# INTRODUCTION AND PURPOSE

This Electronic Mail Addendum (the “Addendum”) is intended as a supplement to the Handbook to which it is attached, and it clarifies the applicability of certain laws, as well as certain of Acme’s internal policies as they relate specifically to *electronic mail*.

The purpose of this Addendum is to assure that: (i) email will be used by you in an ethical and considerate manner in compliance with applicable law and policies, including those policies established by Acme; (ii) you are informed about how concepts of privacy and security apply to email, as well as the applicability of relevant policy and law; and (iii) disruptions to Acme’s email and other services and activities are minimized.

# Application to Other Policies

All policies applied generally at Acme should, when context permits, expressly apply to the digital world. This means that you must be careful to consider other Company policies in conjunction with your participation in the digital world, such as email. For example, if you were to use your email while at work to send what might otherwise be a legitimate work related email, but then include an offensive joke, such an email would run afoul of the Company’s anti-harassment policies. Or, if you were to send to an outsider an email which included Confidential Information of the Company that the third-party had no legitimate right to see, that email would violate Acme’s confidentiality requirements. You get the point.

# SCOPE

This Addendum applies to:

• All email services provided, owned, or funded in part or in whole by Acme.

• You, as well as all users and holders of Acme’s email systems or accounts, regardless of intended use.

• All private email accounts/services belonging to you, but which you might access while you’re using the Company’s Electronic Equipment, or while you’re engaging in services for which you will be compensated by the Company.

• All Acme’s emails, official records, and/or public records created, viewed, or accessed while performing your job duties with the Company or are using the Company’s Electronic Equipment, regardless whether the records were generated on Company owned computers or equipment.

This Addendum does NOT apply to:

• Internet services other than email.

• Voicemail.

• Audio and video conferencing.

• Faxes.

This Addendum applies equally to transmission and receipt data, including email headers, summaries, and addresses associated with email records and attached files or text.

# SPECIFIC USE PROVISIONS

Email addresses and/or services may be provided to you solely for your use to accomplish tasks related to and consistent with your job duties. Company email systems and services belong to Acme. Any email address or account assigned to you by Acme (whether assigned to you by another employee or the Company’s independent contractors) shall at all times belong solely to Acme, with all rights vesting solely in the Company.

At all times, you are required to comply with state and federal law, and if not in conflict with such laws, Acme’s internal policies, including those not specifically set forth in this Addendum. You should at all times exercise the normal standards of professional and personal courtesy and conduct while using email while on Company time, on the Company’s Electronic Equipment, and/or in conjunction with Company business. Access to Acme’s email services is a privilege that may be wholly or partially restricted by the Company without prior your prior notice or consent.

Acme reserves the right to inspect, monitor, disclose, or share any emails generated or received on email accounts owned by Acme. Likewise, at certain times, Acme may permit the inspection, monitoring, or disclosure of your private (non-business related) emails generated on the Company’s Electronic Equipment to third-parties. Instances where the Company might permit such inspection, monitoring, or disclosure may include, without limitation, any one of the following:

• When disclosure is required by or consistent with applicable law or policy, or any appropriately issued subpoena or court order.

• When there is a reasonable suspicion that violations of the law or of one or more of Acme’s policies have occurred or may occur.

• When there are time-dependent or it is critical to the operational needs of the Company.

In such instances, Acme may, as a courtesy only, and at its sole discretion, inform you prior to any inspection, monitoring, or disclosure of email records, except when such notification would be detrimental to an investigation regarding a violation of the law or Company policy.

# misuse

Using email for illegal purposes is strictly prohibited. Illegal purposes may include, without limitation, any of the following: (i) obscenity; (ii) child pornography; (iii) threats; (iv) harassment; (v) theft; (vi) attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; (vii) attempting to intercept any electronic communication transmissions without proper authority; and (viii) violation of copyright, trademark or other intellectual property laws. This is not an exhaustive list. You are tasked with using common sense. Whether or not you actually know that your conduct in a particular instance is illegal or unethical is irrelevant. Failure to follow federal or state law with regard to the disposition of email records may lead to civil liability and/or criminal charges, as might an employee’s theft or unauthorized destruction, mutilation, defacement, alteration, falsification, removal, or secretion of email records.

At no time are you ever permitted to directly or indirectly use a false identity or forge/attempt to forge any portion of an email. You may use an alias (an alternative name or electronic identification for oneself), so long as the pseudonym clearly does not constitute a false identity. You may not send email anonymously (i.e., when the sender’s name or electronic identification are hidden).

In addition to activities that violate federal or state law, you are strictly prohibited from using the Company’s email services to do any of the following:

• Enter, examine, use, transfer, or tamper with someone else’s accounts and files.

• Alter any software or hardware configurations on systems owned by the Company unless doing so is part of your normal job duties.

• Interfere with the work of others or someone else’s Company email accounts.

• Engage in commercial activities unrelated to your job duties for the Company.

• Violate other Company policies.

• Interfere with Acme’s other Electronic Equipment (e.g., cause any strain on any computing facilities).

• Give the impression that you are representing, giving opinions, or otherwise making statements on behalf of Acme unless expressly authorized to do so.

• Send or forward chain letters.

• Produce, send, or forward emails known as “Spam,” or any other type of widespread distribution of unsolicited mail.

• “Letter-bomb” (e.g. to resend the same email repeatedly to one or more recipients) anyone else.

# CONFIDENTIALITY

Acme cannot and does not assure the confidentiality of your emails, and you must therefore understand that confidentiality may be compromised even by access consistent with applicable law or policy, including this Addendum (and including Acme’s absolute right to monitor and review the contents of all emails made or received on Company Electronic Equipment), by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access. You should therefore always exercise extreme caution in using email to communicate confidential or sensitive matters. At no time should you ever assume that any of your emails accessed while at work will be or remain private or confidential.

You may not access, use, or disclose Confidential Information without appropriate authorization, and you must take necessary precautions to protect the confidentiality of personal or Confidential Information, regardless of whether the information is maintained on paper or whether it is found in email or other electronic records.