

ACTION STEPS FOR A JOINT IT/LEGAL RESPONSE TO E-DISCOVERY

Rick Resetaritz
Assistant General Counsel
Oklahoma Department of Human Services
OKDHS Legal Division
P.O. Box 53025
Oklahoma City, Oklahoma 73152-3025
(405) 521-3638
email: richard.resetaritz@okdhs.org

1. Choose an IT e-discovery specialist/liaison from your top talent. Train additional staff to be able to take over in the event that this individual is recruited away.
2. Register these individuals for Kroll Ontrack E-Discovery Certification Course and send to E-Discovery Conferences, such as the ABA Techshow or the ABA National Institute on E-Discovery.
3. Collect information from Sedona Conference and the Federal Judicial Center and provide time for intense self-directed study.
4. Arrange for primary in-house counsel for e-discovery and the designated IT e-discovery specialist/liaison to exchange information regarding respective expertise. This will set the groundwork for the close working relationship.
5. Educate individuals responsible for IT functions about the need for preservation and the need to alter established methods and procedures when a litigation hold is imposed. Establish the individual or individuals to whom all questions can be directed. One of the important roles of the IT e-discovery specialist/liaison is to serve as such a focal point.
6. Educate agency management on the particular nature of electronically stored information, why paper is not equivalent, the breadth of devices and areas where electronically stored information is located, and the importance of a litigation hold.
7. Inventory the following:
 - Computers
 - Servers
 - Mainframes
 - Legacy systems and data
 - Databases (including small Access databases)
 - Method of Distribution of Reports
 - Multifunction Printer Hard Drives
 - Voicemail
 - Instant Messaging
 - System Logs
 - Smartphones

Cell phones
System architecture
Procedure for Re-imaging for Repair
Procedure for Departing Employees
Accuracy of Record Retention Schedules for ESI
Items routinely overwritten or deleted in key databases
Backup Schedules and Method
E-Mail
Default Settings
Automatic deletion
Third-party ESI within control of the agency

8. Assess internal ability to collect ESI and internal ability to conduct culling and searching. Initiate purchase of necessary software.
9. Contract with e-discovery vendor for consulting and comprehensive e-discovery services.
10. Standardize business practices for a litigation hold
11. Upon issuance of a litigation hold, determine whether immediate collection and preservation with a chain of custody is feasible given the scope of electronically stored information which may be relevant to the issues. Proceed to collect or preserve in place.
13. Determine key custodians and databases. Disputes are most likely in e-mails, databases, and automatic deletion features.
14. Determine goals of the 26(f) conference. Prepare a realistic draft of a proposed discovery plan that will produce needed ESI for all parties with the greatest efficiency and cost savings. Approach the conference with a collaborative intent, documented in your written correspondence.
15. IT and Legal should have a co-equal role in all 26(f) conferences.
16. Determine which system information should not be publicly disclosed for security reasons and outline the protective order that is necessary to protect the potential misuse of such information. Avoid public filings which expose the agency to later zero day exploits.

17. Preserve snapshots of backup media as close to the date of the precipitating event as possible.
18. Prepare costs, burden, and time estimates for any motion for protective order as to scope of preservation or production.
19. Assess any ESI affected by mission-critical operations.
20. Estimate the most likely sources of ESI to gather the greatest amount of relevant ESI. This will be matter which will be shared with opposing party in a collaborative effort to narrow the scope of preservation and collection. Early case assessment may be necessary.
31. Prepare for a 30(b)(6) deposition regarding ESI and IT issues.
32. Seek agreement on scope of preservation, categories of ESI that are excluded, number and identity of custodians, search methodology, procedure for encryption while in transit, definition of duplicate and near-duplicate, metadata, and production format.
33. Monitor the effectiveness of the litigation hold, collection, and processing with a regularly scheduled meeting schedule. Document all stages of the e-discovery process.
34. Maintain accurate record of issues discussed and resolution.
35. Trace the distribution of reports to determine unknown caches of ESI.
36. Interview users to determine if actual use differs from expected use.
37. Review training materials intended for users to make sure that no training is given which is contrary to the requirements of the litigation hold.
38. Issue repeated reminders of the litigation hold and make sure all new employees are advised of its effect and importance.
39. Document all incidents and whether or not ESI within the litigation hold was affected.

40. E-discovery and ESI public record production is a cost which must be factored into the economic analysis preceding the decision to add new functions.
41. Foundation requirements for admissibility of ESI must be considered before collection occurs.
42. Public accountability provisions in third-party vendor contracts may give a comprehensive right to examine or audit records relating to contract performance in the possession of the vendor. A formal notice of litigation hold should be directed to such contractors. Agency contract monitors must be fully informed of the litigation hold and able to answer questions.
43. ESI not resembling paper may be overlooked. For example, fleet GPS information may be valuable source data from which a variety of facts may be ascertained.
44. Periodically assess progress and improve the process.