# School of Visual Arts

| | |
|---|---|
| Confidential Data Policy | Created: 1/1/2015 |
| Section of: Corporate Security Policies | Target Audience: Users, Technical |
| CONFIDENTIAL | Page 1 of 6 |

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

## 1.0 Overview

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

## 2.0 Purpose

The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

## 3.0 Scope

The scope of this policy covers all company-confidential data, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

## 4.0 Policy

### 4.1 Treatment of Confidential Data

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

#### 4.1.1 Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

#### 4.1.2 Transmission

Confidential data must not be 1) transmitted outside the company network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the company's network.

#### 4.1.3 Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.

- Storage media (CD's, DVD's): physical destruction is required.

- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially-available methods for data wiping. Alternatively, the company has the option of physically destroying the storage media.

## 4.2 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."

- Users must only access confidential data to perform his/her job function.

- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.

- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.

- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.

- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to the company's outsourcing policy for additional guidance.

## 4.3 Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:

- Strong Encryption. Strong encryption must be used for confidential data transmitted external to the company. If confidential data is stored on laptops or other mobile devices, it must be stored in encrypted form.

- Network Segmentation. Separating confidential data by network segmentation is strongly encouraged.

- Authentication. Strong passwords must be used for access to confidential data.

- Physical Security. Systems that contain confidential data should be reasonably secured.

- Printing. When printing confidential data the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.

- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.

- Emailing. Confidential data must not be emailed outside the company without the use of strong encryption.

- Mailing. If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information.

- Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.

- Confidential data must be removed from documents unless its inclusion is absolutely necessary.

- Confidential data must never be stored on non-company-provided machines (i.e., home

computers).

- If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

## 4.4 Examples of Confidential Data

The following list is not intended to be exhaustive, but should provide the company with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Students social security numbers or personal identifiable information (PII)
- Faculty social security numbers or personal identifiable information (PII)
- Employee/Staff social security numbers or personal identifiable information (PII)
- Medical and healthcare information for students, faculty or employee/staff
- Electronic Protected Health Information (EPHI)
- Student Grades
- Student Class lists
- Student course schedules
- Student Disciplinary records
- Student financial records
- Company financial data
- Financial forecasts
- Product and/or service plans, details, and schematics
- Network diagrams and security configurations
- Communications about corporate legal matters

- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

## 4.5 Emergency Access to Data

A procedure for access to confidential and critical data during an emergency must be developed and documented. The company must establish a procedure for emergency access in case the normal mechanism for access to the data becomes unavailable or disabled due to system or network problems.

The procedure should answer the following questions:

- What process must be followed to activate the emergency access procedure?
- What systems will it will involve?
- In what situations should be activated?
- Will it be activated automatically if certain conditions are met, or will it require human intervention? If so, who is authorized to make the decision to implement the procedure?
- Who will be involved in the process and what roles will they perform?

## 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

**Authentication** A security method used to verify the identity of a user and authorize access to a system or network.

**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 Data Device** A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

**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 2.0, 1/1/2015