School of Visual Arts

Wireless Access Policy	Created: 1/1/2015
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 4

School of Visual Arts is hereinafter referred to as "the company."

1.0 Overview

Wireless communication is playing an increasingly important role in the workplace. In the past, wireless access was the exception; it has now become the norm in many companies. However, while wireless access can increase mobility and productivity of users, it can also introduce security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

2.0 Purpose

The purpose of this policy is to state the standards for wireless access to the company's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its wireless infrastructure.

3.0 Scope

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

4.0 Policy

4.1 Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points must be located central to the office space rather than along exterior walls. Technology must be used to control the signal broadcast strength so that it is reduced to only what is necessary to cover the office space. Directional antennas must be used as necessary to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points must be placed in secured areas of the office. Cabling to and from access points should be secured so that it cannot be accessed without difficulty.

4.2 Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

4.2.1 Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID must be changed to something completely nondescript. Specifically, the SSID must not identify the company, the location of the access point, or anything else that may allow a third party to associate the access point's signal to the company.

- The SSID must not be broadcast. This adds a layer of security by requiring wireless users to know the SSID in order to connect to the network.

- The wireless access point must utilize Mac address filtering so that only known wireless NICs are able to connect to the wireless network.

- The wireless access point must not connect to the company's trusted network without a firewall or other form of access control separating the two networks.

- Encryption must be used to secure wireless communications. The strongest available algorithm must be used (i.e., WPA rather than WEP). Encryption keys must be changed and redistributed quarterly.

- Administrative access to wireless access points must utilize strong passwords.

- All logging features must be enabled on the company's access points.

- Wireless networking should require users to authenticate against a centralized server. These connections should be logged, with IT staff reviewing the log regularly for unusual or unauthorized connections.

- Wireless LAN management software should be used to enforce wireless security policies. The software must have the capability to detect rogue access points.

- Users accessing the wireless network must be provided a personal software firewall to secure their computers.

4.2.2 Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.
- Wireless networking must not be deployed in a manner that will circumvent the company's security controls.
- Wireless devices must be installed only by the company's IT department.
- Channels used by wireless devices must be evaluated to ensure that they do not interfere with company equipment.

4.3 Accessing Confidential Data

Wireless access to confidential data is permitted as long as the access is consistent with this and other policies that apply to confidential data.

4.4 Inactivity

Users must disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC.

Inactive wireless access points must be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the company.

Wireless access points must be disabled during non-business hours. This should be accomplished with management software rather than manually performed.

4.5 Audits

The wireless network must be audited quarterly to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, SSID broadcast, and use of strong encryption.

4.6 Applicability of Other Policies

This document is part of the company'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

This policy will be enforced by the IT Manager and/or Executive Team. 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, the company may report such activities to the applicable authorities.

6.0 Definitions

Mac Address Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

SSID Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

WEP Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WiFi Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

Wireless Access Point A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

Wireless NIC A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

WPA Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

7.0 Revision History

Revision 2.0, 1/1/2015