

Preservation of Evidence (Spoliation) Warning Letter.

[Name of Entity]
[Street Address]
[City, State, Zip Code]

Re: [Cite the specific incident]

[Month, Day, Year]

Dear [Name of person/individual at the Entity],

By this letter, you are hereby given notice not to destroy, conceal or alter **any video, audio, paper or electronic files and other data generated by and/or stored on your computers, and storage media** (e.g., hard disks, floppy disks, backup tapes, Zip cartridges, USB drives, CDs, DVDs, etc.), or iCloud or “cloud” storage, or any other electronic data, such as voice mail. As you know, your failure to comply with this notice can result in severe sanctions being imposed by the Court for spoliation of evidence or potential evidence.

Through discovery we expect to obtain from you a number of documents and things, including Video, audio, files stored at your [location] [school, office, amusement park] or off-site, computers and your computer storage media.

In order to avoid spoliation, you will need to provide the data requested on the original media, or on exact copies of that media (sometimes referred to as image, evidentiary, or mirror copies), and be able to prove that the original matches the copy in every respect. Do not reuse any media to provide this data.

Additionally, in order to avoid spoliation you may have to suspend certain normal computer maintenance procedures, including but not limited to such procedures as de-fragmenting hard drives, deleting internet cookies, deleting browser history and favorites, and running any “disk clean-up” processes. For Video, this would include “loop” recording that would record over the video protected under spoliation.

Although I may bring a motion for an order preserving documents and things from destruction or alteration, your obligation to preserve documents and things for discovery in this case arises in law and equity independently from any order on such motion.

Electronic documents and the storage media on which they reside contain relevant, discoverable information beyond that which may be found in printed documents. Therefore, even where a paper copy exists, I will seek all documents in their electronic form along with information about those documents contained on the media. I will also seek paper printouts of only those documents that contain unique information after they were printed out (such as paper documents containing handwriting, signatures, marginalia, drawings, annotations, highlighting and redactions) along with any paper documents for which no corresponding electronic files exist.

My discovery requests will ask for certain video, audio, data on the hard disks, floppy disks, USB drives, or iCloud or “cloud” storage and backup media used in your computers, some of which data are not readily available to an ordinary computer user, such as "deleted" files and "file fragments." As you may know, although a user may "erase" or "delete" a file, all that is really erased is a reference to that file in a table on the hard disk; unless overwritten with new data, a

Adequate Template for Preservation of Evidence

"deleted" file can be as intact on the disk as any "active" file you would see in a directory listing.

Courts have made it clear that all information available on electronic storage media is discoverable, whether readily readable ("active") or "deleted" but recoverable. See, e.g., *Easley, McCaleb & Assocs., Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994)*; "deleted" files on a party's computer hard drive held to be discoverable, and plaintiff's expert was allowed to retrieve all recoverable files); *Santiago v. Miles, 121 F.R.D. 636, 640 (W.D.N. Y. 1988)*; a request for "raw information in computer banks" was proper and obtainable under the discovery rules); *Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90, 112 (D. Colo. 1996)*; mirror- image copy of everything on a hard drive "the method which would yield the most complete and accurate results," chastising a party's expert for failing to do so); and *Northwest Airlines, Inc. v. Teamsters Local 2000, et al., 163 L.R.R.M. (BNA) 2460, (USDC Minn. 1999)*; court ordered image-copying by Northwest's expert of home computer hard drives of employees suspected of orchestrating an illegal "sick-out" on the internet).

Accordingly, electronic data and storage media that may be subject to my discovery requests and that you are obligated to maintain and not alter or destroy, include but are not limited to the following:

Introduction: description of files and file types sought,

Date range is from [*state the Day, Date, Month, Year and time AM and or PM*], through [*state the Day, Date, Month, Year and time AM and or PM*]: All Video and Audio, (relating to dismissal), digital or analog electronic files, including "deleted" files and file fragments, stored in machine-readable format on magnetic, optical or other storage media, including the hard drives or floppy disks used by your client's computers and their backup media (e.g., other hard drives, backup tapes, floppies, Jaz or Zip cartridges, USB drives, CD-ROMs, DVDs) or iCloud or "cloud" storage or otherwise, whether such files have been reduced to paper printouts or not. More specifically, you are to preserve all video, audio, e- mails, both sent and received, whether internally or externally; all word-processed files, including drafts and revisions; all spreadsheets, including drafts and revisions; all databases; all CAD (computer-aided design) files, including drafts and revisions; all presentation data or slide shows produced by presentation software (such as Microsoft PowerPoint); all graphs, charts and other data produced by project management software (such as Microsoft Project); all data generated by calendaring, task management and personal information management (PIM) software (such as Microsoft Outlook or Lotus Notes); all data created with the use of personal data assistants (PDAs), such as, smart phones, such as Apple iPhones, Samsung Galaxy phones, Google Pixel phones, PalmPilot, HP Jornada, Cassiopeia or other Windows CE-based or Pocket PC and smartphone devices; all data created with the use of document management software; all data created with the use of paper and electronic mail logging and routing software; all Internet and Web-browser-generated history files, caches and "cookie" files generated at the workstation of each employee and/or agent in your employ and on any and all backup storage media; and any and all other files generated by users through the use of computers and/or telecommunications, including but not limited to voice mail.

Further, you are to preserve any log or logs of network (swipe badge logs), used by employees or otherwise, whether kept in paper or electronic form, and to preserve all copies of your backup tapes and the software necessary to reconstruct the data on those tapes, so that there can be made a complete, bit-by-bit "mirror" evidentiary image copy of the storage media of each and every

Adequate Template for Preservation of Evidence

personal computer (and/or workstation) and network server in your control and custody, as well as image copies of all hard drives retained by you and no longer in service, but in use at any time from to the present.

You are also to preserve and not destroy all passwords, decryption procedures (including, if necessary, the software to decrypt the files); network access codes, 10 names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view and (if necessary) reconstruct the electronic data we will request through discovery.

1. Business Records: All documents and information about documents containing backup and/or archive policy and/or procedure, document retention policy, names of backup and/or archive software, names and addresses of any offsite storage provider.

a. All e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) sent or received by the following persons:

List of names and job titles will be forthcoming. For now, this list consists of any [*Name Venue/Entity*] employee, contractor and acting agent of these entities.

b. All video and audio from any and all [*describe area and detail and name of injured person(s)*].

c. All other e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) containing information about or related to:

[*List every potential person, entity and organization you can think of that might hold the evidence to support your position*].

d. All databases (including all records and fields and structural information in such databases), containing any reference to and/or information about or related to:

[*List every potential person, entity and organization you can think of that might hold the evidence to support your position*].

e. All logs of activity (both in paper and electronic formats) on computer systems and networks that have or may have been used to process or store electronic data containing information about or related to:

[*List every potential person, entity and organization you can think of that might hold the evidence to support your position*].

f. All word processing files, including prior drafts, "deleted" files and file fragments, containing information about or related to:

[*List every potential person, entity and organization you can think of that might hold the evidence to support your position*].

g. With regard to electronic data created by application programs which process financial, accounting and billing information, **all** electronic data files, including prior drafts, "deleted" files and file fragments, containing information about or related to:

Adequate Template for Preservation of Evidence

[List every potential person, entity and organization you can think of that might hold the evidence to support your position].

h. All files, including prior drafts, "deleted" files and file fragments, containing information from electronic calendars and scheduling programs regarding or related to:

[List every potential person, entity and organization you can think of that might hold the evidence to support your position].

i. All electronic data files, including prior drafts, "deleted" files and file fragments about or related to:

[List every potential person, entity and organization you can think of that might hold the evidence to support your position].

2. Online Data Storage on Mainframes and Minicomputers: With regard to online storage and/or direct access storage devices attached to your mainframe computers and/or minicomputers: you are not to modify or delete any electronic data files, "deleted" files and file fragments existing at the time of this letter's delivery, which meet the definitions set forth in this letter, unless a true and correct copy of each such electronic data file has been made and steps have been taken to assure that such a copy will be preserved and accessible for purposes of this litigation.

3. Offline Data Storage, Backups and Archives, USB drives, iCloud or "cloud" storage, Floppy Diskettes, Tapes and Other Removable Electronic Media: With regard to all electronic media used for offline storage, including magnetic tapes and cartridges and other media that, at the time of this letter's delivery, contained any electronic data meeting the criteria listed in any of the preceding paragraphs above: You are to stop any activity that may result in the loss of such video, audio, electronic data, including rotation, destruction, overwriting and/or erasure of such media in whole or in part. This request is intended to cover all removable electronic media used for data storage in connection with their computer systems, including magnetic tapes and cartridges, magneto-optical disks, floppy diskettes and all other media, whether used with personal computers, minicomputers or mainframes or other computers, and whether containing backup and/or archive data sets and other electronic data, for all of their computer systems.

4. Replacement of Data Storage Devices: You are not to dispose of any video, audio, electronic data storage devices and/or media that may be replaced due to failure and/or upgrade and/or other reasons that may contain electronic data meeting the criteria listed in paragraph 1 above.

5. Fixed Drives on Stand-Alone Personal Computers and Network Workstations: With regard to video, audio, electronic data meeting the criteria listed above, which existed on fixed drives attached to stand-alone microcomputers and/or network workstations at the time of this letter's delivery: You are not to alter or erase such electronic data, and not to perform other procedures (such as data compression and disk de-fragmentation or optimization routines) that may impact such data, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments, copies have been made of all directory listings (including hidden files) for all directories and subdirectories containing such files, and arrangements have been made to preserve copies during the pendency

of this litigation.

6. Programs and Utilities: You are to preserve copies of all application programs and utilities, which may be used to process video, audio, electronic data covered by this letter.

7. Log of System Modifications: You are to maintain an activity log to document modifications made to any video, audio, electronic data processing system that may affect the system's capability to process any electronic data meeting the criteria listed above, regardless of whether such modifications were made by employees, contractors, vendors, agents and/or any other third parties.

8. Personal Computers Used by [name staff employee if you can. If not, state "staff employee(s)"] Used by You, Your Employees and/or your Secretaries and Assistants and/or their Secretaries and Assistants: The following steps should immediately be taken to safeguard all personal computers used by you and your employees and/or your and/or their secretaries and assistants.

a. As to fixed drives attached to such computers: (i) a true and correct copy is to be made of all electronic data on such fixed drives relating to this matter, including all active files and completely restored versions of all deleted electronic files and file fragments; (ii) full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drives should be written; and (iii) such copies and listings are to be preserved until this matter reaches its final resolution.

b. All USB drives, floppy diskettes, magnetic tapes and cartridges, iCloud or "cloud" storage, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to this matter are to be collected and put into storage for the duration of this lawsuit.

9. Evidence Created Subsequent to This Letter: With regard to electronic data created subsequent to the date of delivery of this letter, relevant evidence is not be destroyed and you are to take whatever steps are appropriate to avoid destruction of evidence.

In order to assure that your obligation to preserve documents and things will be met, please forward a copy of this letter to all persons and entities with custodial responsibility for the items referred to in this letter.

10. Social Media Accounts: At this time, you are to preserve the social media accounts data used by the [name of the entity] and personally by any persons with information, in anyway connected to the above referenced incident, on the date(s) of the incident, [state the Day, Date, Month and time of the incident if possible].

11. Copy of Video and Audio: At this time, you are to preserve the Video and Audio of the entire [state the name of the entity] on the date of the incident, [state the Day, Date, Month and time of the incident if possible]. Specifically, [state as much as you can to identify specific video cameras and or audio or screen shot, etc.], pictured below for your reference [if you can include a picture of the camera and area the camera covers].

Adequate Template for Preservation of Evidence

Original copies will be mailed. This email version is to expedite preservation of potential evidence.

Truly Yours,

[*your full name*]

[*your street address*]

[*your city, state, zip code*]

cc: [*anyone else you want to receive this copy- Corporation Counsel, Headquarters, Corporate office, etc.*]