Tuacahn Center for the Arts

Mobile Device Policy	Created: 7/9/2012
Section of: Tuacahn I.T. Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 4

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

1.0 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose

The purpose of this policy is to specify Tuacahn's standards for the use and security of mobile devices.

3.0 Scope

This policy applies to company data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. This policy covers any mobile device capable of coming into contact with company data. All Laptops connecting to Tuacahn's internal network must be owned and maintained by Tuacahn. Use of personal smartphones is allowed so long as the device meets minimum system requirements set by this policy and the owner accepts the terms of this policy.

4.0 Policy

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. Tuacahn should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

• Mobile devices should be kept out of sight and secured when not in use.

• As a general rule, mobile devices must not be stored in cars. If they must be stored in the vehicle care should be taken to secure the device in the trunk or glove box.

• Tuacahn will employ remote wipe/remote delete technology. This technology allows an administrator to make the data on the mobile device unrecoverable.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting company data. The following sections specify Tuacahn's requirements for data security as it relates to mobile devices.

4.2.1 Laptops

At a minimum, company data must be stored on an encrypted partition. Whole disk encryption should be considered if the data is especially sensitive. Laptops must require a username and password or biometrics for login.

4.2.2 PDAs/Smart Phones/Tablets

Encryption and login passwords are required on PDAs/smart phones/tablets. All smart phones connected to internal systems require Android 4.04 ICS or Apple IOS 4.1 or higher. Android and Apple phones and Tablets are the only devices support by Tuacahn Systems.

4.2.2.1 Users of personal devices on Tuacahn's Exchange system must understand and accept that Tuacahn will have the ability to monitor and wipe all data from the device. Tuacahn will not be liable for any personal data lost from users equipment. Accepting this policy is acknowledgment and endorsement if such action is needed to protect Tuacahn.

4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storing company data on such devices is not permitted under any circumstance. Users can request an exemption for backup devices.

4.2.4 Portable Media Players

No company data can be stored on personal media players.

4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the I.T. Director.

4.3 Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of Tuacahn.

4.4 General Guidelines

The following guidelines apply to the use of mobile devices:

• Loss, Theft, or other security incident related to a company-provided mobile device must be reported promptly.

• Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy.

• Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.

• Users are not to store company data on non-company-provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA. Case by case as long as complies with 4.2.2.

4.5 Audits

Tuacahn must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices must be taken and audited against this policy on a quarterly basis.

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

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

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

Mobile Storage Media A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

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

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

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

Tablet Larger thinner replacement for the PDA.

7.0 Revision History

Revision 1.0, 7/9/2012