IRIS LLC Sample Interrogatories for Electronic Discovery

UNITED STATES DISTRICT
COURT DISTRICT OF [Jurisdiction]

Court File No.:

_____,
Plaintiff

INTERROGATORIES TO [Party Name

v.

_____,
Defendant

I. Definition.
The definitions below will apply to the interrogatories requested in this document

A. Application An application is a collection of one or more related software programs that enable a user to enter, store, view, modify or extract information from files or databases. The term is commonly used in place of "program," or "software." Applications may include word processors, Internet browsing tools and spreadsheets.

B. Backup To create a copy of data as a precaution against the loss or damage of the original data. Most users backup some of their files, and many computer networks utilize automatic backup software to make regular copies of some or all of the data on the network. Some backup systems use digital audio tape (DAT) as a storage medium. Backup Data is information that is not presently in use by an organization and is routinely stored separately upon portable media, to free up space and permit data recovery in the event of disaster.

C. Deleted Data Deleted Data is data that, in the past, existed on the computer as live data and which has been deleted by the computer system or end-user activity. Deleted data remains on storage media in whole or in part until it is overwritten by ongoing usage or "wiped" with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer.

D. Document phonorecords, Fed.R.Civ.P. 34(a) defines a document as "including writings, drawings, graphs, charts, photographs, and other data compilations." In the electronic discovery world, a document also refers to a collection of pages representing an electronic file. Emails, attachments, databases, word documents, spreadsheets, and graphic files are all examples of electronic documents.

E. Hard Drive The primary storage unit on PCs, consisting of one or more magnetic media platters on which digital data can be written and erased magnetically.

F. Mirror Image Used in computer forensic investigations and some electronic discovery investigations, a mirror image is a bit-by-bit copy of a computer hard drive that ensures the operating system is not altered during the forensic examination.

G. Network A group of computers or devices that is connected together for the exchange of data and sharing of resources.

H. Operating System (OS) The software that the rest of the software depends on to make the computer functional. On most PCs this is Windows or the Macintosh OS. Unix and Linux are other operating systems often found in scientific and technical environments.

I. Spoliation Spoliation is the destruction of records which may be relevant to ongoing or anticipated litigation, government investigations or audits. Courts differ in their interpretation of the level of intent required before sanctions may be warranted.

J. Software Coded instructions (programs) that make a computer do useful work.

II. Documents and Data.

A. Individual/Organizations Responsible Identify and attach copies of all company organizational and policy information including:

1. Organizational charts;
2. A list of the names, titles, contact information, and job description/duties for all individuals (or organizations) responsible for maintaining electronic process systems, networks, servers, and data security measures; and
3. A list of the names, titles, contact information, and job description/duties for all individuals employed in the following departments (or their equivalents) for [Plaintiffs/Defendants/Third Party]:
    a) Information Technology;
    b) Information Services;
    c) Incident Response Teams;
    d) Data Recovery Units; and
    e) Computer Forensic or Audit/Investigation Teams

B. Relevant Products/Services Identify and attach copies of all documents related to (including marketing, selling, leasing, sharing or giving to another party) the computer system, programs, software, hardware, materials, tools or information that [Plaintiffs/Defendants/Third Party] uses or has used in relation to the sale or use of [Product/Service]. This includes all electronic data and necessary instructions for accessing such data relating to:

1. The pricing of [Product/Service] in the United States and internationally;
2. Customer invoices for [Product/Service], including the customer names/addresses, purchase volume, prices, discounts, transportation changes and production information;
3. E-mail sent or received by [Plaintiffs/Defendants/Third Party] to customers relating to [Product/Service];
4. Accounting records relating to [Product/Service], including work-in-progress reports, billing records, vendor invoices, time and material records, cost completion reports for each of [Plaintiffs/Defendants/Third Party] customers;
5. Construction and development information relating to web pages offering sale of [Product/Service] to the public;

6. Internal reports, sales reports, customer backlog reports, supplier backlog reports and operation reports related to [Product/Service];
7. Financial reporting information on a monthly and annual basis including profit and loss statements, branch costs, contribution margins and corporate overhead relating to [Product/Service];
8. Budgeting, projection and forecasting information relating to [Product/Service]; and
9. Sales booked, gross profit dollars and percentage for the sales booked, net sales shipped, and gross and net profit dollars and percentages for [Product/Service].

C. Networks As to each computer network, identify the following:
1. Brand and version number of the network operating system currently or previously in use (include dates of all upgrades);
2. Quantity and configuration of all network servers and workstations;
3. Person(s) (past and present, including dates) responsible for the ongoing operations, maintenance, expansion, archiving and upkeep of the network; and
4. 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.

D. Hardware Identify and describe each computer that has been, or is currently, in use by [Plaintiffs/Defendants/Third Party] (including desktop computers, PDAs, portable, laptop and notebook computers, cell phones, etc.), including but not limited to the following:
1. Computer type, brand and model number;
2. Computers that have been re-formatted, had the operating system reinstalled or been overwritten and identify the date of each event;
3. The current location of each computer identified in your response to this interrogatory;
4. The brand and version of all software, including operating system, private and custom-developed applications, commercial applications and shareware for each computer identified;
5. 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, modern and/or direct connection; and
6. All computers that have been used to store, receive or generate data related to the subject matter of this litigation.

E. Software Identify and describe all software programs that have been, or are currently, in use by [Plaintiffs/Defendants/Third Party] including, but not limited to, the following:
1. Titles;
2. Version Names and Numbers;
3. Manufacturers;
4. Authors and contact information; and
5. Operating systems that the programs were installed on.

F. Operating Systems Identify and describe all operating systems that have been, or are currently, in use by [Plaintiffs/Defendants/Third Party] including, but not limited to, operating systems installed during [time period] for the following individuals:

1. [Name & Job Title]

G. E-mail Identify all e-mail systems in use, including but not limited to the following:
1. All e-mail software and versions presently and previously used by you and the dates of use;

2. All hardware that has been used or is currently in use as a server for the e-mail system including its name;
3. The specific type of hardware that was used as terminals into the e-mail system (including home PCs, laptops, desktops, cell phones, personal digital assistants, etc.) and its current location;
4. The number of users there has been on each e-mail system (delineate between past and current users);
5. Whether the e-mail is encrypted in any way and list passwords for all users;
6. All users known to you who have generated e-mail related to the subject matter of this litigation; and
7. All e-mail known to you (including creation date, recipient(s) and sender(s)) that relate to, reference or are relevant to the subject matter of this litigation.

H. Internet Use Identify any Internet policies and procedures in use, including but not limited to the following:
1. Any Internet Service Providers (ISP) that [Plaintiffs/Defendants/Third Party] has provided its employees and the method used to access the Internet;
2. The names and titles for all individuals who had Internet access;
3. Any Internet hardware or software documentation that is used to provide Internet access to the above individuals during [time period];
4. Internet use/access manuals, policies and procedures, including limitations on Internet access and use; and
5. All Internet-related data on the electronic processing systems used by [Plaintiffs/Defendants/Third Party] including but not limited to, saved Web pages, lists of Web sites, URL addresses, Web browser software and settings, bookmarks, favorites, history lists, caches, and cookies.

I. Other Electronic Data Identify any other electronic data in use, including but not limited to the following:
1. Activity log files contained on [Plaintiffs/Defendants/Third Party] network and any equipment needed to access the log files;
2. Manual and automatic records of hardware and equipment use and maintenance;
3. The names of Internet newsgroups or chat groups that [Plaintiffs/Defendants/Third Party] subscribes to; include the name and title of the individuals subscribing to each group as well as any information necessary to access the groups, including passwords; and
4. Any portable devices that are not connected to [Plaintiffs/Defendants/Third Party] network and that are not backed up or archived.

J. Data Transmission 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:
1. All possible ways in which electronic data is shared between locations;
2. The method of transmission;
3. The type(s) of data transferred;
4. The names and contact information of all individuals possessing the capability for such transfer, including list and names of authorized outside users of [opposing party's] electronic mail system;
5. The name and contact information of the individual responsible for supervising inter-connectivity.

K. Data Security Measures List all user identification numbers and passwords necessary for accessing the electronic processing systems or software applications requested in this document. During the course of this litigation, you must supplement all security measures with updated information, if applicable. Include:
1. Computer security policies;
2. The name(s) and contact information of the individual(s) responsible for supervising security; and
3. Information about each applications security settings, noting specifically who has administrative rights.

L. Supporting Information All codebooks, keys, data dictionaries, diagrams, handbooks, manuals or other documents used to interpret or read the information on any of the electronic media listed above.

III. Backup Protocols.

A. Current Procedures As to data backups performed on all computer systems currently or previously in use, identify and describe the following:

1. 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;
2. The tape or backup rotation, explain how backup data is maintained, and state whether the backups are full or incremental (attach a copy of all rotation schedules);
3. 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;
4. The name(s) and contact information for the individual(s) who conduct(s) the backup and the individual who supervises this process;
5. 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,
6. All extra-routine backups applicable for any servers identified in response to these Interrogatories, such as quarterly archival backup, yearly backup, etc., and identify the current location of any such backups, and
7. Any users who had backup systems in their PCs and describe the nature of the backup.

B. Backup Tapes Identify and describe all backup tapes in your possession including:

1. Types and number of tapes in your possession (such as DLT, AIT, Mammoth, 4mm, 8mm);
2. Capacity (bytes) and total amount of information (gigabytes) stored on each tape; and
3. All tapes that have been re-initialized or overwritten since commencement of this litigation and state the date of said occurrence.

IV. Spoliation of Electronic Evidence

A. Document Retention and Destruction Policies Identify and attach any and all versions of document/data retention or destruction policies used by [opposing party] and identify documents or classes of documents that were subject to scheduled destruction.

1. Attach copies of document destruction inventories/logs/schedules containing documents relevant to this action.
2. Attach a copy of any disaster recovery plan.
3. Also state:
    a) The date the policy was implemented;
    b) The date, if any, of the suspension of this policy in toto or any aspect of said policy in response to this litigation;
    c) 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; and
    d) Whether any company-wide instruction regarding the suspension of the data retention/destruction policy occurred after or related to the commencement of this litigation. If so, identify the individual responsible for enforcing the suspension.

B. Document Destruction Identify any data that has been deleted, physically destroyed, discarded, damaged (physically or logically), or overwritten, whether pursuant to a document retention or destruction 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.

C. Organizations or Individuals Responsible for Maintaining the Document Retention and Destruction Policies List the job title, description, business address, telephone number, and e-mail address of any individuals or organizations that are/were responsible for creating, implementing or retaining any and all versions of your document retention or destruction policies.

D. Meetings or Documents Discussing Document/Data Destruction Identify with specificity any meetings or conversations referencing document spoliation in relation to this action.

1. Identify and attach any and all related meeting minutes/notes from [time period here].
2. List the job title, description, business address, telephone number, and e-mail address of any individuals or organizations that are/were responsible for retaining the meeting minutes/notes.

E. Data Wiping For any server, workstation, laptop, or home operating system 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:

1. The date on which each drive was wiped, reformatted, or defragmented;
2. The method or program used (i.e., WipeDisk, WipeFile, Burnlt, Data Eraser, etc.)

F. Data Recycling Identify the person(s) responsible for maintaining any schedule of redeployment or circulation of existing equipment and describe the system or process for redeployment.