School of Visual Arts

Physical Security Policy	Created: 1/1/2015
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 8

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

1.0 Overview

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on the company's physical network infrastructure. In order to secure the company data, thought must be given to the security of the company's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

2.0 Purpose

The purpose of this policy is to protect the company's physical information systems by setting standards for secure operations.

3.0 Scope

This policy applies to the physical security of the company's information systems, including, but not limited to, all company-owned or company-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting the company's office is covered by this policy.

Please note that this policy covers the physical security of the company's Information Technology infrastructure, and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlap, care must taken to ensure that this policy is consistent with any existing physical security policies.

4.0 Policy

4.1 Choosing a Site

When possible, thought should be given to selecting a site for IT Operations that is secure and free of unnecessary environmental challenges. This is especially true when selecting a datacenter or a site for centralized IT operations. At a minimum, the company's site should meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters.

- A site should not be located in an area where the crime rate and/or risk of theft is higher than average.

- A site should have the fewest number of entry points possible.

If these criteria cannot be effectively met for any reason, the company should consider outsourcing its data in whole or in part to a third-party datacenter or hosting provider, provided that such a company can cost effectively meet or exceed the company's requirements.

4.2 Security Zones

At a minimum, the company will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure the company's assets. In addition to this the company must provide security in layers by designating different security zones within the building. Security zones should include:

Public This includes areas of the building or office that are intended for public access.

- Access Restrictions: None

- Additional Security Controls: None

- Examples: Lobby, common areas of building

Company This includes areas of the building or office that are used only by employees and other persons for official company business.

- Access Restrictions: Only company personnel and approved/escorted guests

- Additional Security Controls: Additional access controls should be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged if possible.

- Examples: Hallways, private offices, work areas, conference rooms

Private This includes areas that are restricted to use by certain persons within the company, such as executives, scientists, engineers, and IT personnel, for security or safety reasons.

- Access Restrictions: Only specifically approved personnel

- Additional Security Controls: Additional access controls must be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged. Additionally, an alarm system should be considered for these areas that will alert to unauthorized access.

- Examples: Executive offices, lab space, network room, manufacturing area, financial offices, and storage areas.

4.3 Access Controls

Access controls are necessary to restrict entry to the company premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with the company's guidelines for their use.

4.3.1 Keys & Keypads

The use of keys and keypads is acceptable, as long as keys are marked "do not duplicate" and their distribution is limited. These security mechanisms are the most inexpensive and are the most familiar to users. The disadvantage is that the company has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, good security can be obtained with keys and keypads.

4.3.2 Keycards & Biometrics

The company requires that keycards or biometrics be used for access to security zones designated as private. The company should consider using these methods for all zones, though it is not required.

Keycards and biometrics have an advantage over keys in that access policies can be tuned to the individual user. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorized. Perhaps best of all, these methods allow for control over exactly who possesses the credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled. The granular control offered by keycards and biometrics make them appealing access control methods.

4.3.3 Alarm System

A security alarm system is a good way to minimize risk of theft, or reduce loss in the

event of a theft. The company does not mandate the use of an alarm system, however an alarm system would be an excellent way to increase the security of the site.

4.4 Physical Data Security

Certain physical precautions must be taken to ensure the integrity of the company's data. At a minimum, the following guidelines must be followed:

- Computer screens should be positioned where information on the screens cannot be seen by outsiders.

- Confidential and sensitive information should not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.

- Users must log off or shut down their workstations when leaving for an extended time period, or at the end of the workday.

- Network cabling should not run through unsecured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).

- The company recommends disabling network ports that are not in use.

4.5 Physical System Security

In addition to protecting the data on the company's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

4.5.1 Minimizing Risk of Loss and Theft

In order to minimize the risk of data loss through loss or theft of company property, the following guidelines must be followed:

- Unused systems: If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.

- Mobile devices: Special precautions must be taken to prevent loss or theft of mobile devices. Refer to the company's Mobile Device Policy for guidance.

- Systems that store confidential data: Special precautions must be taken to prevent loss or theft of these systems. Refer to the company's Confidential Data Policy for guidance.

4.5.2 Minimizing Risk of Damage

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

- Environmental controls should keep the operating environment of company systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.

- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.

- Strong magnets must not be used in proximity to company systems or media.

- Except in the case of a fire suppression system, open liquids must not be located above company systems. Technicians working on or near company systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto company systems.

- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for all company systems. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.

4.6 Fire Prevention

It is the company's policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of the company's office. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.

- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.

• Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.

• Only electrical equipment that has been approved by Underwriters Laboratories and bears the UL seal of approval must be used.

• Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if possible.

• Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.

• A smoke alarm monitoring service must be used that will alert a designated company employee if an alarm is tripped during non-business hours.

4.7 Entry Security

It is the company's policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimizing risk to company systems and data. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall security policy.

4.7.1 Use of Identification Badges

Identification (ID) badges are useful to identify authorized persons on the company premises. The company has established the following guidelines for the use of ID badges.

• Employees: Photo ID badges are required and must be displayed at all times while on company premises. Employees must remove their badges from view when out of the office.

• Non-employees/Visitors: Visitor badges are required. Specific, non-generic badges must identify visitors by name and the date of the visit. The company should investigate visitor badges that automatically expire and determine if the use of such technology is feasible for use.

- Users must a report lost or stolen badge immediately to his or her supervisor. A temporary badge may be utilized in such cases until the badge can be re-generated.

- Initial badge generation will be done only at the direction of Human Resources for new hires or users changing jobs. Users must show photo identification for identity verification.

4.7.2 Sign-in Requirements

The company must maintain a sign-in log (or similar device) in the lobby or entry area and visitors must be required to sign in upon arrival. At minimum, the register must include the following information: visitor's name, company name, reason for visit, name of person visiting, sign-in time, and sign-out time.

4.7.3 Visitor Access

Visitors should be given only the level of access to the company premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered "trusted" by the company. Examples of a trusted visitor may be the company's legal counsel, financial advisor, or a courier that frequents the office, and will be decided on a case-by-case basis.

4.8 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

Biometrics The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Datacenter A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

Keycard A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Keypad A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

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

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

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

Uninterruptible Power Supplies (UPSs) A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.

7.0 Revision History

Revision 2.0, 1/1/2015