Tuacahn Center for the Arts

Email Policy	Created: 7/9/2012
Section of: Tuacahn I.T. Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 12

“Tuacahn Center for the Arts” (Tuacahn Amphitheatre and Tuacahn High School) is hereinafter referred to as "Tuacahn”.

1.0 Overview

Email is an essential component of business communication; however it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on Tuacahn's liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose

The purpose of this policy is to detail Tuacahn's usage guidelines for the email system. This policy will help Tuacahn reduce risk of an email-related security incident, foster good business communications both internal and external to Tuacahn, and provide for consistent and professional application of Tuacahn's email principles.

3.0 Scope

The scope of this policy includes Tuacahn's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from Tuacahn network.

4.0 Policy

4.1 Proper Use of Company Email Systems

Users are asked to exercise common sense when sending or receiving email from company accounts. Additionally, the following applies to the proper use of Tuacahn email system.

4.1.1 Sending Email

When using a company email account, email must be addressed and sent carefully. Users should keep in mind that Tuacahn loses any control of email once it is sent external to Tuacahn network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help Tuacahn avoid the unintentional disclosure of sensitive or non-public information.

4.1.2 Personal Use and General Guidelines

Personal usage of company email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user's job performance.

• The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

• The user is prohibited from forging email header information or attempting to impersonate another person.

• Email is an insecure method of communication, and thus information that is considered confidential or proprietary to Tuacahn may not be sent via email, regardless of the recipient, without proper encryption.

• It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.

• Email systems were not designed to transfer large files and as such emails should not contain attachments greater than 10 MB.

4.1.3 Business Communications and Email

Tuacahn uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours. Additionally, users are asked to recognize that email sent from a company account reflects on Tuacahn, and, as such, email must be used with professionalism and courtesy.

4.1.4 Email Signature

Email signatures (contact information appended to the bottom of each outgoing email). Users are asked to keep any email signatures professional in nature; however Tuacahn does not place any restrictions on email signature content. Official disclaimers will be appended to all outgoing mail.

4.1.5 Auto-Responders

Tuacahn recommends the use of an auto responder if the user will be out of the office for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.

4.1.6 Mass Emailing

Tuacahn makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with Tuacahn's employees or customer base), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is Tuacahn's intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, Tuacahn requires that email sent to more than thirty (30) recipients external to Tuacahn have the following characteristics:

1. The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.

2. The email must contain a subject line relevant to the content.

3. The email must contain contact information, including the full physical address, of the sender.

4. The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

Note that emails sent to company employees, existing customers, or persons who have already inquired about Tuacahn's services are exempt from the above requirements.

4.1.7 Opening Attachments

Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:

• Never open unexpected email attachments.

• Never open email attachments from unknown sources.

• Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

Tuacahn may use methods to block what it considers to be dangerous or emails or strip potentially harmful email attachments as it deems necessary.

4.1.8 Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. Tuacahn reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.1.9 Company Ownership of Email

Users should be advised that Tuacahn owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by Tuacahn and it may be subject to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

4.1.10 Contents of Received Emails

Users must understand that Tuacahn has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, Tuacahn may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify his or her supervisor.

4.1.11 Access to Email from Mobile Phones

Many mobile phones or other devices, often called smartphones, provide the capability to send and receive email. This can present a number of security issues, particularly relating to the storage of email, which may contain sensitive data, on the phone. Users are not to access, or attempt to access, Tuacahn's email system from a mobile phone without the permission of his or her supervisor.

Note that this section does not apply if Tuacahn provides the phone and mobile email access as part of its remote access plan. In this case, permission is implied. Refer to the Mobile Device Policy for more information.

4.1.12 Email Regulations

Any specific regulations (industry, governmental, legal, etc.) relating to Tuacahn's use or retention of email communications must be listed here or appended to this policy.

4.2 External and/or Personal Email Accounts

Tuacahn recognizes that users may have personal email accounts in addition to their company-provided account. The following sections apply to non-company provided email accounts:

4.2.1 Use for Company Business

Users must use the corporate email system for all business-related email. Users are prohibited from sending business email from a non-company-provided email account.

4.2.2 Access from Tuacahn Network

Users are permitted to access external or personal email accounts from the corporate network, as long as such access uses no more than a trivial amount of the users' time and company resources.

4.2.3 Use for Personal Reasons

Users are strongly encouraged to use a non-company-provided (personal) email account for any non-business communications. Users must follow applicable policies regarding the access of non-company-provided accounts from Tuacahn network.

4.3 Confidential Data and Email

The following sections relate to confidential data and email:

4.3.1 Passwords

As with any company passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the IT Director and/or the Executive Committee Tuacahn may further secure email with certificates, two factor authentication, or another security mechanism.

4.3.2 Emailing Confidential Data

Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

Tuacahn requires that any email containing confidential information sent external to Tuacahn be encrypted using commercial-grade, strong encryption. Encryption is encouraged, but not required, for emails containing confidential information sent internal to Tuacahn. When in doubt, encryption should be used.

Further guidance on the treatment of confidential information exists in Tuacahn's Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

4.4 Company Administration of Email

Tuacahn will use its best effort to administer Tuacahn's email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related security incident.

4.4.1 Filtering of Email

A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, Tuacahn will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or
B) a potential risk to Tuacahn's IT security. No method of email filtering is 100 percent

effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the IT Manager.

4.4.2 Email Disclaimers

The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in Tuacahn's risk reduction efforts. Tuacahn requires the use of email disclaimers on every outgoing email, which must contain the following notices:

• The email is for the intended recipient only

• The email may contain private information

• If the email is received in error, the sender should be notified and any copies of the email destroyed

• Any unauthorized review, use, or disclosure of the contents is prohibited

An example of such a disclaimer is:

NOTE: This email message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by replying to this email, and destroy all copies of the original message.

Tuacahn should review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all required information.

4.4.3 Email Deletion

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on Tuacahn to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email in an attempt to hide a violation of this or another company policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

Tuacahn must note and document here any applicable regulations or statutes that apply to email deletion.

4.4.4 Retention and Backup

Email should be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: Data Classification Policy, Confidential Data Policy, Backup Policy, and Retention Policy.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

4.4.5 Address Format

Email addresses must be constructed in a standard format in order to maintain consistency across Tuacahn. Some recommended formats are:

• Firstinitail.lastname@tuacahn.org

• Firsname.lastname@tuacahn.org

• Firstname-lastname@tuacahn.org

• FirstnameLastname@tuacahn.org

Tuacahn can choose virtually any format, as long as it can be applied consistently throughout the organization. The intent of this policy is to simplify email communication as well as provide a professional appearance.

4.4.6 Email Aliases

Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for company email, as well as (often) the names of company employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

A few examples of commonly used email aliases are:

• info@tuacahn.org

• spiceworks@tuacahn.org

• boxoffice@tuacahn.org

• newsletter@tuacahn.org

Tuacahn may or may not use email aliases, as deemed appropriate by the IT Manager and/or executive team. Aliases may be used inconsistently, meaning: Tuacahn may decide that aliases are appropriate in some situations but not others depending on the perceived level of risk.

4.4.7 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive company email. Accounts will be set up at the time a new hire starts with Tuacahn, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

Accounts on Tuacahn email system will never be provided to non-employees of Tuacahn.

4.4.8 Account Termination

When a user leaves Tuacahn, or his or her email access is officially terminated for another reason, Tuacahn will disable the user's access to the account by password change, disabling the account, or another method. Tuacahn is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by Tuacahn.

4.4.9 Storage Limits

As part of the email service, email storage may be provided on company servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the IT Manager. Storage limits may vary by employee or position within Tuacahn.

4.5 Prohibited Actions

The following actions shall constitute unacceptable use of the corporate email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate email system to:

• Send any information that is illegal under applicable laws.

• Access another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of company executives in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities.

• Send any emails that may cause embarrassment, damage to reputation, or other harm to Tuacahn.

• Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

• Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.

• Make fraudulent offers for products or services.

• Attempt to impersonate another person or forge an email header.

• Send spam, solicitations, chain letters, or pyramid schemes.

• Knowingly misrepresent Tuacahn's capabilities, business practices, warranties, pricing, or policies.

• Conduct non-company-related business.

Tuacahn may take steps to report and prosecute violations of this policy, in accordance with company standards and applicable laws.

4.5.1 Data Leakage

Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to Tuacahn's control of its data.

Unauthorized emailing of company data, confidential or otherwise, to external email accounts for the purpose of saving this data external to company systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from company systems.

Tuacahn may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the IT Manager.

4.5.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. Tuacahn asks that the user limit email attachments to 10Mb or less.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients, and use restraint when sending large files to more than one person.

4.6 Applicability of Other Policies

This document is part of Tuacahn's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

The IT Director under the direction and discretion of the Executive Committee of Tuacahn Center for the Arts and the Administrative Staff of Tuacahn High School will monitor and enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, Tuacahn may report such activities to the applicable authorities.

6.0 Definitions

Auto Responder An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.

Certificate Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

Data Leakage Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.

Email Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.

Encryption The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Mobile Device A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Password A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Spam Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 7/9/2012