DIGITAL ACUITY
Giving your data a voice

The Checklist for eDiscovery Preservation

What should you do when you think there may be an E-Discovery request? Use this handy checklist to ensure that data preservation is efficient and defensible for you and your client.

Before Known Litigation Occurs	
☐	Work with and advise clients in developing document retention policies
☐	Periodically assess organizations compliance with their document retention policies

After Known Litigation Occurs	
☐	Confer with a broad group of stakeholders, including IT, HR and Legal, to ensure that every person/server related or potentially related to the legal matter is on legal hold
☐	Suspend any automatic deletion or purging of email and other key information systems including: • Pulling current backup tapes from rotation or recycling • Identifying any individual-level laptop/desktop backup routines are running on a scheduled basis; and archiving the most recent backups • Suspending any recycling/reissuance of hardware for departed employees • Suspend any automatic purge of user accounts or individual network shares for departed employees
☐	Send Legal hold notices when litigation is reasonably foreseeable (usually before when notice of suit is given). • Legal Hold Notice Must be in Written Form • The legal hold must remain in place until final disposition of the underlying matter
☐	Assure that the legal hold notice provides clear instructions to employees not to modify, destroy, delete or hide any electronic or hard copy data related to the commenced or anticipated litigation or investigation, including: • All paper or Electronic files (ESI) • Other data stored on the company's computer systems and storage media • Any other electronic data that may apply
☐	Take steps as early as possible to preserve data on user assigned laptops, desktops and mobile devices
☐	Use follow up interviews for employees who are sent the legal hold to ensure that the employee understands the legal obligation that a legal hold presents, as well as the possible sanctions that may be ordered against the company for failure to comply with the legal hold.

8765 W. Kelton Lane
Building C-1, Suite 102
Peoria, AZ 85382

DIGITAL ACUITY
Giving your data a voice

www.digital-acuity.com
602-354-2799

	List of Common Sources for Preservation: Employer-Controlled Sources
☐	E-mail Servers (mailboxes of individual e-mail users)
☐	File Servers and Print Servers (including individually-assigned network stores (home shares)
☐	Network drives accessed by multiple individual users (group shares)
☐	Archival data on backup tape or other storage media
☐	E-mail journaling systems
☐	Document management systems
☐	Proprietary structured databases (e.g databases containing HR, Customer or sales data)
☐	SharePoint and any other web based collaboration sites (e.g. Google docs, Zoho, Dropbox)
☐	Social networking sites and services/accounts used and maintained by the company
☐	Video and audio systems, including voicemail
☐	Legacy data (ESI generated by computer programs no longer used by the company)
☐	Hard copy document archives maintained by the company, including off-site storage
☐	ESI maintained in hosted databases in connection with prior litigation/investigations

	List of Common Sources for Preservation: Employee-Controlled Sources
☐	ESI on user assigned laptop/desktop hard drives including: • Word processessing, spreadsheets, images and other textbased files (e.g. MS Office Documents, PDF's, sound files, graphics, etc.) • Locally stored e-mail archivbes (user archived PSTs and OSTs) • Individual backup and temp files • Internet usage data (cookies, favorites, etc.)
☐	Portable storage media such as external hard drives, flash drives, cd's and DVD's etc.
☐	Company issued mobile devices such as cellphones and tablets

☐	Hard copy documents maintained by employees
☐	Cloud based storage such as DropBox or iCloud
☐	Social media and personal email accounts used by the employee in connection with performance of job responsibilities