

Disclaimer and Terms of Use



No part of this e-book may be reproduced or transmitted in any form or by any means whatsoever, mechanical or electronic, including photocopying and recording, or by any information storage and retrieval system, without the express written, dated and signed permission from the author.

This e-book is © copyrighted by Quality Assurance Solutions and contains material protected under International and Federal Copyright Laws and Treaties. Any unauthorized reprint or use of this material is prohibited.

The author and publisher of this e-book have used their best efforts in preparing this material. The author and publisher make no representation or warranties with respect to the accuracy, applicability, fitness, or completeness of the contents of this e-book.

The author and publisher disclaim any warranties (express or implied), merchantability, or fitness for any particular purpose. The author and publisher shall in no event be held liable to any party for any direct, indirect, punitive, special, incidental, or other consequential damages arising directly or indirectly from any use of this material, which is provided "as is", and without warranties.

No guarantees of income or success are made. The reader assumes all responsibility for the use of information contained herein. The author reserves the right to make changes without notice. The author and publisher assume no responsibility or liability whatsoever on the behalf of the reader of this e-book.

[table of contents](#)

Corporate Email Policy

[table of contents](#)

Background



Company equipment and information in any form is considered an asset of the company and thus must be properly used and adequately protected. This includes the transmission of information over computer communication networks. In addition, the use of computing and technology investments must be for legitimate company business purposes except for personal use deviations outlined in this document.

The purpose of these Guidelines/Policy is to assure that:

1. E-mail will be used by company representatives in an ethical and considerate manner in compliance with applicable law and policies, including policies established by the company.
2. E-mail users are informed about how concepts of privacy and security apply to e-mail, as well as the applicability of relevant policy and law.
3. Disruptions to company e-mail and other services and activities are minimized.

Corporate Email Policy

Scope

Applies to:

1. All e-mail services provided, owned, or funded by the company.
2. All users and holders of company e-mail systems or accounts, regardless of intended use.
3. All company e-mail official records in the possession of or generated by company employees and other users of e-mail services provided by the company, regardless whether the records were generated on company or non-company computers.
4. Applies equally to transmission and receipt data including e-mail headers, summaries, and addresses associated with e-mail records and attached files or text.

Does Not Apply to:

1. Internet services other than e-mail.
2. Voice Mail.
3. Audio and Video Conferencing.
4. Facsimile messages.

[table of contents](#)

Corporate Email Policy

Specific Usage Criteria

1. E-mail services are extended for the sole use of company staff, and other appropriately authorized users to accomplish tasks related to and consistent with the company's mission. Company e-mail systems and services are company facilities, resources and property. Any e-mail address or account assigned by the company to individuals or functions of the company, is the property of the company.
2. Usage Restrictions:
 - a) E-mail users are required to comply with state and federal law, company policies, and normal standards of professional and personal courtesy and conduct. Access to company e-mail services is a privilege that may be wholly or partially restricted by the company without prior notice and without the consent of the e-mail user:
 - I. when required by and consistent with applicable law or policy.
 - II. when there is a reasonable suspicion that violations of policy or law have occurred or may occur.
 - III. when required to meet time-dependent, critical operational needs.
 - b) Company operational units may define additional "Conditions of Appropriate Use" for local computing and network facilities to supplement this document with additional detail, guidelines or restrictions. These "Conditions" must be consistent with and subordinate to this document, and are intended to deal primarily with situations of limited resource supply.
 - c) When an individual's affiliation with the company ends, the company may attempt to forward e-mail for a reasonable period of time as determined by the company for purposes

Corporate Email Policy

consistent with this document and the company's mission. The company may elect to terminate the individual's e-mail account or continue the account.

Authorized Access and Disclosure

1. The company may permit the inspection, monitoring, or disclosure of e-mail when:
 - a) Required by or consistent with applicable law or policy such as any appropriately issued subpoena or court order. The Electronic Communications Privacy Act of 1986 also permits messages stored on company systems to be accessed by authorized personnel in certain circumstances.
 - b) There is a reasonable suspicion that violations of law or company policy have occurred or may occur.
 - c) There are time-dependent, critical operational needs of company business if the company determines that the information sought is not more readily available by other means.
3. In such instances, the company will, as a courtesy, normally try to inform e-mail users prior to any inspection, monitoring, or disclosure of e-mail records, except when such notification would be detrimental to an investigation of possible violation of law or company policy. Users are required to comply with company requests for access to and copies of e-mail records when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the company. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate company personnel policies or Codes of Conduct.

Corporate Email Policy

Indemnification of the Company

Users agree by virtue of access to the company's computing and e-mail systems, to indemnify, defend and hold harmless the company for any suits, claims, losses, expenses or damages, including but not limited to litigation costs and attorney's fees, arising from or related to the user's access to or use of company e-mail and computing systems, services and facilities.

Instances of Illegal and Misuse

1. Using e-mail for illegal activities is strictly prohibited. Illegal use may include, but is not limited to: obscenity; child pornography; threats; harassment; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; attempting to intercept any electronic communication transmissions without proper authority; and violation of copyright, trademark or defamation law.
2. Failure to follow state law with regard to the disposition of e-mail records may lead to criminal charges. Theft or unauthorized destruction, mutilation, defacement, alteration, falsification, removal or secretion of e-mail records may lead to criminal charges.
3. In addition to illegal activities, the following e-mail practices are expressly prohibited: entry, examination, use, transfer, and tampering with the accounts and files of others, unless appropriately authorized pursuant to this policy; altering e-mail system software or hardware configurations; or interfering with the work of others or with company or other computing facilities.
4. If a user has been requested by another user via e-mail or in writing to refrain from sending e-mail messages, the recipient is prohibited from sending that user any further e-mail messages until such time as he/she has been notified by

Corporate Email Policy

the system administrator that such correspondence is permissible. Failure to honor such a request shall be deemed a violation of this document.

5. Company e-mail services may not be used for: commercial activities not approved by appropriate supervisory company personnel consistent with applicable policy; personal financial gain; personal use inconsistent with Section: "Personal Use" of this document; uses that violate other company policies or guidelines; or uses inconsistent with applicable state or federal law. Applicable company policies include, but are not limited to, policies and guidelines regarding personnel, intellectual property, or regarding sexual or other forms of harassment.
6. E-mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements of behalf of the company or any unit of the company unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of the company."
7. Company e-mail services shall not be used for purposes that could reasonably be expected to cause, directly, or indirectly, strain on any computing facilities, or interference with others' use of e-mail or e-mail systems. Such uses include, but are not limited to, the use of e-mail services to:
 - a) Send or forward chain letters. **Special note and refrain** should be paid to the circulation of chain letters. This activity causes a dramatic increase in the allocation of disk space to user data, a dramatic increase in the likelihood of a computer virus attack, and places a strain on resources that could result in deteriorating message delivery and response time or, even worse, system unavailability.

Corporate Email Policy

- b) "SPAM", that is, the widespread distribution of unsolicited e-mail.
- c) "Letter-bomb", that is, to resend the same e-mail repeatedly to one or more recipients.

Personal Use

Company e-mail services may be used for incidental personal purposes provided that such use does not:

1. Directly or indirectly interfere with the company operation of computing facilities or e-mail services.
2. Interfere with the e-mail user's employment or other obligations to the company.
3. Violate this Policy, or any other applicable policy or law, including but not limited to use for personal gain, conflict of interest, harassment, defamation, copyright violation or illegal activities.
4. E-mail messages arising from such personal use shall, however, be subject to access consistent with this policy or applicable law. Accordingly, such use does not carry with it a reasonable expectation of privacy.

Corporate Email Policy

Confidentiality

1. The confidentiality of e-mail cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including this Policy, by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access. Users, therefore, should exercise extreme caution in using e-mail to communicate confidential or sensitive matters, and should not assume that their e-mail is private or confidential.
2. Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information, regardless whether the information is maintained on paper or whether it is found in e-mail or other electronic records.

Security and Preservation

- 1) E-mail users and operators must follow sound business practices in providing for the security of e-mail records, data, applications programs, and systems under their jurisdiction.
- 2) Users and operators must guard against storage media deterioration and e-mail record inaccessibility due to hardware or software obsolescence. To eliminate these situations, users must make provision for future accessibility by:
 - a) Migrating all official e-mail records to the next generation of hardware or software; or
 - b) Migrating only current official e-mail records to new hardware or software, or converting official e-mail records not migrated to other media (e.g., optical disk) for short term storage or to "eye readable form" (i.e., paper or microfilm) for long term storage and preservation.

Corporate Email Policy

- 3) Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized. Each user is responsible for all e-mail transactions made under the authorization of his or her ID, and for all network e-mail activity originating from his or her workstation. Use of e-mail user identifications for commercial purposes is prohibited. Access to user identifications may not be loaned or sold.
- 4) Each operational unit should establish:
 - a) Standards for official e-mail records identification and file organization.
 - b) Measures for protecting sensitive official e-mail stored electronically.
 - c) Procedures for file back-up.

Violations

Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. Violations will be processed by the appropriate company authorities and/or law enforcement agencies. Violations may result in revocation of e-mail service privileges; Code of Conduct proceedings; disciplinary action up to and including dismissal; referral to law enforcement agencies; or other legal action.

Corporate Email Policy

General Use Cautions

1. Both the nature of e-mail and the public character of the company's business make e-mail less private than users may anticipate. For example, e-mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an e-mail message posted on an electronic bulletin board intended only for the originator of the message may be distributed to all subscribers. Furthermore, even after a user deletes an e-mail record from a computer or e-mail account it may persist in whole or in part in system logs, in the directories of the person who received the message, or on system back-up tapes which may be retained for long periods of time. All these items may be subject to disclosure under applicable law and this Policy. The company cannot routinely protect users against such eventualities.
2. E-mail, regardless whether created, received, or stored on company equipment, may be subject to disclosure or access under laws or as a result of litigation
3. The company does not automatically comply with all requests for disclosure, but attempts to evaluate such requests against the precise provisions of the applicable law concerning disclosure and privacy.
4. The company, in general, cannot and does not wish to be the arbiter of the contents of e-mail. Neither can the company, in general, protect users from receiving e-mail they may find offensive. Members of the company community, however, are strongly urged to use the same personal and professional courtesies and considerations in e-mail as they would in other forms of communication, and particularly those applicable to written communications since e-mail creates a tangible record of that communication.

Corporate Email Policy

5. There is no guarantee, unless "authenticated" e-mail systems are in use, that e-mail received was in fact sent by the purported sender, since it is relatively easy, although a violation of this Policy, for senders to disguise their identity. Furthermore, e-mail that is forwarded may also be modified. Authentication technology is not widely and systematically in use at the company as of the date of this Policy. As with print documents, in case of doubt, receivers of e-mail messages should check with the purported sender to validate authorship or authenticity.
6. Encryption of e-mail is another emerging technology that is not in widespread use as of the date of this Policy. This technology permits the encoding of e-mail so that for all practical purposes it cannot be read by anyone who does not possess the right decryption key.
7. Inappropriate e-mail use may expose the company and individual users to claims for damages through copyright infringement, libel, breach of privacy or other personal or proprietary rights.
8. Federal law and company policies regarding copyright and intellectual property apply to e-mail. Do not violate the copyright of others. Unless the material is legally established as being in the public domain or unless there is explicit release by the copyright owner, you may not copy e-mail information.
9. Even though an e-mail sender and recipient have deleted their e-mail, back-up copies may exist for periods of time and in locations unknown to the originator or recipient. These copies may be accessed or disclosed consistent with applicable policy or law.

Corporate Email Policy

E-mail Best Practices

Your support of the following "best practices" will assist us in providing you with fast and reliable electronic mail service:

General

- Respect the business purpose for which computers and access to communication network(s) has been granted.
- Use the computer resource capabilities in a manner that minimizes cost to the company while maximizing value for company business purposes.
- Mail folders should not be used as long term (more than a year) filing systems. Sent e-mail and Inbox folders should be kept current (regular frequency of deleting and/or filing).
- To avoid proliferation of "junk" e-mail, do not reply to "junk" e-mail or provide your e-mail address in Internet chat rooms or discussion groups.
- When using web based e-mail (e.g., Outlook Web Access), be sure to logoff and close your browser session when exiting the program. This will prevent someone from accessing your e-mail with cached credentials when using a public device (such as a kiosk or computer).

For Senders

- Do not transmit any obscene, lewd, or pornographic material. This is strictly prohibited.
- Personal messages should not be widely distributed utilizing company e-mail services. This is an inappropriate use of company resources.

Corporate Email Policy

- The company provides electronic mail systems to employees, at company expense, for company business purposes. The company electronic mail systems should not be used to send chain letters, games, sounds, wallpaper, bitmaps or other non-business related items through the e-mail as attachments.
- Do not use e-mail as a means to solve a problem when a phone conversation could be more effective. Consider following up an e-mail with a phone call.
- E-mail should be used as a communication medium not as a collaboration tool. If multiple reviews, responses, markups are needed, use the appropriate collaboration tool or Network drive, as appropriate.
- Avoid emotional overtones in your e-mail such as anger or sadness. It is best to wait before sending out such e-mail until after a "cooling off" period and another review of your message.
- Avoid sending e-mail that may contain controversial subject matters. Once again, a phone call will have far better results.
- Use capitalization of entire words only to highlight an important point. WHEN PEOPLE SEND AN ENTIRE MESSAGE IN CAPS, we generally perceive it as someone yelling or upset.
- Proofread e-mails before sending them.
- Use the spell check feature routinely.
- Use distribution lists cautiously. Send e-mail messages only to recipients who need the information.
- Be succinct! The most effective e-mail messages are short and to the point.

Corporate Email Policy

- Keep the message focused on a single topic.
- Include a subject line that helps the recipient prioritize, file, and search messages.
- Tag messages appropriately – do not label messages "High Priority" or "Urgent" unless required.
- Do not use delivery and read receipts for general e-mail use. Only use these for important messages requiring receipts.
- Do not broadcast someone else's message without permission.
- Choose the number and size of file attachments with great care. The entire e-mail message cannot exceed 10 Megabytes. Check the size of a file before attaching it to a message. Before sending an attachment over 4 megabytes (MB) in size, consider other delivery options, e.g., File Transfer Protocol (FTP). All large attachments should be zipped using file compression software, e.g. Winzip. The combined size of multiple attachments can also impact e-mail delivery. Multiple small attachments should be zipped together as one file. Larger attachments should be zipped and sent individually. Messaging gateways process a set amount of data per hour. The available bandwidth can fill up with large attachments thus slowing or stopping the movement of other e-mail.
- Broadcasts to an "Everyone" e-mail group should be in support of Company business purposes, be used only where large groups of people would have an interest, and where targeting individual addresses would be too labor intensive or prone to error. Make such broadcasts only selectively and rarely.
- Address e-mail according to the expected action – list people in the "To" field if they should respond, and in the "cc" field if

Corporate Email Policy

they should read the message as information only. Take care not to overuse the "cc" option.

- Avoid using blind courtesy copy addressees as they could unknowingly forward your e-mail and "reveal" themselves.
- Consider use of message formatting because the recipient's e-mail system may not display the message as intended by the sender. Do not depend on alignments, fonts, or colors to make a point.
- Consider file attachment compatibility for the recipient.
- Use e-mail communications when it is the most cost effective means. For example for overseas communication or to reduce or eliminate paper distribution.
- Licensed application software should never be e-mailed as an attachment. This not only is an inappropriate use of company resources, it is contrary to the company's software licensing policy.
- Large distribution lists can also delay e-mail delivery. If any recipients are on a non-company e-mail system, e.g., Lotus Notes, cc:Mail, Internet, limit distribution to 30 names, or less, per message. Divide large distribution lists and send the message multiple times, if necessary.

For Recipients

- Develop a regular schedule for using e-mail.
- Delete messages no longer needed.
- File important messages into organized folders or "save to" project related data repositories.
- Browse the subject line to identify important messages.

Corporate Email Policy

- Reply or acknowledge receipt of messages promptly if the originator expects a response.
- Use auto-replies or delegate authority when unable to check e-mail.
- Do not reply to all recipients unless they all need to see your reply.
- Request removal from unwanted distribution lists.
 - Do not respond to e-mail (subscribe or unsubscribe) from non-company distribution lists that are from unknown sources. The sender may be using your unsubscribe e-mail to send you more undesired information/SPAM.
 - Avoid opening e-mail attachments from an unknown or untrustworthy source, or with a suspicious or unexpected subject line. If in doubt, do not open the attachment. Immediately contact the IT Dept.
 - Attachments are also a major contributor to corruption of user e-mail files. The more attachments stored in the user's e-mailbox file, the greater the chance of corruption. Attachments that must be retained should be saved to the user's local drives or, to home or group drives on the server (preferably after being virus scanned).