Information Systems Security Policy

Creative Touch Cosmetology School

Creative Touch Cosmetology School

234 E 3rd St Waterloo IL 62298

618-939-0322

www.creativetouch.edu

7/01/2020

Outline

Introduction

This general security policy has been developed to ensure data integrity and confidentiality for all administrative computer systems at Creative Touch Cosmetology School. This document will provide guidelines for the classification of data resources, and subsequent retrieval and dissemination of that data by various user groups. These guidelines will allow individual departments to approve data access authorizations for their data (in general cases). Any exceptions to user access situations covered in this general policy will be taken under special consideration by the school director.

More and more school employees have access to confidential information via computers. This security policy is not intended to hamper the use of computers in obtaining information necessary to conduct school business. However, it is intended to encourage responsible use of computers and discretion in dissemination of student and employee information.

Data Retrieval and Dissemination

Procedure

Each set of data will be classified as having an "owner". This owner will be represented by a specific individual within the School department responsible for that data. Any time a department or individual wishes to gain access to another department's data, they must follow the procedure below:

1) *If you are requesting access to student information, fill out the appropriate Security access forms that can be found on the school website www.creativetouch.edu under the "about" tab and submit it to the Registrar's Office.*

2) *Once your request for data access has been approved by the owner/department responsible, you will be asked to sign a "Statement of Accountability" form in order to receive a sign-on code and password from the Registrar. (If you are gaining access to the Student Records system, you will be asked to sign a "Statement of Confidentiality/Accountability" for the Registrar's Office, as well.)*

(The following section, Data Sources, provides data descriptions and departmental sources.)

Enforcement of Policy

Each department is responsible for enforcing this data security policy. School policy states that confidential information is to be used only when necessary for School business. Refusal to adhere to this policy is a clear violation of the Family Educational Rights and Privacy Act of 1974. Offenders will be subject to disciplinary action and possible referral of the violation to the proper authorities.

Confidential Data

Confidential data, also referred to as Personally Identifiable Information or PII, includes any information defined as such in Federal, State, School data privacy laws and regulations. Examples include, but are not limited to: Social Security; Driver's License; Passport Numbers; Birth Date; financial information; individual's medical or academic information; any data covered by FERPA, HIPAA, PCI-DSS Standards, or the Illinois School Student Records Act 105 ILCS 10. Unauthorized access, transmission, collection or storage of confidential data is prohibited. Access to and storage of confidential information on personal (user owned) devices can pose substantial risk to the School (as well as the individual) and is prohibited.

Data Sources

For the purposes of this policy, data types are categorized as follows:

Student Information
Student Financial Aid Information
Student Grade *Information*
Administrative Financial
Information Human Resources
Information Institutional Research
Information

Within these general categories, the different types of data are broken down into subsets; a University source is provided for each.

Student Information

Data Owner: Registrar

The Office of the Registrar is the official source of information on individual students. For security purposes, student information is divided into the two categories of directory and academic.

Directory Information

School personnel may have access to directory information and may, without restriction, disseminate information for official use on and off campus. The Family Educational Rights and Privacy Act of 1974 and the School specify the following as directory information:

- *Student's name, address, telephone number, e-mail address, photograph, date and place of birth*
- *Major, dates of enrollment, degree conferred and dates of conferral, any graduation distinction*
- *Institutions attended prior to admission to Creative Touch Cosmetology School*
- *Participation in officially recognized activities*

Directory information is available on Eduquette.

If a student does not wish any of the above information released to non-institutional persons or organizations, a Non-Disclosure of Directory Information must be completed in the Registrar's office. Once the student has completed the form, this request will remain in effect until the student notifies, in writing, the Registrar's office to remove the form.

Academic Information

Academic information, including grades, academic status, class schedules, etc., cannot be released to third parties without the student's written permission. Academic information can be used by Creative Touch Cosmetology School employees having a legitimate educational interest in the student and who are acting within the

limitations of their need to know may access student educational records without prior consent of the student. This includes personnel in academic offices as well as student support offices, such as Admissions, Student Accounting, Financial Aid, Registrar, etc.). This is true even if the student has been granted non-disclosure.

Academic information not available from Eduquette should be requested from the Office of the Registrar. Requests for information from students or from agencies or individuals outside the School should also be referred to the Office of the Registrar.

Summary Student Information

The Office of Registrar is the official source of aggregate or summary student information, such as enrollment or credit hour data intended for on- or off- campus dissemination. Requests for reports and analyses involving summary student data to be produced through Eduquette will be developed in conjunction with the Office of Financial Aid. This will ensure that reports and analyses are based upon the most accurate information and will enhance the consistency and integrity of information generated by the School.

Student Financial Aid Information

Data Owner: Director, Financial Aid Office

The Financial Aid Office is the official source of information on individual University students receiving financial assistance from various aid programs, including grants and scholarships and loans. All requests for this type of information should be addressed to the Director of Financial Aid.

Information on students receiving financial assistance through student loans is maintained by the Financial Aid Office and should be requested from the director of that department.

Student Grade Information

Data Owner: Director, Department of Curriculum

Any information pertaining to student grades on campus should be requested from the Director of curriculum.

Payroll Information

Data Owner: Director, Payroll Office

The Payroll Office is the official source of financial information on individual School employees. All requests for this confidential financial information should be submitted to the Director of Payroll.

Human Resources Information

Data Owner: Director, Human Resources

Information concerning specific job positions (classifications, descriptions, etc.) at the School is maintained by the Human Resources department. All requests for employee information (excluding payroll information) should be sent to the Director Human Resources.

Institutional Research Information

Data Owner: Registrar

Institutional research information includes data on student enrollment, faculty reports, clock hour production, surveys (e.g., retention of students), government reports, etc. The official source for this type of information is the Office of the Registrar, and all requests for such information should be submitted to the Director of that office.

Financial Accounting Information

Data Owner: Business Office

Revenue, expenditure and budget information is maintained for each account. Requests for access to information should be submitted to the Business office.

Classification Standards

Data Classification

Data classification indicates what the user is able to do with the data. Specific restrictions are outlined and enforced by individual departments responsible for the data. Specific levels of access clearance include the following:

1. *Read only*
2. *Maintenance (Update, Add, Delete)*

Various user classifications will have access to data through one or a combination of these clearance levels. Each user ID is restricted by the forms that the user has been granted to access, i.e., their clearance level will provide them the ability to access a limited number of forms. If a user tries to access a form inappropriate to his/her clearance level, a security violation message will appear on the screen.

Data should not be downloaded to other storage medium without permission from the departmental owner of that data. Downloading of administrative data requires a separate authorization from the data owner. Individual users will be held responsible for any violation of this procedure.

Departmental Security

Each department will designate an "owner" for the data it maintains. Appropriate procedure for retrieval and dissemination of School data will be followed as outlined in the previous section, Data Retrieval and Dissemination.

Departments storing data subject to School regulations are responsible for ensuring that all such data is protected in accordance with institutional regulations. This applies to all such data from any source, whether electronically transferred from the administrative systems, or entered by the individual department from printed documents.

Specifically, departments must ensure that access to individual workstations or servers containing this information or access to output generated from departmental systems, is restricted to individuals authorized to access the data. Password security on individual stations or servers is not sufficient to ensure compliance; any such systems on which regulated data is stored must also be in secure, supervised areas, such as departmental or individual offices.

Backup tapes, disks or copies of data on printed or electronic media must be similarly protected. Under no circumstances shall confidential data or access to it be granted to personnel from other departments or non-School personnel without express written authorization from the appropriate administrative office. Any unauthorized storage and/or reproduction of confidential School data (e.g., grades, transcript files, etc.) is strictly prohibited.

Physical Security

President and department/division heads are responsible for ensuring the physical security and responsible use of computers located in departments and offices under their authority. The following policy statements should be made available and/or posted prominently so that all personnel working with computers know the extent of their responsibility.

1) *Computers will be located in physically secure areas which can be locked when not in use.*

2) *Access to computers will be limited to individuals engaged in official school business.*

3) *Use of computers by student workers should be restricted to those cases in which student workers are absolutely necessary to supplement regular School staff members. Student workers should be thoroughly instructed in the proper and responsible use of computers.*

4) *Each individual with access to administrative information is assigned his/her own account credentials (user id and password). The owner of the account is not to share this information with anyone else; the owner is responsible for any misuse of his/her sign-on credentials.*

5) *Under no circumstances will account credentials be posted on or near computers .*

6) *Computers which are "signed on" should never be left unattended.*

7) *Requests for improvement of computer security, as well as suspected violations, should be addressed to the Director of Operations.*

Computers which are routinely used by individuals not cleared for access to such data are inappropriate locations for confidential data (e.g. computers in student labs or other public locations.) Placing confidential information on systems of this nature constitutes a clear violation of School regulations.

Because of the possibility of theft and discovery of data, neither portable computers (notebooks, laptops, etc.) nor portable storage devices, including USB keys and portable disks, should be used to store confidential or regulated data, unless such data is encrypted.

Computer Security

1) *Confidential data should only be accessed from non-public, School owned computers assigned to employees.*

2) *Computers should have School issued Anti-Virus software installed and Windows Update active and patches applied on a regular basis.*

3) *In some circumstances, School provided PII searching software should be installed on the system (see Data Security below).*

4) *If accessing School Information systems, software should not be configured to use a stored password or otherwise bypass entering a password.*

5) *Users should log off the computer when not actively using it (for example, when leaving the office for a meeting or lunch). It is recommended that screen lockout be configured to automatically lock the computer after it is inactive for more than 10 minutes.*

Data Security

Any individual who accesses School data, through a computer or a report, is responsible for the confidentiality of that data. Likewise, any individual who stores School data on a personal computer will be held accountable for the confidentiality of that information.

Under no circumstances should confidential data be stored on a cloud service such as Dropbox, Google Drive, Box, or One Drive *etc. T*

Electronic files containing Social Security Numbers shall not be stored on desktops, laptops, departmental servers, cloud services, portable media devices, or stored in email without explicit written permission from the Director of Operations. The files containing SSNs approved for local storage must be encrypted; all unapproved files must be deleted. For departments that must have access to SSNs, as part of essential business purposes, the School provides Eduquette *software that is installed on employee computers which assists with removing PII. For more information, please contact the Director of Operations.*

Web Servers and Departmental Servers

Web Servers and Departmental Servers

Information subject to School or confidentiality regulation should not be placed on the main University web server without prior written approval from the appropriate administrative offices as well as the Manager of Web Services. Such data should, in general, be placed on Web or other departmental servers only if absolutely essential to School business and only if appropriate safeguards, including appropriate file permissions, access controls and security patch procedures are in place.

Electronic Mail System Security

Electronic mail poses additional risks in the handling of confidential data. Data may quite readily be transmitted to unintended recipients through misaddressing or similar error. In addition, the routine maintenance of mail systems may require or inadvertently lead to viewing of some pieces of mail by mail systems administrators. The School will respect the privacy of all such mail and will not reveal the contents of such mail to any other parties. However, if activities in violation of law or School regulations are discovered through this procedure, the School may report such information to appropriate authorities.

Departments are advised that information subject to confidentiality regulations should not be transmitted via electronic mail without prior written approval from the appropriate administrative offices.