



ARTCENTER COLLEGE OF DESIGN SYSTEM SECURITY POLICIES & PROCEDURES

Updated April 2024

Table of Contents

I.	INTRODUCTION	3
II.	PURPOSE	3
III.	POLICY	3
	A. PHYSICAL ENVIRONMENT	4
	B. NETWORK LAYER.....	5
	C. APPLICATION LAYER.....	7
IV.	ASSET IRREGULARITY REPORTING	8
V.	NETWORK INCIDENT RESPONSE	10
VI.	DATA PROTECTION.....	13
	APPENDIX A.....	15
	APPENDIX B.....	18
	APPENDIX C.....	19
	APPENDIX D.....	21

I. INTRODUCTION

As a leading institution of higher education, ArtCenter College of Design has taken significant steps to secure access to its student, faculty, and administrative systems as well as to protect its investment in all technology assets.

II. PURPOSE

The purpose of these security methods is to minimize the opportunities to compromise ArtCenter's systems which are vital to the ongoing operations of the College. Faculty, staff and students are expected to comply with the policy or risk disciplinary action.

III. POLICY

This policy addresses the security methods that are deployed in each of the 3 layers in the technology architecture. The security layers are described in a hierarchical structure, from the physical environment to the application layer. The 3 layers include:

PHYSICAL ENVIRONMENT

- Authorization to enter secured areas on campus – data center and telecommunications rooms
- Physical security of technology assets in computing labs, offices, and classrooms

NETWORK LAYER

- Authorization to access the ArtCenter network and Internet connection
- Authorization to use ArtCenter email services

APPLICATION LAYER

- Authorization to access a specific student, faculty, or staff administrative system

A. PHYSICAL ENVIRONMENT

1. The data center and telecommunications rooms are accessible to authorized Information Technology staff only. Authorization is granted by the Director of Network Services. Once authorization is granted, a request for an electronic key card and/or key is submitted to the Director of Campus Security, who assigns the keys and tracks all usage.

Doors to the data center and telecommunications rooms must be closed and locked at all times. When facilities personnel must access secured sites to perform maintenance or tenant improvements, requests for temporary access must be scheduled through the Director of Network Services. Outside vendors will be issued a temporary pass with the prior approval of the Director of Network Services. All workers must be supervised until work is completed.

2. Physical security of technology assets begins immediately upon the assets' delivery to ArtCenter. The following procedure is performed to ensure optimal security upon delivery of technology assets:
 - The Technology Department's Inventory Administrator is contacted by the Receiving Clerk to receive new technology assets.
 - The Inventory Administrator un-boxes the assets, affixes inventory barcode stickers (as required), and enters the assets into the asset management system. The assets are then stored in a locked cage until assigned and scheduled for deployment to the end-user.
 - Once a technology asset is assigned (but before it is deployed), the Inventory Admin will update the individual asset record within the asset management system to reflect the location and/or end-user assigned the asset.

The Information Technology Department maintains an inventory record of its technology assets and reconciles this record with physical inventory on an annual basis.

3. Technology assets are secured in various ways to protect the asset from theft or damage. Assets include computers, printers, scanners and audio visual equipment. Cables, locks and cabinet enclosures are installed on equipment that is at highest risk,

which is dependent on usage and physical exposure. The most appropriate security measures will be added to all equipment by the Information Technology Department.

Any employee (staff and faculty) or student who vandalizes the locking mechanisms to gain access to physical assets will face severe fines and disciplinary action up to and including expulsion or termination.

B. NETWORK LAYER

1. Authorization to access the ArtCenter network and Internet connections is granted by the Director of Network Services for faculty, students and staff. The Human Resources Department notifies Information Technology of all new and terminated employees.

During registration each term, Enrollment Services updates or enters new student information into the Ellucian Colleague system. Colleague then generates unique Student ID numbers and user/email accounts.

Upon the creation of the new user account, students are granted access to network resources specific to the program/discipline to which they belong (i.e. Network folder access for each class and individual home folders.)

2. Information Technology assigns a network login ID (username) to the employee at which time a new user account is created. Access to ArtCenter's network resources is granted to employees for services such as email and department folders. Access is limited to the specific requirements generated by each department head. When a new employee starts, the following occurs:
 - a. Notification of a new employee is originated from Human Resources.
 - b. The hiring manager requests accounts for email, voice mail, and applications appropriate to their business process.
 - c. A ticket is generated for the request and distributed to Information Technology personnel to complete the request.
 - d. A random initial password is generated for the new employee and prompts the user to reset. During this process, the employee must go through a second factor authorization process.

3. ArtCenter reserves the right to provide network access to employees and students as well as the right to terminate access at any time to assure compliance with ArtCenter's policy. Information Technology may inspect any and all files stored on ArtCenter's network to ensure protection and security.
4. All students are provided ArtCenter's Responsible Use Policy (RUP) policy during new student orientation, and employees at the start of employment. The policy is also available in the Student Handbook as well as the Employee Handbook, and posted online on the College's portal.
5. To ensure the safety and security of ArtCenter's network, ArtCenter has installed screening programs and other security systems (firewall, Internet address screening programs, gateways, and other systems.) Any employee or student who attempts to disable, defeat or circumvent any college security facility will be subject to immediate dismissal.

Users with specific business need to remotely connect into ArtCenter network may request access in writing to the Information Technology Help Desk after obtaining approval from their supervisor. Remote users must abide by security measures dictated by ArtCenter.

6. All approved vendors will be required to use secure access methods, such as Secure Shell (SSH)* or Virtual Private Networking (VPN)** to connect to ArtCenter's network. Insecure protocols such as telnet, rsh, and rlogin are not accepted methods. Access will be based on a signed Statement of Work, and will only be granted permission for the duration of the engagement.

All third-party vendors (contractors, consultants, etc.) are required to submit a complete Statement of Work (SOW) prior to requesting access into ArtCenter network. No one is allowed

* 'SSH' is an interface and protocol for securely accessing remote computers. It is an industry standard protocol, which is both encrypted and secure, protecting both ends of the client/server connection by using Public-Key Cryptography.

** 'Virtual Private Networking' is defined as those technologies that establish a private or secure network connection across a public network, such as the Internet.

to access ArtCenter's network resources without a complete SOW. The Vice President of Information Technology and the head of the hiring department must approve the SOW in advance. Once approved, ArtCenter's Technology staff grants specific permissions based on the approval. (See template SOW, Appendix B.)

7. Revocation of Privileges:
 - a. Employees: Privileges to any ArtCenter system (for all security layers) are revoked upon termination of employment with ArtCenter, or upon violation of the System Security Policy.
 - b. Students: Privileges to any ArtCenter systems (for all security layers) may be revoked when a student withdraws or changes to "inactive" status. Additionally, privileges may also be revoked upon expulsion from the college or upon violation of the System Security Policy.
8. ArtCenter forbids the use of the college's electronic communications resources for any purpose that could strain or compromise these resources or that interfere with the use of these resources. Therefore, employees and students may not use the college's network to send or create any attacks or abusive actions such as spam, spyware/malware proliferation, phishing, or denial of service (DoS) attacks. See RUP (Appendix A) for further detail.
9. ArtCenter recognizes the global problem of the aforementioned abusive tactics. To control and mitigate such tactics, Information Technology monitors and logs network traffic and protects ArtCenter's resources by blocking spam, DoS, and the like.

ArtCenter systems are protected with a multi-layered threat management system: starting at the Gateway, followed by a second layer of protection at the server level, and concluding at the 3rd layer of protection on the Client desktop.

C. APPLICATION LAYER

1. The hiring manager initiates a request to the Information Technology Help Desk where the new hire's name, position, and application access is specified.
2. Application access is defined according to an employee's department and job role, such as access to Ellucian Colleague.

3. The Technology Help Desk forwards the work request to appropriate individual(s) within Application Services for completion.
4. Application Services processes the work request verifying the access request and obtaining appropriate approvals from the data owners. Once verified and confirmed, access is granted with appropriate level of access. The hiring manager is then notified upon completion.

IV. ASSET IRREGULARITY REPORTING

A. PURPOSE

Good business practice dictates that every suspected asset irregularity be promptly identified and reported. For the purposes of this document, “asset irregularity” is defined as theft (actual or suspected), vandalism, or loss due to misreporting or improper disposal of an asset. ArtCenter is committed to the highest standards of ethical behavior. As such, all ArtCenter employees and students are expected to report known or suspected irregularities of technology assets to either their department manager or the Information Technology Department.

B. ASSET RESPONSIBILITY

Technology asset management and security is the responsibility of the Information Technology Department. Information Technology records and controls these assets on an ongoing basis. Such control extends from the acquisition of the asset to the disposition, including any transfer, sale, relocation, or reporting of irregularities associated with loss of the asset.

The Inventory Administrator tracks and conducts general inventories of technology assets once a term to ensure accurate inventory.

C. DEFINITION OF TECHNOLOGY ASSETS

'Technology Assets' are defined as those assets purchased by ArtCenter and under the direct management of the Information Technology Department. These assets include the following:

- Desktop and laptop computers
- Network and desktop printers
- Software licenses
- Scanners, tablets and other computer peripherals
- Audio Visual equipment (cameras, lights, projectors, displays, etc.)
- Network devices (switches, hubs, routers, etc.)
- Servers and server components
- Network infrastructure equipment (fiber-optic/UTP cabling, racks, etc.)
- Telephony equipment (PBX, handsets, headsets, etc.)

D. PROCEDURE FOR REPORTING LOSSES

All losses of ArtCenter assets, including those which ArtCenter has accepted custody and responsibility for, must be reported regardless of the cause and amount. The procedure for reporting technology asset loss is as follows:

- In the event of a theft that is "in-progress" or has just occurred, the employee or student should immediately notify the Campus Security Department.
- Upon report or discovery of a missing technology asset, Information Technology should notify Campus Security within 24 hours.
- After being notified, Campus Security begins an investigation under the Director of Campus Security's lead. Campus Security interviews Information Technology and any other reporting party (if applicable.)
- The Information Technology Department's Inventory Administrator locates the item on record by either the item's location or assignee's name and updates it as a missing item.
- Information Technology and/or the reporting party are interviewed and asked to fill out a Campus Security report form. This form includes a description of the item along with other pertinent information regarding the loss event.
- Depending on the dollar amount, Campus Security may or may not be required to report the loss to police. In the event of a police report, both the Information Technology Department representative and the reporting party may be interviewed again.
- Upon completion of the investigation, Campus Security will submit a copy of their case report to the Senior Vice President and Chief Financial and Administrative Officer. The Director of Campus Security interfaces with the Accounting Department to determine the appropriate course of action in item replacement (if applicable.)

- The Information Technology Inventory Administrator will not delete the item from ArtCenter’s inventory record until all investigative action has been completed and all attempts to recover the item have failed.

V. NETWORK INCIDENT RESPONSE

A. PURPOSE

Cyber security threats are ever-multiplying and evolving across the internet. Since the ArtCenter network is connected to the internet, the Information Technology Department must be prepared for and be able to respond in case of a network incident. (See template response workflow, Appendix D.)

A “network incident” is defined as an adverse event or series of events that impact the security or ability of a network to operate in a normal fashion. Some example threats that can create an incident are:

- Denial of Service (DoS) attack
- Phishing
- Computer virus/worms and Malware
- Brute force password cracking
- Rootkits

Network incidents are not limited to just external threats – they can and often do occur as a result of an internal security violation. Incident response is everyone’s responsibility. Employees are accountable for understanding their responsibilities within the context of information security, reporting suspected and actual information security or privacy incidents to designated individuals, and cooperating with designated individuals in performance of the incident response process.

All users should report suspected security incidents to VP of IT, or by contacting Campus Security.

The purpose of monitoring activities by Information Technology department includes maintaining the integrity and security of the College’s network infrastructure and collecting information to be used in network design, engineering and troubleshooting.

Automated tools used to monitor system status include physical and virtual servers, network devices, the telephone system, networked storage devices, and all networked server appliances. Automated tools are deployed to monitor real time detection of intrusion and vulnerability exploitation for services such

as network and email traffic. System logs are checked for signs of intrusion and vulnerability exploitation which include intrusion detection system logs, firewall logs, user account logs, network scanning logs, system error logs, application logs, backup and recovery logs, Help Desk logs, and telecommunication activity reports.

B. PROCEDURES

1. Documentation of Event(s) – Immediately after an event is recognized as out-of-the-ordinary, the following information is documented:
 - Date and time of event
 - Name and contact information of who reported the event. If the event was reported by a monitoring system, document which system made the report.
 - Detailed description of the event.
 - Identification and specification of the host system(s)
2. Assignment of Event(s) to an Incident – If the event appears to be related to an open or previously closed incident, then the event is assigned to that incident number (using the appropriate tracking system) and the incident is reactivated as necessary. If the event appears to be a new incident, then a new incident number is created and the event is associated with that incident.
3. Assignment of an Incident Handler – Depending on the affected technology, the discoverer of the incident may or may not become the Incident Handler. The incident is handed off to the on-call systems administrator or network engineer who will then become the Incident Handler.
4. Definition of Severity Level for Incident – The Incident Handler makes a determination of the incident’s severity level based on the incident documentation at hand and confirmation from the Incident Handler’s manager. Severity levels are defined as 1, 2, or 3 with 1 being the highest severity and 3 being the lowest.
5. Coordination of an Incident Response (IR) Team – The Incident Handler remains the primary handler of the incident while the Incident Manager is responsible for coordinating and briefing the Incident Response Team on the situation.

Severity of the incident dictates which members of the Technology Department are called upon to participate in the Incident Response Team, and how quickly they are contacted.

- For a Severity 1 incident, the Incident Handler contacts all Technology managers along with the VP of Technology immediately.
- For a Severity 2 incident, the Incident Handler contacts the Technology managers and the VP of Technology within 1 hour.
- For a Severity 3 incident, the Incident Handler contacts the affected Technology manager(s) within 2 hours.

The Incident Manager works with the Incident Handler to verify with the IR team as much information as possible and requests any and all resources necessary to resolve the incident. Based on severity and impact to ArtCenter, the decision on whether to contact Law Enforcement will be made during the IR team meetings.

6. Containment and Eradication – Depending on the nature of the network incident, containment and eradication methods vary. The following guidelines are adhered to by the Incident Handler and IRT members participating in the hands-on resolution of the incident:
 - Preserve as much evidence in original form as possible
 - Take detailed notes on steps taken and those taken by others
 - Record each piece of evidence found along the way including a description, time found, and any other distinguishing characteristics.
 - Restrict information on a need to know basis
 - Do not rush to complete the investigation

If there are strong indications that a host computer or network device has been compromised, the host will either be disconnected or isolated from the production network. The computer may not be powered off until after a forensic analysis has been completed.

7. Forensic Analysis – For any computer system where an intrusion is suspected, there are several steps that are taken prior to shutting down the system:
 - Recording a list of running processes on the system
 - Checking the network interface card for promiscuous mode
 - Recording a list of all listening network ports and active connections
 - Performing as few file system operations as possible on the affected system
 - Making at least one bit level copy of the system's hard drive (if applicable)

- Removing the hard drive from the affected system and storing for evidence (if applicable)
8. Follow-up with External Organizations – In the event of an Internet-based attack, ArtCenter’s Information Technology Department may at its discretion follow up with Internet Service Providers in order to trace the source of the attack. Additionally, ArtCenter may contact the appropriate law enforcement agencies to report the incident at this time, either to pursue criminal or civil penalties, or as a matter of record.
 9. Summary Report Generation – After the incident has been contained and any threat eradicated, a summary report (1-2 pages) is generated to present to the ArtCenter leadership. The report contains the following:
 - A high-level description of the incident and its scope
 - The impact on ArtCenter
 - Law enforcement findings (if applicable)
 - Actions taken to prevent further occurrences
 - Recommendations for further action, if any, such as proactive response communication
 10. Storage of Incident Evidence & Documentation – In the event that ArtCenter engages a law enforcement agency as part of the network incident response, all evidence, logs, data, and documentation associated with the incident will be placed in sealed, tamper resistant containers and put into limited access secure storage.

VI. DATA PROTECTION

A. PURPOSE

ArtCenter must protect confidential or sensitive data from loss to avoid damage and to protect its clients. The protection of data is a critical institutional requirement as is the flexibility to access data effectively by authorized personnel. The definition of data to be protected include, but are not limited to, personally identifiable information, financial information, and intellectual property information.

B. PROCEDURES

All personnel must abide by the RUP and protect confidential or sensitive data. It is not anticipated that technology alone can control and effectively handle malicious or accidental acts of data loss or compromise. Therefore, ArtCenter personnel must also

adhere to the following requirements to safeguard its data:

- Employees are not to communicate by external e-mail systems not hosted by ArtCenter to distribute email.
- Maintain a clean and organized desk/work area. To maintain information security, all data on printed material must not be left on workstations.
- Use a secure password on all ArtCenter systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
- Immediately notify the Information Technology department in the event that a device containing in scope data is lost.
- Inform the Information Technology department in the event that you suspect a system or process is not compliant with this policy so that appropriate measures can be taken to follow-up and correct as needed.
- Handle all data securely through appropriate physical care (not leaving devices unattended, etc.) and through the use of password protection.

APPENDIX A

Responsible Use Policy (RUP)

ArtCenter grants computer, network and electronic communication privileges to its community. All members of ArtCenter are expected to use its network, computer facilities, and electronic communication provided through those facilities in a responsible manner. The purpose of this policy is to:

- Secure the integrity of all computers, networks, data and communication devices at ArtCenter or ArtCenter systems used or accessed by students, faculty or employees;
- Encourage behavior that is aligned with the ArtCenter code of ethics;
- Uphold freedom of speech within the context of responsible action and law;
- Protect ArtCenter against damaging or legal consequences;
- Enforce ArtCenter policies against harassment or threats

The ArtCenter network, computer facilities, and electronic communications include all hardware, software and data that support the following systems and uses:

- Administrative applications
- Email
- Educational Computing Lab hardware and software
- Data and voice networks
- Library systems
- Scanners, telephone systems, voice mail, fax machines
- Digital video, webcasts, multimedia files
- ArtCenter web sites, both internal and external, and gateways to external sites
- Wireless access points and networks
- Any other related computer systems

ArtCenter maintains its computer, network and electronic communication systems for business and educational purposes. The systems and the communications are the property of ArtCenter and ArtCenter reserves the right to inspect and monitor the systems to ensure that they are being used properly. Employees, faculty and students should not expect that use of the systems, e-mails, Internet usage, or other on-line communications and usage will be confidential or private. ArtCenter may monitor Internet, e-mail or other on-line transactions as well as any computer usage at any time, with or without notice, in its sole and absolute discretion.

Policy Violations

Violations of this policy include but are not limited to using student, faculty and staff owned computers and other digital devices, ArtCenter computers, networks, or electronic communications, to:

- Harass, threaten, intimidate, libel or slander, or otherwise harm specific individuals or classes of individuals whether by direct or indirect means; for example sending an individual repeated

and unwanted (harassing) email, or using email, voice mail or telephonic communications to harass, threaten or stalk someone.

- Cause destruction or damage to equipment software, or data belonging to ArtCenter or to others.
- Disrupt, impair, or cause harm to the activities of others; for example propagating electronic chain mail, sending forged or falsified email, tampering with others' files, storage media, passwords or accounts.
- Copy, download, post, or transmit across ArtCenter's network, illegal, proprietary, or unauthorized copyright-protected, patented, or trademarked material, or any material that is damaging to ArtCenter; for example, launching a computer virus, distributing pornography, offensive or inappropriate material, distributing or downloading copyrighted musical recordings, lyrics, movies, videos, or images via a file-sharing application, or posting an ArtCenter site-licensed program to a publicly accessible site.
- Gain unauthorized access to other systems, facilities or data either directly or via the network
- Conduct any commercial activity, including activity published from personally owned computers or web sites which use ArtCenter's network; for example, using e-mail or telephonic communication to solicit sales, conduct business, creating web sites to advertise, or sell a service or product
- Impersonation of another's identity or misrepresentation of one's own identity
- Any illegal activities that violate any state or federal laws
- Any inappropriate or annoying activity

Guidelines for Responsible Use

The following guidelines apply to any actions you take using any System:

- Respect the privacy of other users, and do not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users without permission.
- You are prohibited from "spoofing" and "phishing" or any other method of deception, redirection, and impersonation of any person's identity, headers, identifiers, email address, server address, internet server provider, email provider or host.
- Do not publish, post, email or otherwise transmit any content that you do not have a right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements).
- Do not email or otherwise transmit any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation.
- Do not upload, post, email or otherwise transmit any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
- Do not interfere with or disrupt our sites, services or servers, or disobey any requirements, procedures, policies or regulations of networks connected to the Service. Here are some examples of interference or disruption: inappropriate use of mail relay, wide-scale distribution of messages to inappropriate forums or mailing lists, propagation of computer worms or viruses, and use of the network to make unauthorized entry to other devices or resources.

This includes unauthorized security probing activities or other attempts to evaluate the security integrity of a network or host system without permission.

- Do not collect or store personal data about other users or harvest or otherwise collect information about others, including e-mail addresses, without their consent.

Safeguarding your Password(s)

Passwords are the front-line protection for user accounts. A poorly chosen password may result in the compromise of ArtCenter's entire network and online information. Employees (staff and faculty) and students, as well as contractors and vendors with access to College systems, are responsible for taking appropriate steps, as listed below, to select and secure their passwords.

- Do not write down or store on-line (unless encrypted.)
- Do not share your password with anyone.
- Do not use "Remember Password" feature of applications.
- Do not reuse or recycle old passwords.
- Change password immediately if you feel it has been compromised.
- Do not discuss passwords in front of others or give hints.
- Do not reveal a password on questionnaires or forms.
- Do not include a password in an email or other forms of electronic communication.
- Set your password to minimum 10 alphanumeric characters.
- Avoid passwords that are not easily guessed or decoded, such as birthdays, names, and common words.

Reporting Violations

Students and Faculty can file an incident report with the Provost, or the VP of Information Technology. An investigation will be conducted by the Dean of Student Affairs, in conjunction with the Provost for student related incidents. The Dean may form a committee to investigate the incident and recommend action to the Provost. Criminal acts will be turned over to the proper authorities.

Employees can file an incident report with the Office of Employee Experiences (HR) or the VP of Information Technology. An investigation will be conducted through HR. Criminal acts will be turned over to the proper authorities.

ArtCenter Property/Right to Restrict Access

ArtCenter reserves the right to monitor, restrict or deny access to its computers and networks at any time and for any reason. Improper use of the network, computers and/or electronic communications may result in disciplinary actions up to and including expulsion (if a student) or termination (if an employee) from ArtCenter, in addition to state or federal prosecution.

APPENDIX B

Statement of Work for ArtCenter Contracted Services

Contractor/Consultant Information:	
Project Name:	
Project Description:	
Client Contact:	
Scope:	
Vendor responsibilities:	
Project costs:	
Estimated time to complete:	
ArtCenter Authorization/ date	

APPENDIX C

Computer Labs General Policies and Procedures

The Computer Lab office has instituted the following policies to ensure that equipment is available when needed and that students are able to complete their work without unnecessary distractions. If you have any comments or suggestions regarding these policies, please contact the lab office at (626) 396-2240.

1. Students rely on the computer labs to provide them proper tools, as well as a proper environment, to successfully complete their coursework. Because the labs service many students in a shared space, please act in a manner that is considerate of fellow students and treat each other with mutual respect and courtesy. Inappropriate behavior may result in a student being reported for disciplinary action and/or removal from the lab.
2. Students must wear their student IDs.
3. To protect the equipment and the work of fellow students and to ensure a clean environment, food and drinks are not permitted in the labs, even when bottled, covered or contained.
4. Student coursework always takes priority over other activities.
5. To protect personal information and College network, never share login accounts.
6. Because the computer labs are a limited, high-demand facility, rendering of files during the day is not allowed. Computers left unattended with “do not disturb” signs may be rebooted for the use of other students at the discretion of the lab staff.
7. Don’t risk losing your important files by storing them on College desktop or laptop computers. You run the risk of losing all of your work if the machine goes out for repair, or is scheduled for an upgrade.
8. Students may store their work on College servers, but should keep multiple copies of anything that is important. Files on servers are not guaranteed to be safe.
9. Moving, removing or otherwise tampering with cables is not permitted. Only computer lab staff can change cabling and configurations. This ensures that the computer will function properly for the next user.
10. Other studio materials not allowed in the computer labs include, but are not limited to, sprays and paint.
11. Students are expected to follow all laws that protect the intellectual property of others. Using the College network and/or its desktop or laptop computers to make or distribute unauthorized

copies of copyrighted materials or attempting to defeat or disable software security systems is prohibited. Students caught engaging in such activity will be reported to the Dean of Student Affairs for disciplinary action.

APPENDIX D

Cyber Security Incident Response Process

