Tuacahn Center for the Arts

Acceptable Use Policy	Created: 7/9/2012
Section of: Tuacahn I.T. Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 8

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

1.0 Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how Tuacahn information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be guided to the I.T. Director.

2.0 Purpose

Since inappropriate use of networked computer systems exposes Tuacahn to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of Tuacahn information technology resources for the protection of all parties involved.

3.0 Scope

The scope of this policy includes any and all use of Tuacahn's IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection. And while all computer users at Tuacahn are obligated to abide by this policy and its guidelines users who are also students attending Tuacahn High School must accept and abide by the Student Acceptable Use Policy, which conforms to Federal CIPA requirements.

All Tuacahn I.T. Policies – including this one - are available in digital format on the Tuacahn Sharepoint Site at http://sharepoint.tuacahn.org/itpolicy.

4.0 Policy

4.1 E-mail Use

Personal usage of Tuacahn 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 larger than 10MB.

Please note that detailed information about the use of email is covered in Tuacahn's Email Policy.

4.2 Confidentiality

Confidential data must not be A) shared or disclosed in any manner to non-employees of Tuacahn, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies refer to the proper use of this information in more detail.

4.3 Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4.4 Unacceptable Use

The following actions shall constitute unacceptable use of the Tuacahn network. 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 Tuacahn network and/or systems to:

• Engage in activity that is illegal under local, state, federal, or international law.

• Engage in any activities that may cause embarrassment, loss of reputation, or other harm to Tuacahn.

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

• Engage in activities that cause an invasion of privacy.

• Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

• Make fraudulent offers for products or services of Tuacahn.

• Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.

• Install or distribute unlicensed or "pirated" software.

• Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

4.5 Blogging and Social Networking

Blogging and social networking by Tuacahn's employees are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging and social networking is never allowed from a point of sale computer. In no blog or website, including blogs or sites published from personal or public systems, shall Tuacahn business matters be discussed, or material detrimental to Tuacahn published. Users must not identify themselves as acting in an official capacity on behalf of Tuacahn in a blog or on a social networking site. Excessive use of social networking sites while working is cautioned against and subject to portions of this policy to include but not limited to sections 4.2, 4.4, 4.6, 4.7. Using or installing imbedded games or applications and/or downloading attachments is prohibited on Tuacahn computers. The user assumes all risks associated with blogging and/or social networking.

4.6 Instant Messaging

Instant Messaging is allowed for Tuacahn communications only. The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

4.7 Overutilization

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted. See 4.10, 4.11, 4.13, 4.14.

4.8 Web Browsing

4.8.1 The Internet is a network of interconnected computers of which Tuacahn has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. Tuacahn is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

4.8.2 Personal Use. Tuacahn recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of Tuacahn computer systems to access the Internet is permitted during breaks, and before/after business hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on Tuacahn or on the users job performance. Personal use of the internet is never allowed on systems directly connected to point of sale or ticketing systems.

4.9 Copyright Infringement

Tuacahn's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without written permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which Tuacahn has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.10 Peer-to-Peer File Sharing

Peer-to-Peer networking (Bit Torrent, LimeWire, Napster, etc.) is not allowed on the corporate network under any circumstance.

4.11 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only. Internal network resources should never be used to stream video or music for personal use. The guest network can be used in this manor however, no guarantee of usability is implied.

4.12 Monitoring and Privacy

Users should expect no privacy when using the Tuacahn 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, C.I.P.A, and PCI-DSS 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.

4.13 Bandwidth Usage

Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be completed during times of low network-wide usage.

4.14 Personal Usage

Personal use of company computer systems is not permitted except when complying with section 4.4 and under the guidelines in section 4.8.2 of this policy. Personal use on any point of sale system is never allowed.

4.15 Remote Desktop Access

Use of remote desktop software and/or services is allowable as long as Tuacahn provides it. Remote access to the network must conform to Tuacahn's Remote Access Policy.

4.16 Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

4.17 Use for Illegal Activities

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

• Unauthorized Network Hacking - Port Scanning, Packet Sniffing, Packet Spoofing, Denial of Service

• Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system

• Acts of Terrorism

• Identity Theft

• Spying

• Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues

• Downloading, storing, or distributing copyrighted material

Tuacahn will take all necessary steps to report and prosecute any violations of this policy.

4.18 Non-Company-Owned Equipment

Non-company-provided equipment is expressly prohibited on Tuacahn's network, it is allowed on the guest network and subject to the guest access policy.

4.19 Personal Storage Media

Personal storage devices such as USB devices, thumb drives, hard drives, SD cards, iPods, and phones represent a serious threat to data security and are expressly prohibited on Tuacahn's network.

4.20 Software Installation

Installation of non-company-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance; all software must be licensed, and maintained by Tuacahn or THS.

4.21 Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

• Suspected compromise of login credentials (username, password, etc.).

• Suspected virus/malware/Trojan infection.

• Loss or theft of any device that contains company information.

• Loss or theft of ID badge or keys.

• Any attempt by any person to obtain a user's password over the telephone or by email.

• Any other suspicious event that may impact Tuacahn's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to the I.T. Director. Users must not withhold information relating to a security incident or interfere with an investigation.

4.22 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

Blogging The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

C.I.P.A. (Child Internet Protection Act) Federally mandated set of guidelines for facilities allowing K-12 students access to and use of the internet connected computer technologies.

PCI-DSS A Policy created by a consortium of banks and credit card companies to protect cardholder data and privacy.

7.0 Revision History

Revision 1.1, 8/23/2012