



E-discovery Sample 30(b)(6) Deposition Notice

Pursuant to Rule 30(b)(6) of the Federal Rules of Civil Procedure, the party shall designate one of more officials, employees, agents or consultants who has knowledge of and will testify regarding:

E-mail Systems

1. The current and any prior system(s) used to create, transmit, store, retrieve, and delete e-mail including, but not limited to, name and version, installation dates, number of users, and location of users' mail files.

Computer Systems and Databases

2. The types of computers and hardware, desktop operating systems, types of networks and communications hardware and software.
3. Accessibility including information about user names, logons, passwords, and encryption programs.
4. Accessibility of computer systems from outside of the office.
5. Acquisition, location, and disposition of personal computers used by employees and others and any systems for recording such information.
6. Maintenance of hardware, software, including upgrades or replacements, and utility programs used.
7. The chain of custody of hardware and software, including processes when an employee leaves, and replacement and repair of equipment.
8. How electronic documents are maintained, archived, indexed, including descriptions of hardware and software used, and where this is physically located.
9. Corporate policies regarding employee use of company computers, software, e-mail and data.
10. The types of databases used, including how the database is accessed, and any standard reports prepared.

Backup

11. The name and version of software presently (and formerly) used; medium for storage of backed up information; the retention of the backup data; and information as to how and where such data is stored.

Document Retention and Collection

12. Corporate policies regarding use of computers and other technology, such as phone, faxes, PDA's, and voicemail.
13. Electronic records management policies and procedures.
14. The manner in which documents are indexed, located, maintained, including electronic and paper document retention policies.



Sample 30(b)(6) Request for Production of Documents

The designated witness shall produce in advance of the deposition the following documents:

1. All documents which the deponent has utilized or may need to refresh his or her recollection as to any of the issues made the basis of this lawsuit.
2. All documents which the deponent plans to consult or rely upon in preparation for the deposition.
3. All documents that refer or relate to the items above as the subject matter of the Rule 30(b)(6) deposition.
4. All document retention plans, technical manuals, network architecture diagrams, instructions, policies, booklets, memoranda, or guidelines to employees regarding the systems.



E-discovery Sample 30(b)(6) Deposition Questions

E-mail Systems

1. Identify current and former personnel responsible for administering the e-mail system.
2. Describe the current types of e-mail systems in use including the name and version numbers and date of installation.
3. Are all offices/locations using the same package and version?
4. What previous e-mail systems have been used? What date did you migrate to the new version?
5. Were the mailboxes from the previous system converted to the new system?
6. Was the e-mail from the former system kept on the server? Do the former servers still exist? Were the disks copied or imaged, other than to tape and, if so, where is that media if it still exists?
7. Where is e-mail saved? Is this a default or are there options as to where a user may save e-mail?
8. How many users on this e-mail system?
9. Where are the users mail files kept? Do they select the location for storage or does the system administrator? Is there a default storage location?
10. Can users access their e-mail remotely? If so, what systems do they use to do so?
11. Is there any transaction record for remote or dial-up access?
12. Are e-mail passwords routinely changed? If so, how often are they changed?
13. How is e-mail transferred? (SMTP, for instance)
14. What e-mail retention settings are active?

Computer Systems and Databases

1. How many different locations do you have operations and where are they located?
2. Are you primarily responsible for operations at all sites? If not, who is?
3. Are passwords or encrypted files used on computer systems? What is protected and how? Who has access and what types of access do they have?
4. Are passwords and access codes revoked/changed when an employee leaves the company?
5. Do employees work from home computers?
6. How do employees access the computer system and networks when working from home?
7. If employees are issued laptops, are there any additional security measures for these computers?
8. How are files transferred to and from employees' home computers?



9. Are there any standard file-naming or location-saving conventions employed by the company?
10. What types of data processing and data storage devices are used by your company in the course of business, including operating systems; backroom hardware; workstation hardware; whether notebooks or desktops are used; operating system; whether PDA's are used; any backup apparatus; types of storage devices (optical or electronic); computer faxing capability; office machines used (scanners, copiers, fax machines, voicemail)?
11. What is your network architecture?
12. Can you identify which servers support which application?
13. What are your usage policies, including number of users on the network, access rights?
14. What software is used on your computer systems?
15. What databases are used?
16. Identify the types of database software used. (Microsoft Access, Oracle, etc.)
17. Identify the persons responsible for maintaining the fields in the databases, including the source of the information, whether the information is verified, etc.
18. How are databases accessed and by whom? Are there different security levels? What are the queries, tables? What are the responses to the queries and are they stored anywhere?
19. Are there any standard reports prepared on a routine basis?
20. Identify any parties responsible for database design, maintenance, and backup.
21. Have database files been re-indexed, purged, repaired, or archived?
22. Are utility programs used on computers in the office? If so, which programs?
23. What upgrades to hardware have been done in the relevant time period? What was done with the replaced parts?
24. What upgrades to software or replacements have been done in the relevant time period? Was data backed up before the upgrade?
25. How are individual directories of employees leaving the company handled?
26. Are workstations reassigned to incoming employees? Are they purged, hard drives wiped or reformatted for new user, are hard drives backed up before the new user receives the system?
27. How are disks and drives destroyed?
28. Have you employed an outside contractor for hardware or software upgrades? If so, what contractors?



Backup

1. Are your servers backed up?
2. Who is currently responsible for backing up the files and archiving the files and data on the computer system? Who was previously responsible?
3. What backup systems are you currently using? What backup systems have you formerly used and what dates did you use each of the systems?
4. Are you using the same system at all offices/locations? If you are using other systems, what are they and why are you using different systems?
5. If you used other systems in the past, what happened to the old data when you migrated to the new system? Were both the media and software retained so that you could access the data?
6. What type of storage media do you use currently? Historically? Are all offices/locations using the same storage media?
7. What computer systems are backed up, including the backup software used, the content of the backups, the frequency of the backups, whether the backup process is automated, what type of media is the backup put on?
8. Describe tape rotation schedule.
9. Have any tapes been pulled from tape rotation? Why was this performed and who was responsible for performing?
10. Where is backup media stored and in what manner is it stored (shelving, safety deposit boxes)? How is the backup transported to this location? By whom is it transported? Where have you previously stored backups (for each office/location)?
11. Do you inventory/audit tapes stored off-site and, if so, how frequently? Is the storage site the same for all locations/offices? If not, what are the storage locations for each site?
12. Who has access to the backups?
13. What tape destruction method do you employ?
14. What archival backups, if any, have been created? What files are backed up and where are they stored?
15. Have any mailboxes been restored from backup tapes? If so, when was (each) performed? Which mailbox(es)? Describe the backup (How long did it take in labor hours? What equipment was needed?) Why was it performed?
16. Have you modified your backup procedures to comply with the discovery requests?
17. Have files been deleted from the computer system?
18. Are files archived off the system? If so, what files and where are the backups maintained?
19. How do you inventory the tapes? Do you maintain an inventory catalog of the backup tapes? For what time period does the catalog cover?
20. Can you identify which backup tapes contain data from a selected server?



Document Retention and Collection

1. Have you modified your use of computers to comply with discovery requests?
2. Have any responsive documents been purged since the inception of the lawsuit?
3. What steps have been taken to ensure preservation of relevant electronic data?
4. What changes were made to the tape rotation schedule to comply with the discovery request? When were the changes put in to effect? How was it determined what tapes were to be held and was there any action taken to confirm that the right tapes were being held?
5. Describe any disaster recovery plans in place now and for the relevant time period.
6. What is the company's document retention policy regarding electronic information and how long has it been in effect? It is published and, if so, where?
7. Are the company's retention policies always complied with? If not, why? Were there former policies and, if so, what were they?
8. Is the same document retention policy in effect for all locations of the company?
9. Is there any sort of an audit at all locations to ensure compliance with the policy?
10. Who performs the audit and how frequently is it performed?
11. Who is the person or persons in charge of your document retention policies and for what region/office are they responsible?