

Preparation Notes for IT Manager Deposition

1. Prior to deposition, request IT manager to bring:
 - a. Copies of all IT policies and procedures;
 - b. Copies of any IT inventories;
 - c. Any other documents necessary to refer to in order to fully describe the IT infrastructure.

2. General questions regarding infrastructure
 - a. Who is the system administrator? Who are the other employees who may be knowledgeable about the electronic data or IT systems in questions?
 - b. Identify all servers and their function i.e. web servers, print servers, database servers, fax servers. What operating system and version are they running on?
 - c. What are the logging and authentication practices that are being used?
 - d. What other equipment is being used onsite? This could include notebook computers, PDA's, cell phones, fax machines, printers, pagers, and voice mail. It is important to make sure your request includes these.
 - e. What kinds of media are being used? This could include diskettes, Zip Disks, CD-ROM, CD-RW DVD, tape, memory cards, memory sticks, USB key-chain type devices etc.
 - f. What equipment/media/software is being used offsite?
 - g. Are there any system audits or similar reports available?

3. Identify and describe each computer that has been, or is currently, in use by employees associated with this matter (including desktop computers, PDAs, portable, laptop and notebook computers, cell phones, etc.), including but not limited to the following:
 - a. All computers that have been used to store, receive or generate data related to the subject matter of this litigation.
 - b. Computer type, brand and model number (a company IT inventory would be useful here);
 - c. Computers that have been re-formatted, had the operating system reinstalled or been overwritten and identify the date of each event;
 - d. The current location of each computer identified as relevant to this matter.
 - e. The brand and version of all software, including operating system, private and custom developed applications, commercial applications and shareware for each computer identified;
 - f. The communications and connectivity for each computer, including but not limited to terminal-to-mainframe emulation, data download and/or upload capability to mainframe, and computer-to-computer connections via network, modem and/or direct connection;

4. Identify all email systems in use, including but not limited to the following:
 - a. Does your firm have a policy and procedures document regarding email? Can you produce the document?
 - b. Does the document require user signatures?
 - c. Do you have a copy of the signed documents for <names>?
 - d. Do you have a policy on the use of third party web mail accounts such as Yahoo?
 - e. List all email software and versions presently and previously used and the dates of use.
 - f. Identify all hardware that has been used or is currently in use as a server for the email system.

- g. Identify the specific type of hardware that was used as terminals into the email system (including home PCs, laptops, desktops, cell phones, personal digital assistants [“PDAs”], etc.).
 - h. State how many users there have been on each email system (delineate between past and current users).
 - i. State whether the email is encrypted in any way and list passwords for all users.
 - j. What is the archive policy on the email server?
 - k. Do you set up local mailboxes for synchronization on users computers?
 - l. Can and do the users set up their own local mailboxes for synchronization on their computers?
 - m. Identify all users known to you who have generated email related to the subject matter of this litigation.
 - n. Identify all email known to you (including creation date, recipient(s) and sender) that relate to, reference or are relevant to the subject matter of this litigation.
5. As to each computer network, identify the following:
- a. Brand and version number of the network operating system currently or previously in use (include dates of all upgrades);
 - b. Quantity and configuration of all network servers and workstations;
 - c. Person(s) (past and present including dates) responsible for the ongoing operations, maintenance, expansion, archiving and upkeep of the network;
 - d. Brand name and version number of all applications and other software residing on each network in use, including but not limited to electronic mail and applications.
 - e. Network storage of users’ data including shared and personal storage space.
6. Describe in detail all inter-connectivity between the computer system at [opposing party] in [office location] and the computer system at [opposing party # 2] in [office location # 2] including a description of the following:
- a. All possible ways in which electronic data is shared between locations;
 - b. The method of transmission;
 - c. The type(s) of data transferred;
 - d. The names of all individuals possessing the capability for such transfer, including list and names of authorized outside users of [opposing party’s] electronic mail system.
 - e. The individual responsible for supervising inter-connectivity.
7. As to data backups performed on all computer systems currently or previously in use, identify the following:
- a. All procedures and devices used to back up the software and the data, including but not limited to name(s) of backup software used, the frequency of the backup process, and type of tape backup drives, including name and version number, type of media (i.e. DLT, 4mm, 8mm, AIT). State the capacity (bytes) and total amount of information (gigabytes) stored on each tape;
 - b. Describe the tape or backup rotation and explain how backup data is maintained and state whether the backups are full or incremental (attach a copy of all rotation schedules);
 - c. State whether backup storage media is kept off-site or on-site. Include the location of such backup and a description of the process for archiving and retrieving on-site media;
 - d. The individual(s) who conducts the backup and the individual who supervises this process;
 - e. Provide a detailed list of all backup sets, regardless of the magnetic media on which they reside, showing current location, custodian, date of backup, a description of backup content and a full inventory of all archives.
 - i. Types and number of tapes in your possession (such as DLT, AIT, Mammoth, 4mm, 8mm);
 - ii. Capacity (bytes) and total amount of information (gigabytes) stored on each tape;

- iii. All tapes that have been re-initialized or overwritten since commencement of this litigation and state the date of said occurrence.

8. With regard to preserving the data associated with this matter:

- a. Have the proper steps been taken to preserve the evidence? Have employees been instructed not to alter or delete electronic data that may be in issue? Is it understood that all equipment in question should not be replaced, sold, or discarded?
- b. Identify all extra-routine backups applicable for any servers identified in response to this matter, such as quarterly archival backup, yearly backup, etc. and identify the current location of any such backups.
- c. For any server, workstation, laptop, or home PC that has been “wiped clean”, defragmented, or reformatted such that you claim that the information on the hard drive is permanently destroyed, identify the following:
 - i. The date on which each drive was wiped, reformatted, or defragmented;
 - ii. The method or program used (e.g., WipeDisk, WipeFile, BurnIt, Data Eraser, etc.).
- d. Identify and attach any and all versions of document/data retention policies used by [opposing party] and identify documents or classes of documents that were subject to scheduled destruction. Attach copies of document destruction inventories/logs/schedules containing documents relevant to this action. Attach a copy of any disaster recovery plan. Also state:
 - i. The date, if any, of the suspension of this policy *in toto* or any aspect of said policy in response to this litigation;
 - ii. A description by topic, creation date, user or bytes of any and all data that has been deleted or in any way destroyed after the commencement of this litigation. State whether the deletion or destruction of any data pursuant to said data retention policy occurred through automation or by user action;
 - iii. Whether any company-wide instruction regarding the suspension of said data retention/destruction policy occurred after or related to the commencement of this litigation and if so, identify the individual responsible for enforcing said suspension.
- e. Identify any users who had backup systems in their PCs and describe the nature of the backup.
- f. Identify the person(s) responsible for maintaining any schedule of redeployment or circulation of existing equipment and describe the system or process for redeployment.
- g. Identify any data that has been deleted, physically destroyed, discarded, damaged (physically or logically), or overwritten, whether pursuant to a document retention policy or otherwise, since the commencement of this litigation. Specifically identify those documents that relate to or reference the subject matter of the above referenced litigation.
- h. Has any of the equipment been taken out of service to prevent data from being overwritten? Has the proper imaging software and methodologies been employed to prevent changing dates of modification, access, users etc.?
- i. If there has been a forensic acquisition, who performed it? What software i.e. Encase or hardware was used?
- j. Has anyone touched or altered in any way any evidence prior to the forensics acquisition?
- k. Is there any equipment in anybody's home or remote office that may contain relevant information?
- l. Have there been any changes to the system or policies and procedures regarding electronic data during the time period in question?
- m. Is any of the electronic data in question protected by intellectual property or other rights?

9. May users store voice mail messages? If so, please provide the following information:

- a. Do users have the option of storing voice mail messages?

- b. If users can store messages, how long do they remain on the system? How many messages may be stored by the user?
- c. Are voice mail messages automatically purged? If so, describe the destruction schedule.

10. Is instant messaging (IM) being used? What kind and version?

11. Is remote access (PC-Anywhere, VPN) used? What kind? Are there any security methods used?

12. Is there any encryption being used? If so, request the encryption keys.