Cc to Conni
& Sally
11/2/97

Babin, Babs

Fr m: Glynn, Lynne (LE)
Sent: Friday, October 03, 1997 12:43 PM
To: Allen, Carol; Anderson, Scott; Babin, Babs; Beard, Fay; Boronat, Jose; Brown, Rob; Chalub, Marcelo; Chan, Joe; Chou, Ching; Correia, Jose F.; Danos, Pattie; Davis, Matt; Dolliente, Evangeline; Dupont, Julien; Dust, Sandra; Egan, Sue; Farfone, Frank; Fung, Jerisa; Hernandez, Jaime; Kobayashi, Gisleine; Kowalski, Alfredo; Krause, Jean; Lebans, Tanya; Lee, Alan; Leonhard, Ursula; Lorenzo, Antonio; Lui, Isabel; MacKintosh, Lena; Mantinian, Manuel; Martinez, Lidia; Masten, Dave; Morales, Gustavo; Morales, Martha; Namkung, Hae-Rim; Newman, Cindy; Pieri, Paul; Ring, Jerold; Rossi, Enrica; Sirait, Jorang; Subramanian, Narayan; Sugano, Shinya; Suthep, Tanthanasarn; Tamborra, Jack; Van Loon, Wilhelmus; Yates, Catherine; Cislak, Lauren; Cross, Debbie; Crowley, Linda; Dittenhafer, Diane; Emmel, Becky; Espinosa, Sarah; Henson Jr, Bob; Johnson, Theresa; Lichon, Linda; Murray, Lois; Pearson, Gaye; Salerno, Kathy; Siemak, Sally; Smith, Carol; Smith, Jan; Swick, Martha; Zellers, Linda
Subject: Records Management for Community Advisory Panels and Charitable Donations

A retention period has been developed for charitable donations and community advisory panels. Th retention period is five years plus current year. This information will be included in the addition to the records management manual. If you have any questions, please let me know.

Lynne Glynn
Public Affairs
47 Building
517/636-9846
fax 517/638-7238
lglynn@dow.com

CONFIDENTIAL

DO 006494

El ctronic Information Records Management Policies and Recommendations (Section 111)

Storage Schedules & Compliance	Records retention schedules apply regardless of the recording or storage media. Electronically stored records require special diligence because their creation, storage and destruction are often automated and may be performed by another function. The function which authorized the creation of the electronic record (the creator/user) is responsible for records management compliance.
Annual Reviews	If records are stored by a custodian such as Information Systems, the creator/user of the records shall annually review storage inventory reports and/or directory listings to assure compliance with retention schedules. The custodian of the records shall furnish sufficient information to allow for annual review. This normally includes file name, media reference (volume #), creation date and scheduled destructi n date. If additional copies of the records are retained by the custodian, (i.e. backup or archive copies, as part of an overall disaster recovery plan), the custodian shall inform the user in writing of the retention schedules of such copies. Backup schedules must not violate records management policies.
On-line Storage	Except for electronic filing systems, "On-line" disk files are not the official company records for retention purposes and should be transferred to another media for retention.
Off-line Storage	Magnetic storage media, i.e. magnetic tapes, floppy disk, etc. are to be maintained in a suitable storage area that is free from temperature and other environmental extremes.
File Names	Names used for electronic file maintained by a custodian shall contain references that designate functional ownership and point to related programs and system documentation. End user generated files, not maintained by a custodian, must be traceable back to the creator.
Ad Hoc Reports from Electronic Files	The person requesting an ad hoc report is responsible for making sure there is an established records retention period for the report and for compliance with the retention period.
Back-up	Each time an electronic file is used there is risk of its destruction. The creator/user should assure that a backup copy exists.

CONFIDENTIAL

DO 006495

Electronic Information Records Management Policies and Recommendations (Section 111), Continued

Public Domain Software Guidelines

To meet their responsibility to protect Dow's computer systems, Dow employees must follow these guidelines:

1. All public domain software shall be submitted to a Dow Computer Security Focal Point for individual review to detect viruses prior to installation or use on a Dow computer.

2. All public domain software not previously cleared by a Dow Computer Security Focal Point shall be deleted form the computer and the computer checked for viruses before that computer is used to process Dow data.

3. Dow data processed on a computer on which public domain software previously had been used shall be submitted to a Dow Computer Security Focal Point for review to detect viruses.

4. Antivirus software available from Dow shall be used on all computers used to process Dow data.

NOTE: Contact your local computer security administrator if you suspect a virus might exist on your system or for clarification of Dow's Security Policy.

Subject File Index

A recommended practice is to maintain an index of electronic filed by subject matter, showing the file name, purpose, creation dare, storage media and location. A periodic comparison of inventory listings and/or directory listings with the index should disclose new or forgotten files.

An electronic file may contain many physical files of unrelated information which may have varying records retention periods. Such files will require multiple entries in the subject matter index.

Off-line Storage

On large computer systems, the retention and eventual destruction of magnetic tape files is mostly automatic. Special attention by the creator/user may be required if tapes are to be kept beyond the normal retention schedules because of a suspension order issued by the Legal, Tax, or Patent Departments. Tapes created by computer reruns or special recovery procedures should also receive close attention to ensure the correct retention period has been specified and followed.

Records stored on tape should be copied to new media before the end of the manufacturer's recommended media life. This is generally five years on tape reels and ten years on cartridge tapes. Similarly, if the technology is becoming outdated, please transfer data files to the new media while we still have equipment to read the files.

Section 112

Electronic Information Records Management

ANSWERS TO 15 COMMONLY ASKED QUESTIONS ON RECORDS MANAGEMENT FOR ELECTRONIC RECORDS

November 1992

CONFIDENTIAL

DO 006497

Electronic Information Records Management Questions and Answers - Section 112

Question 1 - Electronic Notes?

How long may/must I keep the notes I <u>receive</u> by electronic mail?

You need not keep them at all. Retention is the responsibility of the originating department, not the recipient. However, if you do keep the message, you may <u>not</u> keep it longer than the established retention time. Most messages that are sent by electronic mail are "short-term" records. Once they have served their purpose, they should be destroyed. Notes that are not "short-term" records must be transferred to an appropriate filing system (see question 5). Thus, it is preferable to discard or file messages on a note-by-note basis. At a minimum we recommend quarterly cleanup.

Question 2 - My Messages?

How often should I delete a copy of the messages I have <u>sent</u> to other people?

Messages that are "short-term" records should be deleted note-by-note when they have served their purpose. If this cannot be done, we recommend a quarterly cleanup as a minimum. Notes that are not "short-term" records should be transferred to other media (see question 5).

Question 3 - "Short-Term"?

How can I tell if a message is a "short-term" record or not?

Generally, a "short-term" record has three characteristics:

A. It does not fall into any of the categories of documents with specific retention times, in the Dow Records Management Manual.

B. It is intended to be acted upon, or otherwise serve its purpose, in a rather short period of time.

C. Once it have served its purpose, there is no business need to keep it, and no legal requirement to keep it.

EXAMPLES: meeting notice, a note saying to return a telephone call, or a draft that will be revised.

Question 4 - Ownership?

Do electronic messages belong to the individual employee?

No. Messages sent by Dow electronic mail systems are Dow property. This is the same policy as for other Dow Records.

Question 9 - E-Mail deletes?

If I delete a document from electronic mail, is it really gone?

After a time, yes. Many computer records, including electronic mail are "backed up" periodically and continue to exist for a time even if you delete the message from your electronic mailbox. Backup copies are destroyed periodically, on a schedule that varies from one Dow computer system to another. If you need to know the backup policy for a specific system, contact your Information Systems representative.

Question 10 - Audits?

How often will I be audited? Who will audit my electronic records?

Those decisions are made by your management. However, the Records Management Committee recommends the following as a minimum audit policy:

A. The Records Management Coordinator for the site or function has primary responsibility for auditing. As a minimum, each year audits should be conducted for a representative sample of employees, plus <u>each</u> employee who ceases employment in the function/site over which the coordinator has responsibility.

B. The Coordinator should have the specialized expertise to audit electronic records, or should obtain the assistance of a qualified expert.

C. The audit of electronic records may, but need not, coincide with an audit of paper records.

Question 11 - Draft Documents?

If I create a draft document in electronic media and later I revise the draft, what is the "starting date" for records retention?

There are two documents to discuss: the draft copy and the final document.

The draft has its own retention as a "short-term" record. When you revise it, the draft normally should be destroyed because it has served its purpose. Some computer systems do this automatically; others keep one or more past revisions unless you specify otherwise.

As for the revised (final) document, the "starting date" for records retention is the date written in the document. Many computer systems will also have a "directory" with a date. The directory date is <u>not</u> the controlling date for records retention, but may be used if it is consistent with the date written in the document. As long as th <u>year</u> is the same, there is no problem for documents whose retention is one year or more.

Electronic Information Records Managem nt Questions and Answers - Section 112, Continued

Confidential business information - **"Restricted for Use Within Dow"**	This classification is for records whose disclosure outside Dow might not harm Dow, but the information has not been made public. You may use this classification under the following guidelines: a. Mark the note "Restricted for Use Within Dow". b. Unless a secrecy agreement is in place that covers these records, you must obtain the permission of the department responsible for the information before sending the message to anyone who is not a Dow employee. This includes: (i) a contractor employee, even if that person is working on Dow projects. (ii) an employee of a Dow subsidiary r Dow-associated company.
Confidential business information - **"Dow Confidential Information"**	This classification is for records whose disclosure to the public would harm Dow - - for business reasons, legal reasons, or any other reason. EXAMPLES: the specifications for process equipment, the formula for a product, or marketing plans. These records may be sent by electronic mail, but only to Dow employee <u>who need to know.</u> Please observe the following: a. Unless a secrecy agreement is in place that covers these records, you must obtain proper clearance, including Legal Department or Patent Department approval, before sending the note to persons other than Dow employees. This includes: (i) a contractor employee, even if the person is working on Dow projects. (ii) employees of Dow subsidiaries or Dow-associated companies. b. If you use a standard "mailing list", check first to see if everyone on the list has a need to know this information. c. Double-check the distribution to assure that the message is going to the proper persons. Is anyone forwarding his/her electronic mail to a person (including a supervisor, a co-worker, a subordinate or an office professional) who has no need to know? d. Mark <u>every page</u> of the note "Dow Confidential Information."
	continued on next page

Electronic Information Records Management Questions and Answers - Section 112, Continued

Question 13 - Records on Disk? (continued)

C. Undated disks. Each document stored on a disk must be dated. We recommend that d date also be put on the disk itself. That will help you know whether the documents on your disk are still within their retention time.

D. Disks with documents that do not all "expire" at the same time. Remember that when a document reaches the end of its retention time, it must be destroyed.

That can be difficult if the disk also contains other documents that have not expired. There are two options:

1. Don't "mix" records on your disk. Store only one type of record on your disk (so that all documents are kept the same number of years). Then start new disks every year. When a disk expires, destroy all the documents on it. This requires more time "up front", but save time during the annual review of records.

2. If you do store records with different expiration dates on a single disk, you must review that disk at least annually to see if any documents have expired. Destroy any expired documents in one of the three Dow-approved ways. If your computer system cannot overwrite specific files, you probably will have to copy off "current" documents onto a new disk, then destroy or overwrite the old disk.

E. Disks that contain proprietary information, but are not properly secured. A documents is subject to the same security requirements, whether it is written on paper or stored on a disk. Thus, a disk must be protected according to Dow policies for the most confidential document it contains.

F. Disks that "travel" with an employee to a new job. Documents are "owned" by the function or department where they were created – not by the individual employee. If a transferred employee's new duties do not include the subject matter of those documents, someone else must assume the responsibility for keeping them until they expire.