process.

3. Appoint records coordinators throughout the company.
The actual implementation of the information management policy should be carried out by records coordinators at the department level and monitored by department heads. It's useful to keep the ratio of coordinators to employees somewhere between 20:1 and 25:1.To ensure department heads aren't overly accommodating on deciding what to keep, company leadership should conduct periodic audits.

4. Institute a strict email retention policy.
Many people treat their email as a "to do" list: letting their emails manage them, instead of managing their emails. To solve this problem, create an email policy that automatically deletes any email not moved to the Safe Harbor folder within a certain time frame (90 days is a good starting point)—no exceptions. This policy is also subject to audit.

5. Kick off and sustain your program with records retention week and periodic audits.
Give each business unit and department a deadline for cleaning up their records, which culminates into a "Records Retention Week," during which everyone goes through all data under their control—both electronic and paper files—and decides what to keep, archive and trash. **Give**

advance notice (four weeks is plenty) so your employees have time to analyze their data without compromising their work schedule.

6. Prevent unauthorized data removal or archiving.
An information management policy would be meaningless if data can be removed from the audit process, which is why companies should require that all data be saved on the company's servers, not on individual desktop computers. To ensure that all data resides with the company's servers, install a secure mobile access system that allows employees to access their data anywhere, anytime. Don't provide USB ports, CD burners or any other data removal devices on any terminal.

7. Implement a BYOD policy to control data stored on personal devices.
Nowadays, people use personal devices for work-related tasks because it can seem easier than using typical work resources. This is referred to as the Bring Your Own Device (BYOD) phenomenon, and it's affecting information management because it creates crossover between data that is controlled by an individual versus a company. While it may be more convenient for an employee to use his/her tablet to take notes during an office meeting, it makes it more difficult for a company to know about the data that is stored on a personal device.

Storing company data on personal devices can also cause forensics and e-discovery issues. If a company's data needs to be collected from a personal device that the company does not control or have access to, it can effectively halt the investigation and collection process. The best way to avoid BYOD issues is not allowing personal devices to be intermingled with or connect to the company environment. If an employee needs mobile access or a new media device to complete work, it should be the company's place to provide that device.