E-MAIL GUIDELINES

E-MAIL GUIDELINES

FOR

MANAGERS AND EMPLOYEES

Prepared by the Collaborative Electronic Records Project
Rockefeller Archive Center
September 2006

TABLE OF CONTENTS

EXECUTIVE SUMMARY

To prepare the Rockefeller Archive Center (RAC) for receiving donations of e-mail[1] and other information in digital form, the Center partnered with the Smithsonian Institution Archives on a three-year Collaborative Electronic Records Project launched in August 2005. The project's primary objective is to develop management guidance and technical preservation methods that will enable archives to make electronic information accessible and usable for future researchers. To accomplish this goal, depositing organizations should establish policies and procedures for generating and saving electronic information long before records are transferred to an archive. By raising awareness among donor organizations when electronic records are being generated rather than waiting until the records are deposited, RAC hopes to receive electronic records with their authenticity[2] and integrity[3] intact. While it may be two years or so before we have the technical infrastructure in place to accept quantities of e-mail, we may be able to assist organizations in planning for the transfer of electronic records, whether to the RAC or another archive.

This document sets forth archivally acceptable methods of managing e-mail, and may be adopted, in whole or in part, by any non-profit organization. Circumstances may dictate modification to fit the needs of a particular office. Before implementing e-mail guidelines, each organization should review their Records Management Policy[4] with their legal, financial, and administrative advisors. While this document is intended to apply to records retained for historical research purposes, organizations should consider its applicability to other information retained (usually in a repository other than an archive) short or long-term for operational, legal, or financial reasons. This Preliminary E-mail Guidance, although being made available now as a stand-alone document, will be incorporated into a generic Records Management Policy scheduled for publication near the end of the Collaborative Electronic Records Project in 2008. Both products will be available at no charge for adoption by RAC depositor organizations or other non-profit groups. Organizations may wish to treat each section as a separate document rather than reproducing it in its entirety for all employees. Recognizing that most of our depositors do not have a dedicated Records Manager, we are including a basic outline of duties generally ascribed to the position.

---

[1] Electronic mail, commonly known as e-mail, is a form of communication in which messages are sent and received through an electronic device including computers and memory sticks.

[2] Authenticity means a record that is what it purports to be, i.e., includes the e-mail with its attachments and transmission data, and that was created by the credited author.

[3] Integrity is confirmation that a record has not been altered, intentionally or accidentally, since its creation or receipt.

[4] Records Management Policy is a formal, written document containing an organization's procedures for managing records, paper and electronic, of its activities. It typically includes guidelines regarding which records to retain, the length of time they should be kept, the manner in which they should be organized, and the procedures for disposing of them or transferring them to an archive.

SECTION I

E-MAIL GUIDELINES FOR MANAGERS

E-MAIL GUIDELINES FOR RECORDS MANAGERS

Reasons to Develop E-mail Guidelines

Business Climate

Over the past twenty-five or so years, the use of electronic devices such as computers has changed the way organizations conduct business and has altered the form and quantity of records documenting policies and activities. A 2003 study by the University of California-Berkley determined that the quantity of information created between 2000 and 2003 almost doubled and that approximately 93 percent of it was "born digital."[5] Other research indicates that in 2006, 60 billion e-mails will be sent each day and that electronic records are increasing by 80 percent annually.[6] Despite technological advances, the majority of official records[7] continue to be printed out on paper for long-term retention. Due to the proliferation of paper documents, the increasing cost of storage space, and perennially inadequate processing staff, archives now find it necessary to work proactively with their donors to find ways to maximize the use of space, time, and funds, yet continue to retain records of enduring value.

Businesses, whether non-profit or for profit, are subject to legal and/or governmental requirements that mandate retention of certain information. An e-mail can be an official record; thus, it is imperative that organizations establish compliant e-mail policies. A 1993 ruling in Armstrong v. Executive Office of the President upheld a lower court decision that a printed copy of an e-mail is merely for "convenience" whereas the electronic version contains complete information regarding the transmission. It also held that separate retention schedules must be maintained for paper and electronic records.[8] Communication may be with anyone who has an e-mail address, whether or not both parties are connected to the same local area network; hence, an organization may need to retain received as well as created e-mail. E-mail systems have the capability of transmitting messages with attachments that range from digital images, to correspondence with interactive links, to websites, to financial spreadsheets. Generally, an attachment and the e-mail that is transmits it must remain electronically linked in order to qualify as an acceptable and complete record copy of the communiqué. Ideally,

---

[5] NECCC Analysis of State Records Laws Work Group, "Challenges in Managing Records in the 21st Century," Lexington, KY: National Electronic Commerce Coordinating Council, 2004, <http://www.ec3.org/Downloads/2004/Challenges_in_El_Records.pdf> (4 February 2006),14-15.

[6] David Silverberg, "E-mail Retention Reaching Critical Mass," *Business Edge*, Vol. 1, No. 21 (27 October 2005) http://www.businessedge.ca/printArticle.cfm/newsID/10991.cfm (4 November 2005); Stefanie Murray, "Management of records more important than ever" *Lansing State Journal*, 13 Oct 2005, http://www.tallahassee.com/mld/tallahassee/busiess/12888528.htm?template=contentModules/printstory.jsp > (18 Oct 2005).

[7] Official record: information created or received in the course of conducting an organization's business.

[8] Graduate School of Library and Information Science, University of Texas at Austin, "Managing E-Mail as Records," < http://www.gslis.utexas.edu/~scisco/lis389c.5/email/public.html> (7 February 2006).

electronic records procedures will be incorporated into a company's Records Management Policy, and the retention period[9] will be determined based on a record's content rather than its physical form. Although most businesses regularly copy information from their server(s) onto backup media (usually magnetic tapes) for disaster recovery purposes, this process does not meet legal, regulatory, or historical record-keeping responsibilities. The latter may not require production of information for years after records are created, whereas the former would likely necessitate accessing only recently created documents.

E-mail and other electronic records are created, saved, or deleted by almost all employees in an organization. Typically a company no longer employs file clerks to be sure important documents are retained and placed in designated folders that are named according to company or department-wide specifications. Often organizations neglect to establish electronic filing procedures, nor do they routinely train employees about company policies regarding electronic records. As a result, some business records are being lost or are inaccessible without spending inordinate amounts of time and money searching for particular messages. If backup tapes are retained longer than a disaster recovery period, e-mail pertinent to a particular policy question or lawsuit could be in every tape, none of which have searchable, standardized subject headings. Demands for greater financial accountability, e-mail legal discovery requirements, new federal and state regulations, and the need for operational security and efficiency mean that e-mail guidelines are a critical part of conducting business. Lack of, or inadequate procedures for, managing e-mail can cost a company in fines, wasted time, customer or donor goodwill, and increased expenditures for storage space. These issues will become increasingly important with the exponential increase in the number of e-mails.

At a glance, here are the key reasons to institute appropriate e-mail guidelines:

- to minimize an organization's legal liability
- to comply with privacy laws
- to facilitate the legal discovery process
- to enhance compliance with governmental regulations
- to improve organizational efficiency and effectiveness
- to establish information audit trails
- to reduce the likelihood of information loss
- to prevent unauthorized access to information
- to reinforce organizational control over electronic traffic
- to preserve institutional memory and history
- to assist in training employees
- to ensure that records of enduring value which will be transferred to an archive will be accessible and readable by researchers.

[9] Retention period: the organization's pre-determined 'expiration' dates – the point in time when a record may be destroyed. Financial, legal, and governmental requirements, in addition to the organization's administrative needs and the historical value of the records, are considerations in establishing retention periods.

Financial Accountability

Although non-profit organizations are exempt from the stockholder oversight and governmental reporting required of for-profit businesses, non-profits are increasingly being brought under state and federal legislative regulations. Issues addressed include electronic filing, independent accounting audits, and excessive compensation of Board members and officers. For example, for 2005 and later tax returns, the Internal Revenue Service requires tax-exempt organizations having assets of $100 million or more to file electronically. The following year, private foundations and charitable trusts, regardless of asset size, will be required to file Form 990-PF electronically if they generate at least 250 returns (e.g. 245 employees).[10] New York is one of the first states to propose regulation of non-profit organizations, initially focusing on the most well-funded ones.[11] Precisely because non-profits lack a 'big brother' watchdog, their financial practices may be more lax as well as subjected to closer scrutiny by the media and other parties concerned about the misuse of tax-exempt funds. Properly managed e-mail could help protect an organization's reputation, tax-exempt status, and donation flow.

Legal Issues

Multi-million dollar fines against companies for failure to provide e-mail subject to legal discovery, while thus far having little impact on the non-profit world, may soon reach tax-exempt organizations. Non-profits are as susceptible as for-profit companies to lawsuits regarding employment-related issues such as discrimination and harassment. Recent statistics indicate that "one in five employers has had an e-mail subpoenaed by courts and regulators, and another 13 percent have battled workplace lawsuits triggered by employee e-mail."[12] Four primary situations create financial and legal difficulties for companies: 1) inability to cost effectively search for e-mail relating to one person, topic, or department (the way discovery requests usually specify); 2) lack of a records retention schedule and a records management policy; and 3) failure to follow the retention schedule or records policy; and 4) deletion of e-mail.

Despite a dearth of case law regarding electronic evidence, courts have applied a broad definition of electronic documents that encompasses e-mails, instant messages, backup tapes, metadata, calendar notations, notes, and deleted files. Generally courts prefer, but do not always require, that electronic documents be presented in their original format because the metadata may contain critical evidence missing when files are printed or converted to other formats such as PDF. Based on the few court decisions regarding electronic records to date, companies have an obligation to maintain records, including electronic ones, and may weaken their defense if pertinent records are not available.

---

[10] Internal Revenue Service, U.S. Department of Treasury, "Tax Information for Charities & Other Non-Profits," <http://www.irs.gov/charities> (4 February 2006).

[11] Eliot Spitzer, Attorney General, State of New York, Charities Bureau, "Internal Controls and Financial Accountability for Non-Profit Boards," http://www.oag.state.ny.us/charities/charities.html > (10 March 2006).

[12] Jennifer LeClaire, "The Future of E-Mail Archiving" *TechNewsWorld* 13 Oct 2005 http://www.technewsworld.com/story/46481.html (18 Oct 2005).

Legal tests espoused in *Zubulake v. UBS Warburg*[13] are often used to determine if a company may be liable for sanctions and should be considered when developing an e-mail policy:

1) Was there an obligation to preserve e-mail at the time it was destroyed?
2) Was the evidence intentionally, willfully, or negligently destroyed?
3) Was the evidence relevant to the case?

In some instances destruction has been determined relevant evidence. Potential consequences include fines, dismissal, default, summary judgment, and in extreme instances, criminal penalties. Failure to retain or losing e-mail as required by the Securities and Exchange Commission led to a $15 million fine in one of several lawsuits against financial institutions. Other fines were smaller, although still in the millions.[14] Informal and forwarded e-mail may not meet a court's standard for a reliable business record, and could be considered hearsay.[15]

Operational Needs and Security

Organizations use records, paper and electronic, for their institutional memory as well as to provide service and information to customers, whether the general public, employees, or directors. Developing and following appropriate e-mail guidelines will streamline the workflow and minimize the risk of information loss when it is necessary to locate critical evidence of a policy or program decision or of an activity. Cost efficiencies will result from effective e-mail guidelines because elimination of files according to the retention schedule will free more hard drive and server space, reduce the need for duplicate paper systems, and make locating files faster.

Staff changes provide opportunities for an employee who is leaving to delete, encrypt, or abscond with company information. Security risks involved in the use of laptops, off-site computers, devices such as memory sticks, iPods, digital cameras, etc. should be addressed in e-mail guidance and records management policies. Not only can the accidental loss of a portable device expose confidential information (such as employee medical information, expense accounts, social security numbers; credit card numbers of seminar attendees, buyers of publications, etc.) to unauthorized users, it can also allow the intentional use of computerized tools to extract data for unauthorized purposes or to spread viruses, worms, or similar menaces. Organizations face enormous financial and legal risks from security breaches. Management controls should be part of effective e-mail and records policies. Even if an outside contractor handles or disposes of sensitive information the hiring company is responsible for evaluating the vendor's capability of properly managing the data. A general rule of thumb is to institute security

---

[13] Brian J. Leddin and Dean Gonsowski, "Spoilation of Electronic Data," *New Jersey Law Journal*, Vol. CLXXIX, No. 3, 17 January 2005.

[14] Gregory Cresci, "Morgan Stanley to Pay $15 Million for Failure to Save E-Mails," Bloomberg 14 February 2006. <http://www.bloomberg.com/apps/news?pid=10000103&sid=aBoVvwOm0I6I&refer=us>.

[15] Kathryn Keneally, "E-mails sent during the business day may not be admissible as business records," *Champion Magazine*, January/February 2004 <http://www.nacdl.org/public.nsf> (7 February 2006).

measures suited to the exposure to loss and in line with procedures taken by peer companies, but also considering emerging trends across industry lines.

Regulatory Requirements

The Sarbanes-Oxley Act (SOX) has drastically changed the way for-profit businesses operate and is having a trickle-down effect on non-profit organizations. In a 2005 study, researchers found that 97 percent of participating non-profit groups have been affected by SOX.[16] A few states including New York have enacted, or have proposals in their legislatures, to adopt similar legislation. Significant concerns for non-profits are that companies such as Moody's have incorporated the Act's reform measures into their tax-exempt debt rating criteria, and that Congress and the IRS are reviewing non-profit governance, ethics, and openness. Strengthening controls in accordance with Sarbanes-Oxley may be valuable in attracting and retaining donors, board members, and lenders as well as in preparing for the anticipated extension of regulations to non-profits. Because retaining records that may be pertinent to a federal investigation is required, e-mail that reflects decisions and actions to implement SOX criteria, and to ensure that executive salaries and benefits are not excessive, will be useful documentation for regulatory inquiries, Congressional testimony, and institutional memory.[17]

Although legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to health care plans, clearinghouses, and providers as well as "business associates," some researchers may be considered health care providers.[18] Organizations involved in research using human subjects should consult their attorneys and/or the U.S. Department of Health and Human Services to determine if their research is exempt from HIPAA. The Food and Drug Administration (FDA) has privacy regulations applicable to research on human subjects similar to those under HIPAA. To avoid potential problems, and in anticipation of HIPAA expansion, an organization should handle personal health care data in accordance with HIPAA and FDA guidelines.

Similarly, under Federal Trade Commission (FTC), Fair and Accurate Credit Transactions Act authority (16 C.F.R. 682), effective June 1, 2005 companies that obtain consumer information for credit card purchases or from sources such as consumer credit

---

[16] Foley & Lardner LLP, "Foley & Lardner Study Finds, Despite Intentions of Public Company Governance Reforms, Many Private and Nonprofit Organizations Continue to Be Impacted," *Business Wire*, 9 March 2005.

[17] Marv Balousek, "Private Companies, Nonprofits Can't Ignore SOX: Federal Law Mandates Document Retention, Other Internal Controls," *Wisconsin State Journal*, 1 May 2005; Carol Hymowitz, "In Sarbanes-Oxley Era, Running A Nonprofit is Only Getting Harder," *Wall Street Journal*, 21 June 2005. "The Next Challenge for Nonprofits," *NJBIZ*, 19-26 December 2005. Susan Kinzie and Valerie Strauss, "After AU, Colleges Increase Scrutiny: Scandal Heightens Efforts to Seek Advice, Ask for New Audits," *Washington Post*, 21 November 2005; Jonathan D. Epstein, "Tougher Accountability Rules are Impacting Nonprofit Groups," *Buffalo News*, 5 December 2004.

[18] For more information, see U.S. Department of Health and Human Services, HIPAA, <http://www.dhhs.gov/ocr/hipaa/privacy.html> and <http://www.dhhs.gov/ocr/hipaa/guidelines/businessassociates.pdf>.

reports are required to take reasonable measures to ensure the privacy of that data. Organizations that obtain such information about prospective employees, vendors, consumers, or grantees, etc. are required to destroy or erase electronic media so that the information cannot be read or reconstructed. Lack of an effective information security program may be considered a violation of FTC requirements.[19]

The Independent Sector's Nonprofit Panel has developed "Proposed Governance Principles for Discussion with Large Foundations" for foundations to use in strengthening their accountability and transparency in accordance with regulatory and legal issues discussed above. See http://www.independentsector.org/programs/gr/charityreform.html.

E-mail Policy & Procedures Suggestions

In order to lessen employee confusion, e-mail guidelines should be incorporated into a Records Management Policy and employee manual. All departments, particularly Information Technology, Records Management, and Human Resources, should collaborate on establishing the organization's records management policies and procedures. The following suggestions are not comprehensive and should be reviewed by legal counsel and the management team before adoption.

Creating and Managing E-mail

Employer's Right to Access

The Federal Electronic Communications Privacy Act of 1986 allows employers to monitor employee e-mail for legitimate business purposes. E-mail may be subject to public access and legal subpoena.

- Provide for regular audits by Information Technology Department
- Establish authority levels for altering and deleting messages that have been sent

Privacy protection

- Institute data privacy measures for employee records (i.e., medical, personnel, academic, social security numbers)
- Warn employees that all e-mail on company equipment is company property and subject to being made public

Security

- Require password change on a regular basis
- Prohibit password sharing
- Establish guidelines for passwords, e.g. combination of numbers and letters, and program system to refuse weak ones
- Establish Information Technology (IT) department monitoring of log-ins for unauthorized access

[19] Charlene Brownlee and Melissa Cozart, "FTC Issues Rules for Disposal of Consumer Report Information," *Legal Update*, Fulbright & Jaworski, L.L.P, May 2005.

- Develop a formal policy and train employees on handling security risks and breaches
- Designate one person as co-coordinator of information security to handle suspected security breaches and other information management matters. Be sure all employees have the person's contact information.
- Require encryption for sensitive data that will be on laptops or other portable or remote devices that are particularly susceptible to theft and viruses, worms, etc.

Other

- Define and put in writing (paper and/or electronic) roles and responsibilities of each staff member regarding e-mail and electronic record creation, organization, access, privacy, security, and retention
- Develop and disseminate to all employees the company's Records Management policy when it is enacted and upon hiring new employees; Require that they read, understand, and sign an agreement to abide by the policy (see sample in Appendices)
- Give all employees the contact information for your Records Manager
- Define copyright rules and be sure employees involved in the issue understand them and have a reference copy

Saving E-mail

- Establish organization-wide (or at least department-wide) subject heading and Inbox file folder naming standards to be sure that e-mail can be accessed and retrieved in the future
- E-mail that is considered a record should be archived. Give employees adequate instructions and/or training to accomplish this.
- When employees retire, leave, or change work units, records stored in folders on their hard drives should be retained.
- E-mail back-ups are short-term storage for disaster recovery only. This function is not appropriate for long-term storage of information, nor is it compliant with accepted archival practice.
- Establish a "hold" policy for e-mail that may be pertinent to a known or expected legal case or investigation

SECTION II

E-MAIL GUIDELINES FOR RECORDS MANAGERS

E-MAIL GUIDELINES FOR RECORDS MANAGERS

Role

Although an organization's Records Manager bears the primary responsibility for development and enforcement of the company's Records Management Policy, the entire management team, including Information Technology, should be involved in the process. Key functions of a Records Manager with respect to e-mail follow.

- Authenticity, integrity, and reliability – Coordinate with IT department to be sure e-mail contains audit trails adequate to assure authenticity, integrity, and reliability to satisfy legal and regulatory requirements; include access restrictions and encryption procedures for sensitive data
- Disaster recovery – Set policy regarding backup procedures, frequency, storage, duplicate off-site copies, etc.
- E-mail Policy – Communicate the organization's policies to all incoming employees, interns, volunteers, and provide at least annual refreshers to all employees
- Former employees – Establish policy for migration, retention, or deletion of e-mails when an employee leaves, retires, or changes work groups
- Off-site and portable device use – Develop company policy regarding use of home computers, laptops, portable electronic devices such as flash, iPod, and digital cameras. Consider privacy, data security, virus protection, and information availability issues.
- Organization-specific needs – Consult with your legal, financial, and regulatory advisors to develop guidelines that meet your particular organization's needs
- Passwords – Issue password protection instructions
- Record keeper – Designate 'official' keeper(s) of a department's e-mail, i.e. the person who has primary responsibility for retaining the record copy of the e-mail, usually the creator
- Retention – Determine e-mail retention periods for each record category
- Retention Procedures – Establish procedures to ensure that record copies of e-mail are retained for required retention periods and that they are deleted at the expiration of the retention period
- Retrieval – Develop organization-wide standardized names and filing rules for folders, business functions, document types, e-mail subject headings, etc.
- Review e-mail guidance at least annually to be sure it complies with current state and federal laws (and foreign laws if the organization operates internationally)
- Spam control – Install filters and provide employees instructions to manage
- Storage – Work with the IT department to provide a shared drive, backed up on the company's server, for storage of record copies of e-mail and communicate appropriate instructions to employees; determine media, facility, and procedures for intermediate, long-term, and off-site storage
- Virus checks – Provide employees with anti-virus software and instructions regarding method and frequency of conducting scans

What to Keep

E-mail messages, sent and received, are evidence of an organization's decisions, business transactions, and activities, and thus are official records. For e-mail sent by an organization's employees, the record copy[20] of an e-mail is usually the creator's original message. When an e-mail is received by an employee, the record copy is usually the one received by the primary addressee. In cases when e-mail has been replied to multiple times, the record copy is usually the last one if all the previous messages are included. The content of an electronic communiqué determines its status, just as it does when the communication is transmitted on paper. A complete copy of names and e-mail addresses for group distribution lists should be retained for legal and historical purposes. Metadata[21] is considered part of the record. (See Appendices.)

Affirmative answers to the following tests indicate that an e-mail is a record:

- Proves a business-related event or activity did or did not occur;
- Demonstrates a transaction;
- Identifies who participated in a business activity or had knowledge of an event;
- Has legal or compliance value;
- Supports facts you claim to be true, since the person with direct knowledge of the facts is not able to testify;
- Addresses a topic specifically covered by law or regulation.[22]

Examples of e-mail that could be considered records include:

- Agendas and meeting minutes including management teams, committees, and governing body
- Appointment calendars of executive-level daily appointments and activities; similar logs reflecting employee schedules, meetings, visitors, telephone calls
- Business transaction documentation
- Correspondence related to official business communications at the executive level to and from others inside and outside the organization
- Distribution list member names and e-mail addresses for each list
- Documentation of departmental and organizational decisions and operations
- Drafts of documents circulated for comment or approval. Those reflecting evolution of policies or programs and key factors in those decisions may be subject to subpoena and should be retained on a shared drive with subsequent revisions denoted by, e.g., "HR.Computer Use.Draft.Rev.1" or ".b", etc.
- Final reports or recommendations

---

[20] A record copy, also known as the official copy, contains information created or received in the course of conducting an organization's business. Its retention is determined by the organization's Records Management Policy and Records Retention Schedule.

[21] Metadata is electronic information, often referred to as a header, that is automatically produced for an electronic document, including subject, date created, sender, and recipients.

[22] Charlene Brownlee, and Melissa Cozart, "The Challenge of Electronic Records," *The Corporate Counselor, Law Journal Newsletters*. Vol. 20, No. 1 (June 2005) http://www.ljnonline.com/.

- Grant proposals, approvals, reports
- Legal and financial records
- Organizational charts
- Policy, program, and procedure directives issued by the organization's executive-level staff addressing organizational operations, key functions, mission goals, or issues of public interest such as manuals, bulletins, orders, rules, directives, policy statements
- Press releases
- Transmittal e-mails – messages containing no substantive information that are sent only to provide attachments. Because the authenticity of an e-mail requires retention of its metadata (the transmission data), transmittals may supply a key part of the record.
- Work schedules and assignments

E-mails generally **not** considered records include:

- Announcements of social events, e.g. retirement parties
- Drafts of documents without substantive changes
- Duplicate copies of messages
- Inter or intra-organization memoranda, bulletins, etc. for general information
- Personal messages not related to conduct of business (however, these could have historical value depending on the correspondent and subject)
- Portions of documents sent as reference or information-only copies
- Published reference materials
- Requests for information[23]

How Long to Keep Records

Each organization should determine how long to keep which records based on its particular mission and legal, financial, and regulatory requirements. It may be useful in making retention decisions to sort types of information into three categories – no value, limited value, and enduring value – and establish time periods to keep each group regardless of their form (paper or electronic). Remember to consider e-mail messages and attachments and metadata as one document.

Category 1 – E-mail messages of no value Retain: 0-30 days
Examples: SPAM
Personal
Electronic copies that have been printed out with metadata
Messages to/from distribution lists (Listservs) not business related
Copies of publications
Routine requests for information or publications
Informational e.g. holiday closings, charitable drives

[23] State of Washington, Division of Archives & Records Management, Office of the Secretary of State, "Guidelines for Developing Policy & Establishing Prodedures for E-Mail," <http://www.MERresource.com/libraryRecordsTechnologies/Email>.

Copies of internal messages if the recipient is not the primary addressee

Category 2 – E-mail messages with limited value Retain: Indefinitely
Examples: Reference Use--delete when no longer needed
Legal Use – until litigation is settled and appeal time expires
Administrative Use – Delete after 3 years

Category 3 – E-mail messages with enduring value Retain: Permanently
Examples: Policy and Program Use

Collaboration with the IT Department should determine how to route each category in order for data to be retained on the appropriate media. Both the Records Manager and IT contact should set up calendar reminders to migrate data from older media at regular intervals. Migration decisions should consider the possibility of metadata loss or alteration; keyword search capability; the inability to annotate files; the necessity to maintain operating systems and software that supports original file formats; and the difficulty in tracing file users and dates.[24]

Three terms unique to electronic records retention refer to the type of storage media, not to the length of time the informational content of a particular type of record should be retained. The Records Manager and Information Technology Manager should collaborate to determine which type of storage is appropriate for each category of record.

1) On-line retention period: usually refers to retaining data on magnetic disks for disaster recovery purposes, generally 1 week to 3 months.

2) Near-line retention period: data may remain on-site but on removable media such as CDs. Depending on the type of information contained, the records may be Category 1, 2, or 3. In the case of Category 3 records, the data may need to be migrated periodically to avoid loss of information from deteriorating media.

3) Off-line retention period: data may be stored off-site, typically on magnetic tapes. Like near-line retention, records in Category 3 should be transferred regularly to more permanent, stable media.[25]

[24] Mary Mack, "Native File Review: Simplifying Electronic Discovery?" in *Law Journal Newsletters Legal Tech Newsletter*, Vol. 23, No. 2 (May 2005) <http://www.ljnonline.com/alm?It>.

[25] David O. Stephens and Roderick C. Wallace, *Electronic Records Retention: New Strategies for Data Life Cycle Management*, Lenexa, KS: Arma International, 2003.

SECTION III

E-MAIL GUIDELINES FOR EMPLOYEES

E-MAIL GUIDELINES FOR EMPLOYEES

Initiating e-mail:

- Limit use of e-mail to official business
- Write in formal style, using salutations, e.g. "Dear Mr. Smith:"
- Use a closing signature consisting of your name, title, organization, address, telephone number, and e-mail address. Most e-mail programs provide an option for entering this information once for automatic attachment to all outgoing e-mail.
- Always use the spelling and grammar check feature and proofread for errors.
- Follow your department's subject heading name standards.
- When replying to a message, always put your response at the top of the sender's e-mail.
- Keep messages brief and to the point.
- Be considerate of other people's time by not answering e-mails simply to say "I agree" or "Thanks" unless it is important to let the sender know you received the message.
- Use blind copies judiciously and be aware that recipients could inadvertently "reply to all" including the person who received the blind copy.
- If confidential information must be sent via e-mail, follow departmental procedures regarding encrypting or marking as confidential.
- Do not write down your password and do not give it to other employees.

Managing, organizing, saving e-mail:

- Handle each e-mail only once.
- Delete immediately after reading any e-mails that are not considered records under your employer's Records Retention Policy.
- File those that are records immediately after reading in accordance with your organization's policy.
- Use file and folder names consistent with the organization's policy, e.g. folders titled "Grant.Thompson.Brazil" and "Board Minutes.2006."
- Regularly move e-mail no longer needed for active projects from the Inbox to "archive" folders according to your employer's Records Management Policy.
- Unless instructed otherwise, save e-mail on a drive that will be automatically captured in regular server backups. You may need to consult your Network Administrator or Records Manager to identify the appropriate drive.
- If you will not be checking your e-mail for longer than one day, set up an "out of office" automatic reply feature.
- Any e-mail transmitting an attachment that is considered a record should be retained in order to show that the attachment was sent, to whom, and when.
- Don't open attachments unless you are expecting them as viruses are often transmitted that way.
- Regularly run the anti-virus program your IT department offers.
- E-mail and attachments saved on laptops, removable devices such as flash, iPod, and offsite computers, should be transferred as soon as possible to a designated drive that is regularly backed up on the server.

- Log off when you will be away from your computer for more than a few minutes; at the end of the day, log off or shut down according to IT guidelines.

E-mail etiquette:

- Although humor or sarcasm will rarely, if ever, be part of a business e-mail, if you include either, identify it as such. Remember that one person's joke may be another's humiliation and could cause personnel action against you or a lawsuit.
- Avoid emotional responses. Give yourself at least several hours to calm down after receiving an upsetting e-mail before you respond. Compose and save your reply as a Draft, then edit and send after reflection.
- Do not forward or quote messages without permission of the author.

Unacceptable E-mail Use:

- E-mail with content or links that are threatening, obscene, repeated and unwanted, harassing, and/or racially, sexually, or ethnically offensive
- E-mail with content that slanders, libels, or defames anyone
- E-mailing software programs, audio, or video files from the Internet unless required for your job. If that is the case, discuss the issue with the IT Department as such large attachments could cause problems.
- Fraudulent e-mail
- Chain letters
- Sending work-related information to unauthorized recipients
- Sending or receiving software or other products outside of licensing agreements
- Using your employer's e-mail for personal use (including political, social, religious, recreational, financial gain)
- Accessing your personal e-mail account through your employer's system unless specifically allowed by the company's Records Management Policy
- Using ListServs or other discussion groups that are not work-related
- Unauthorized access of someone else's computer or mailbox
- Taking or accessing your employer's data outside your workplace without your department head's approval
- Revealing confidential business information
- Interfering with or attempting to interfere with others' access to computer use or in any other way to damage the organization (including launching computer viruses, worms, or engaging in criminal activity)
- Using e-mail for illegal or unethical activities

APPENDIX 1

GLOSSARY

Active record: A record used frequently in conduct of daily business.

Archival record: a record with legal, financial, administrative, or research value that should be kept permanently.

Audit Trail: a record of what operations have been performed on a computer system. It includes user identification as well as time and date information.

Authenticity: a record is what it purports to be and has not changed since its creation. Authentic e-mail requires the e-mail message as well as any attachments and its transmission data.

Convenience copy: a copy of a record kept for reference and quick access.

Discovery: legal process in which one party to a lawsuit is required to furnish documents requested by the opposing side.

Document management system: computer software that files, routes, and retrieves documents created electronically regardless of the document's original format (Word, Excel, etc.).

Electronic Communications Privacy Act (ECPA): federal law that defines invasion of privacy regarding electronic communication, including e-mail, cellular telephones, pagers, etc.

Electronic record: information created or stored in an electronic form that provides evidence of activities, events, decisions, programs, policies, or transactions.

Encryption: method of hiding electronic information by encoding it so that only authorized persons who have the decryption code may access the data.

Enterprise Content Management (ECM): use of technology to manage an organization's information flow from creation through storage. The term typically is used when referring to a company that provides software that captures, preserves, and retrieves electronic records. ECM also often includes management of digital rights, web content, and records retention.

Format: type of computer file, e.g. Microsoft Excel or JPEG image.

Information Technology (IT): the system that handles information generated or stored through computers and telecommunications. Also known as Information Services (IS) or Management Information Services (MIS).

Integrity: confirmation that a record has not been altered, intentionally or accidentally, since its creation or receipt.

Life Cycle Management: retaining or destroying documents when they reach a pre-determined age and in accordance with government regulations, legal or financial guidelines, or an organization's internal policies regarding records retention.

Metadata: data automatically produced for an electronic document that describes its subject, date created, sender, recipients, etc.

Migration: transferring data from one electronic media to another, usually from older technology to newer. This is done to preserve information that might otherwise be lost as the data's old format or media deteriorates or becomes obsolete.

Near-line storage: storing information in an electronic format apart from the e-mail system, such as on a desktop computer's hard drive or a shared drive. E-mail remains somewhat functional.

Official copy (also known as record copy): original record or a copy that is retained in compliance with an organization's Records Management Policy and Records Retention Schedule. If the e-mail is created within the organization, the sender usually maintains the official copy. When it is received from outside the organization, the primary recipient usually holds the official record.

Official record: information created or received in the course of conducting an organization's business.

Off-line storage: storing information outside an electronic environment, such as in paper copies, magnetic tape, optical disk, or computer-output-to-microfilm.

On-line storage: storage of e-mail, metadata, and attachments within the e-mail system currently being used by an organization. E-mail remains fully functional, i.e., it can still be forwarded, replied to, etc.

Record: formal or informal information generated within an organization or received by it during its course of business. A record may be in various forms, printed or electronic: book, CD/DVD, e-mail, instant message, map, memory card or stick, handwritten notes, memos, and sketches, photograph or other image, spreadsheets, audio or video tape, voice mail.

Records Management Application (RMA) or Records Management System (RMS): electronic document management system with an added feature that applies the organization's retention schedule to determine how long to retain a particular record. The purchasing organization usually works with the software provider to assign recognition identifiers (such as keywords in e-mail subject headings) and retention criteria.

Records Management Policy: a formal, written document containing an organization's procedures for managing records of its activities. It typically includes guidelines regarding which records to retain, the length of time they should be kept, the manner in which they should be organized, and the procedures for disposing of them or transferring them to an archive.

Records Management System: See Records Management Application.

Records retention schedule: a list of the organization's records by record type that indicates how long each type should be retained.

Retention period: the organization's pre-determined 'expiration' dates – the point in time when a record may be destroyed. Financial, legal, and governmental requirements, in addition to the organization's administrative needs and the historical value of the records, are considerations in establishing retention periods.

Spoiliation: destruction of records pertinent to lawsuits or regulatory body investigations, or potential suits or investigations.

APPENDIX 2

E-MAIL AND INTERNET POLICY ACKNOWLEDGEMENT

I will not use e-mail, the Internet, or other employer-provided electronic access for illegal, unethical, unprofessional, or personal purposes.

I will not allow others to use my login or password. During my absence, trusted staff members requiring access to my files and mail may be delegated those rights. When I am given temporary rights to a colleague's e-mail, I agree to maintain the confidentiality of their e-mail.

I understand that my use of e-mail and the Internet may be monitored and that I am responsible for all activity on my computer, e-mail account, and network access under my user name.

I understand that my e-mail is the property of my employer, that it is not personal and private, and that it may be subject to legal discovery.

I will follow procedures outlined in the E-mail and Internet Policy to maintain system security and to prevent unauthorized access to private or confidential information.

If I receive suspicious, threatening or harassing e-mail, or suspect that my system has been sent e-mail containing harmful material such as worms or viruses, I will immediately notify the Information Systems manager.

If I have reason to believe another employee is engaging in unauthorized use of e-mail or the Internet, I will immediately advise my supervisor, Human Resources, and the Information Systems manager.

When I leave this organization's employment, I will ensure that my e-mail messages are handled in accordance with my employer's E-mail and Internet Policy .

I understand that I am responsible for complying with the policies above. I affirm that I have received, read, and understand my employer's E-mail and Internet Policy and will abide by the terms and conditions of this policy.

I understand that failure to do so can result in immediate suspension of network access as well as disciplinary action or termination of employment.

Print Name: _____

Signature: _____

Title: _____ Date: _____

APPENDIX 3

FOR ADDITIONAL INFORMATION

Association for Information and Image Management. <http://www.aiim.org>.

Association of Records Managers and Administrators. <http://www.arma.org/>.

Balousek, Marv. "Private Companies, Nonprofits Can't Ignore SOX: Federal Law Mandates Document Retention, Other Internal Controls." *Wisconsin State Journal*, 1 May 2005.

Brownlee, Charlene and Melissa Cozart. "FTC Issues Rules for Disposal of Consumer Report Information." *Legal Update*. Fulbright & Jaworski, L.L.P. May 2005.

_____. "The Challenge of Electronic Records." *The Corporate Counselor, Law Journal Newsletters*. Vol. 20, No. 1 (June 2005) <http://www.ljnonline.com>.

Bushell, Sue. "Juris E-Prudence." CIO. 19 October 2005 <http://www.cio.com.au/pp.php?id=561063778&fp=16&fpid=0>.

Cresci, Gregory. "Morgan Stanley to Pay $15 Million for Failure to Save E-Mails." Bloomberg 14 February 2006. <http://www.bloomberg.com/apps/news?pid=10000103&sid=aBoVvwOm0I6I&refer=us>.

Dearstyne, Bruce W. *Effective Approaches for Managing Electronic Records and Archives.* Lanham, MD: Scarecrow Press, 2002.

Duranti, Luciana, ed. *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*. San Miniato, Italy: Archilab, 2005.

Epstein, Jonathan D. "Tougher Accountability Rules are Impacting Nonprofit Groups." *Buffalo News*, 5 December 2004.

Flynn, Nancy. *The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies*. New York: American Management Association (AMACOM), 2001.

_____ and Randolph Kahn. *E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication*. New York: American Management Association (AMACOM), 2003.

Foley & Lardner LLP. "Foley & Lardner Study Finds, Despite Intentions of Public Company Governance Reforms, Many Private and Nonprofit Organizations Continue to Be Impacted." *Business Wire*, 9 March 2005.

Graduate School of Library and Information Science, University of Texas at Austin. "Managing E-Mail as Records." <http://www.gslis.utexas.edu/~scisco/lis389c.5/email/public.html>.

Huth, Geof. "Managing E-Mail Effectively." Albany, NY: University of the State of New York, 2002 <http://www.archives.nysed.gov/altformats/ServicesGovRecs/ns_Serv_mg_pub62.pdf>.

Hymowitz, Carol. "In Sarbanes-Oxley Era, Running a Nonprofit is Only Getting Harder." *Wall Street Journal*, 21 June 2005.

Independent Sector. <http://www.independentsector.org/>.

Keneally, Kathryn. "E-mails sent during the business day may not be admissible as business records." *Champion Magazine*, January/February 2004 <http://www.nacdl.org/public.nsf>.

Kinzie, Susan and Valerie Strauss. "After AU, Colleges Increase Scrutiny: Scandal Heightens Efforts to Seek Advice, Ask for New Audits." *Washington Post*, 21 November 2005.

LeClaire, Jennifer. "The Future of E-Mail Archiving." *TechNewsWorld,* 13 October 2005 <http://www.technewsworld.com/story/46481.html>.

Leddin, Brian J. and Dean Gonsowski. "Spoliation of Electronic Data: The Wages of Sin in a Virtual World." *New Jersey Law Journal*, Vol. CLXXIX, No. 3.

Mack, Mary. "Native File Review: Simplifying Electronic Discovery?" *Law Journal Newsletters Legal Tech Newsletter*, Vol. 23, No. 2 <http://www.ljnonline.com/alm?It>.

Murray, Stefanie. "Management of records more important than ever." *Lansing State Journal*, 13 October 2005 <http://www.tallahassee.com/mld/tallahassee/busiess/12888528.htm?template=contentModules/printstory.jsp>.

National Archives and Records Administration. "Electronic Records Management Guidance on the Web." <http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html>.

National Electronic Commerce Coordinating Council, Analysis of State Records Laws Work Group. "Challenges in Managing Records in the 21st Century." Lexington, KY: NECCC, 2004 <http://www.ec3.org/Downloads/2004/Challenges_in_El_Records.pdf>.

_____, Digital Case Law Work Group. "Effectively Managing the Discovery of Electronic Records: Current Learning and Suggested Best Practices." Lexington, KY: NECCC, 2004 <http://www.ec3.org/Pubs/PubWGPapersYr.htm>.

_____. "Managing E-Mail." Presentation at the NECCC Annual Conference, December 4-6, 2002, New York, NY. Lexington, KY: NECCC, 2002 <http://www.ec3.org/Downloads/2002/managing_email.pdf>.

National Library of Australia. *Guidelines for the Preservation of Digital Heritage*. Canberra: UNESCO, 2003 <http://www.naa.gov.au/recordkeeping>.

"Privacy& Data Protection." *The Legal Reporter, Law Journal Newsletters*. Vol. 1, no. 1 (November 2005) <http://www.ljnonline.com/alm?privacy>.

Sedona Conference. "The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age." Sedona, AZ: The Sedona Conference, September 2005.

Silverberg, David. "E-mail Retention Reaching Critical Mass." *Business Edge*, Vol. 1, No. 21 (27 October 2005) <http://www.businessedge.ca/printArticle.cfm/newsID/10991.cfm>.

Spitzer, Eliot. "Internal Controls and Financial Accountability for Non-Profit Boards." Charities Bureau, State of New York. <http://www.oag.state.ny.us/charities/charities.html>.

State of Washington, Division of Archives & Records Management, Office of the Secretary of State. "Guidelines for Developing Policy & Establishing Procedures for E-Mail." <http://www.MERresource.com/libraryRecordsTechnologies/Email>.

Stephens, David O. and Roderick C. Wallace. *Electronic Records Retention: New Strategies for Data Life Cycle Management*. Lenexa, KS: ARMA International, 2003.

"The Next Challenge for Nonprofits." *NJBIZ*, 19-26 December 2005.

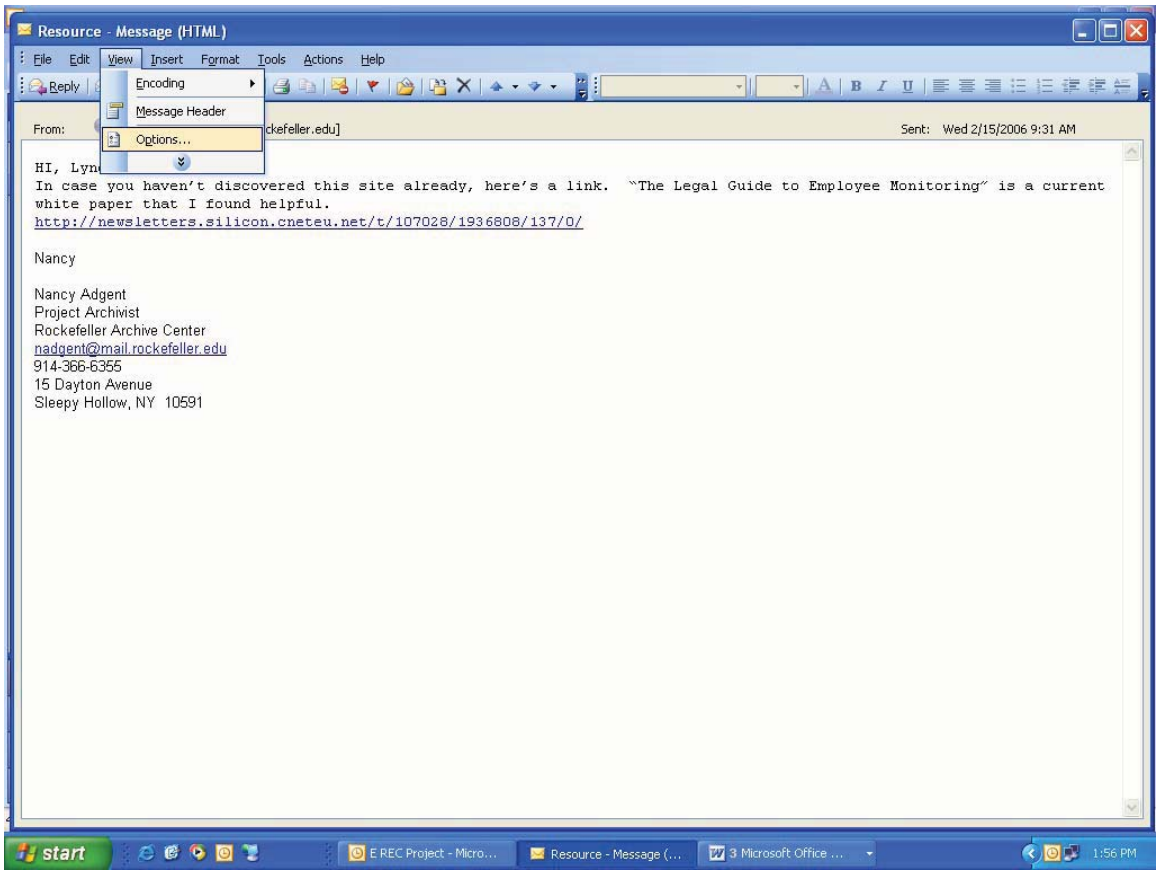
U.S. Department of Health and Human Services. "HIPAA." <http://www.dhhs.gov/ocr/hipaa.html>

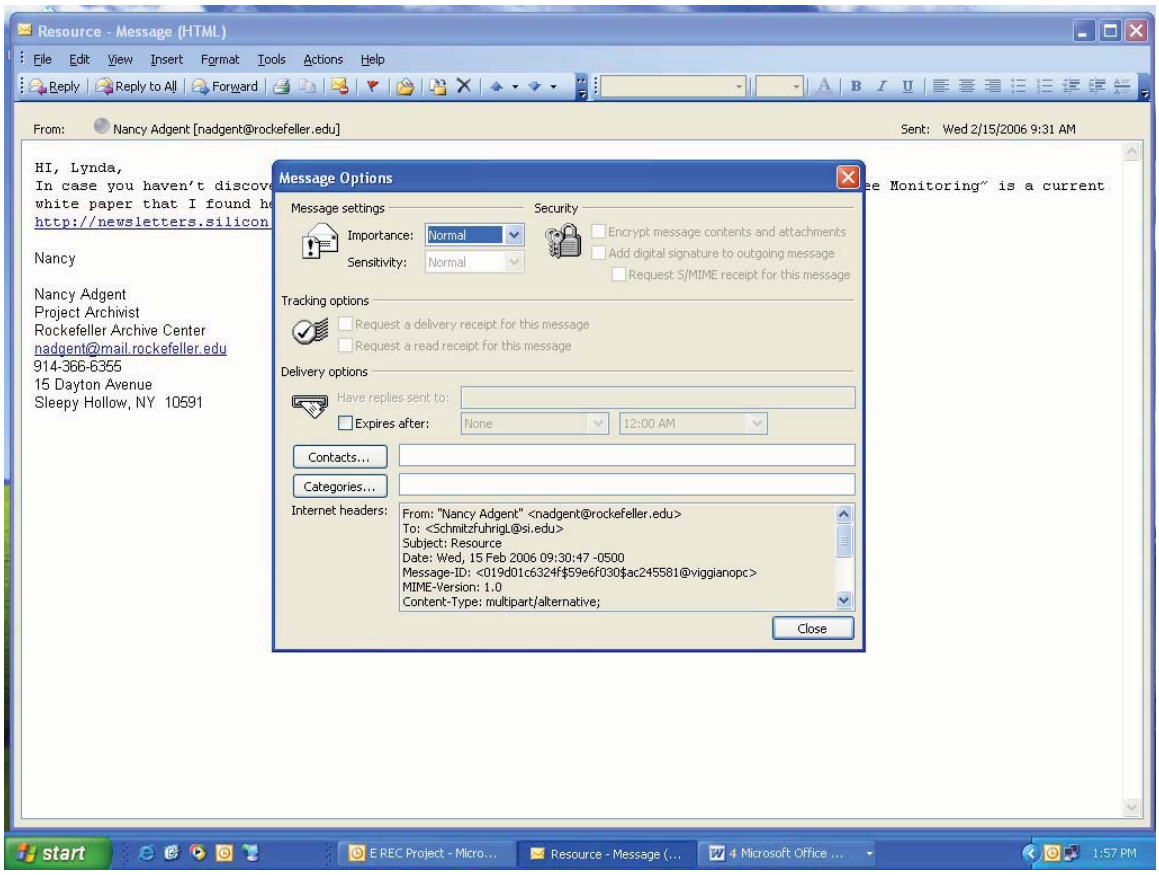
U.S. Department of Treasury, Internal Revenue Service. "Tax Information for Charities & Other Non-Profits." <http://www.irs.gov/charities>.

U.S. Internet Industry Association. <http://www.usiia.org>.

APPENDIX 4

SAMPLE E-MAIL HEADER (METADATA)





From the Internet Headers box:

From: "Nancy Adgent" <nadgent@rockefeller.edu>
To: <SchmitzfuhrigL@si.edu>
Subject: Resource
Date: Wed, 15 Feb 2006 09:30:47 -0500
Message-ID: <019d01c6324f$59e6f030$ac245581@viggianopc>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0199_01C63225.7110E830"
X-Mailer: Microsoft Office Outlook, Build 11.0.6353
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
Thread-Index: AcYyPGloBfD29AUjSFCKgkkFLbZA+w==
X-OlkEid: E6C44722424AB3623858174E88512873FB698596