

Information Technology Discovery Questions*

This document identifies the types of questions that may be asked of an information technology (IT) professional throughout the course of litigation. These questions are intended to identify how data and records (potential evidence) are handled and managed in the “normal course of business.” IT managers should consider how they or their staff would respond to these types of questions for the various systems they support, and whether new policies or procedures are needed to protect their agency from an adverse ruling from the courts.

General IT Questions

- § In how many different locations do you have operations?
- § Where are they located?
- § How many servers does your agency use?
- § Can you identify which server(s) support each application?
- § Can you identify which school-owned IT assets (hardware, software, peripherals, accessories) are used by each employee, non-employee consultant, consulting firm or contractor?

IT Security Questions

- § How do you document the assignment and removal of user privileges for shared applications, especially those that contain sensitive or confidential information?
- § How are user account rights assigned/removed?
- § Do you have an acceptable use policy for employees who use IT resources? Is the document available?
- § Do you document that users are informed of the acceptable use policy?
- § What audit trails are employed to track access to IT resources? How long are the logs retained?
- § Do you have a firewall or other security system to protect technology resources from attack? Do you keep logs of this security system(s)? How long are the logs kept?
- § How is remote access to the network authorized, provided, secured, authenticated and tracked?
- § Do you have policies or procedures for IT security, remote network access, data transfer outside the network and home use?

Record/Data Retention Questions

- § Does your agency have formal data storage policies? Who is responsible for approving data storage policies?
- § Are the data storage policies published, and is the document available?

- § When was the policy approved? Is this the first version of the policy, or were other versions of the policy in place when the relevant records/data to this litigation were created?
- § Does your school have an approved records Retention and Disposal Schedule(s)?
- § Who approved the schedule?
- § When was the schedule(s) approved? Is this the first version of the schedule, or were other versions of the schedule in place when the relevant records/data to this litigation were created?
- § Does anyone audit compliance with the data storage policy and the schedule(s)? When and whom?
- § Is any data relevant to this litigation automatically deleted or overwritten by new data? When was this activity suspended?

E-mail Questions

- § What e-mail systems are you using? What versions?
- § Is the e-mail system operated and maintained in-house or by an outside vendor or service provider?
- § Do you employ account size limits or automatic purge routines (time limits) for e-mail in active accounts and/or e-mail system archives (.pst files)? Do these or other limits also apply to calendars, notes, tasks and trash bins?
- § Do you employ e-mail archiving software? When was this software implemented? What rules are applied to its operation?
- § When did you migrate from the previous version to this version? What was the time frame of the migration?
- § Were all offices using the same system at the same time?
- § Were old mailboxes converted or did the users simply have an old and new mailbox?
- § What happened to the old e-mail? Was it deleted or allowed to stay on the server?
- § Do the older e-mail servers still exist?
- § Were the disks ever imaged or copied other than to tape?
- § Does that media still exist today?
- § Can a user have multiple e-mail accounts?
- § How are these accounts tracked?
- § Where is e-mail saved when a user saves it?
- § What options are users provided for storing e-mail? E-mail system archives? Network server storage? Hard drive storage? Peripheral device storage? Document management repositories? Printing?
- § What other electronic messaging, communication and collaboration tools (such as instant messaging, text messaging, voice mail, cell phones, pagers, PDAs, intranets, peer-to-peer tools, Web 2.0 tools, etc.) are used by employees, consultants and

contractors when conducting business? Are these tools operated and maintained in-house or by an outside vendor or service provider? Please answer the above questions from this section as they apply to these tools.

Tape Backup Questions

- § Are all servers backed-up for disaster recovery purposes? If not, which servers are not backed-up?
- § Have you ever restored a deleted or corrupted file from your backup system?
- § What backup systems are you currently using?
- § How long have you been using them?
- § Is the same version in use across all sites? If not, why not?
- § What other systems have you used historically?
- § When you migrated from one system to another system, what happened to the old data?
- § What types of storage media are you currently using?
- § Are all sites using the same generation of technology?
- § What other types of technology have been used historically?
- § When you migrated from the older technology to the new technology, what happened to the old tapes?
- § Did you retain the old tape drives and software to allow access to this technology?
- § Can you identify which backup tapes contain data from a selected server, and the date of the backup?
- § How do you keep track of which tapes you own and which tapes are onsite vs. off-site?
- § Have you always kept track of the tapes this way? If not, when did you start and how did you do it previously?
- § When you move a tape off-site, how do you reconcile the media move?
- § Is the off-site location owned by a vendor?
- § How often do you perform a physical media audit to ensure that all tapes are accounted for?
- § How is your media stored?
- § Is the media on a rotation cycle? Is the rotation cycle the same for all systems/applications/data?
- § How frequently do you run full and incremental backups for each server?
- § How do you address incomplete or unsuccessful backups?
- § Do you ensure that data and metadata backups are synchronized to ensure successful restoration?
- § Is there a written backup policy to document these activities?
- § Do you have a procedure for verifying the accuracy of backups?
- § Do you employ any redundant storage systems? Please describe.

Evidence Preservation Questions

- § When were you instructed to preserve potentially relevant records/data relating to this litigation? Who instructed you? How did you receive the instruction (is there a document that contains the instructions)?
- § Once you received instructions, what actions were taken to:
 - § Preserve potentially relevant electronic and paper records
 - § Notify employees, consultants, contractors and other third parties (such as other government entities or private sector partners/clients) to stop deleting or altering potentially relevant records/data
 - § Prevent PCs of key individuals from being disposed of should they leave the agency or receive new equipment
 - § Prevent key individuals from destroying or altering relevant records/data
 - § Prevent vendors or service providers who are storing and maintaining records/data from destroying or altering relevant potential evidence
 - § Prevent automatic purging or overwriting of data or records on active computer systems (including e-mail, databases, etc.)
 - § Prevent backup tapes from being overwritten
 - § Suspend normal destruction of records/data
- § What changes were made to the backup tape rotation cycle to accommodate the litigation hold? When were these changes implemented?
- § How did you determine that the correct tape(s) were held?

-
- Adapted from Kirke Synder, JD and David Ison, Esq., "A 30 (b) (6) Can Sink Your Ship," Information Management Journal, ARMA International, January/February 2006: 52 - 55.
 - For additional questions, see Nelson, Sharon D., Olson, Bruce A. and Simek, John W.; The Electronic Evidence and Discovery Handbook; American Bar Association Publishing; 2006.