Acceptable Use of Information Technology Resources and Services Policy

Functional Area: OITS

Applies To: All consumers and service providers of Excelsior College's Information Technology resources and services

Policy Reference(s):
Data Classification Policy

Date Issued: October 1st, 2014

Date of last review: December 29th, 2014

Date of next review: July 1, 2015

Page(s): 7

Responsible Person

This policy will be re-evaluated on or about the first day of July each calendar year to determine whether all aspects of the policy are up to date and applicable in the current business environments, and will be revised as necessary. The Information Security Director is responsible for the review and accuracy of this policy.

Purpose / Rationale

This policy sets forth standards for responsible use of Excelsior College's information technology (IT) resources.

Definitions

Information Technology (IT) resources – which include, but are not limited to computer systems, applications, networks, software, Voice over IP (VOIP) telephones, and data owned, managed, or maintained by Excelsior College.

Policy

IT resources are the property of Excelsior College and shall be designated for official College business, instructional, research, public service, administrative, and approved contract purposes.

Each individual with access to Excelsior's IT resources is responsible for ensuring these resources are used appropriately and for complying with all applicable policies and regulations within the College and with all applicable State and Federal laws and regulations.

All devices used to store, process, or transmit College information or that are otherwise connected to the College IT computer network or College owned devices are covered by this policy.

All employees and contractors must limit their personal use of College Computing Resources and refrain from using those resources for personal commercial purposes or for personal financial or other gain. Personal use of College IT resources is permitted when it does not interfere with the user's job or other College responsibilities, does not consume a significant amount of College resources, and is otherwise in compliance with this and other College policies. . Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

General responsibilities for users of IT Resources:

- Protect user ID, password, and system from unauthorized use.
- Respect the intellectual property rights of authors, contributors, and publishers in all media.
- Adhere to the terms of software licenses and other contracts.

Prohibited Use of College Computing Resources:

- Accessing or attempting to access another's accounts, data, private files, e-mail messages without the owner's permission.
- Exposing restricted or confidential information or disclosing any electronic information that one does not have the authority to disclose.
- Misrepresenting oneself or affiliation to gain access to College resources and services.
- Users may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as appropriate and required within the scope of their academic or professional duties.
- Altering system software or hardware configurations without authorization; disrupting or interfering with the delivery or administration of IT resources; facilitating access to College IT resources by unauthorized users.
- Engaging in any activity that willfully interferes with the proper functioning of the College's information technology resources. Examples include, but are not limited to, propagating viruses, damaging files, making unauthorized modifications to College data.
- Violating copyright, College trademark, and/or software agreements or applicable federal and state law by installing, copying, distributing, or using software, music, text, images, and video.
- Failure to adequately protect confidential and sensitive data by reasonable due diligence
- Using College IT resources for personal gain (i.e. commercial or profit-making purposes)
- Knowingly using IT resources for illegal activities. Criminal or illegal use may include obscenity, child pornography, threats, harassment, defamation, and theft.

Requirements for College decives toaccess College resources and services

In order to adequately protect College information systems from being compromised, users must conduct College business with Excelsior owned devices which incorporate industry sanctioned security best practices that include but are not limited to the following:

- Establish strong passwords for all computer accounts (see Password Requirements below)
- Ensure that passcode or screen locks are enabled on all mobile devices
- Ensure that all confidential information is encrypted when stored on a portable device, such as a laptop, USB thumb drive, cell phone, iPod or tablet.
- Lock or log off before leaving their computer unattended

Password Requirements

To ensure the confidentiality and integrity of all College information the following composition rules must be followed when passwords are created for computer accounts and resource access:

- Passwords must be at least eight characters in length.
- Unless unsupported by the system Passwords need to include at least one character from three of the following character groups:
    - upper case alphabetic characters (A-Z)
    - lower case alphabetic characters (a-z)
    - numbers (0-9)
    - special characters ($,!,&,etc.)

All passwords for all Excelsior systems must be periodically changed. For most systems, including network accounts, this is 90 days.

Passwords must never be shared or stored in a location accessible by others. If a user suspects passwords may have been compromised, it is the user's responsibility to contact the Office of Information and Technology Services (OITS) for procedures related to password resets. If the resource used is not under the control or operation of OITS, but another approved agency, then the user is responsible for contacting the appropriate party for assistance.

Passwords used to access confidential information should be unique from personal passwords used outside of College responsibilities.

Personal Devices

To ensure the confidentiality and integrity of Excelsior data and systems the college provides many types of approved remote access methods. In the event that these approved remote access methods are not able to be utilized the following guidelines have been established for personal devices which are used to transmit, store, access, or process any College data:

- Confidential information is not allowed to be stored on any non-Excelsior owned or provided device without OITS approved encryption.
- The personal device must run an anti-virus software package if available by the operating system, with the application kept up to date. If the device is not capable of running an Anti-Virus application, then additional security controls should be considered. OITS can assist with selection of these controls.
- The device must require a password to access

The College's Right to Access Files

Subject to applicable law, the College reserves the right to access and copy files and documents (including e-mail and voicemail) residing on College-owned equipment. The College may be required to produce data in compliance with a valid subpoena or court order.

Non-intrusive monitoring of campus network traffic occurs routinely, to assure acceptable performance and to identify and resolve problems. If problem traffic patterns suggest that system or network security, integrity, or performance has been compromised, network systems staff will investigate and protective restrictions may be applied until the condition has been rectified.

Ensuring Resource Performance

Users must not attempt to intercept, capture, alter, or interfere in any way with information on local, campus or global network pathways. This also means users may not run "sniffers" (programs used to capture information being transmitted) on the campus network or any portion thereof without authorization from the CIO or designee. Users may not operate routers, unauthorized wireless access

points or Dynamic Host Configuration Protocol (DHCP) servers on the College networks.

Users must not attempt to obtain system privileges to which they are not entitled, whether on College computers or on systems outside the College. Attempts to do so will be considered serious offenses which may result in appropriate disciplinary actions.

Computer procedures, programs and scripts that permit unauthenticated or unauthorized senders to send e-mail to arbitrary recipients from unrestricted sources are prohibited.

Users must refrain from creating and/or implementing code intended to periodically or randomly interrupt computer systems or services. Users must not intentionally propagate computer viruses. Users must not conduct unauthorized port scans. Users must not initiate nuisance or denial-of-service attacks, nor respond to these in kind. Malicious use of any device or method to disrupt network services or lessen the integrity of system data will be considered a violation of College Acceptable Use Policy.

Respect the finite capacity of College Computing Resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with College business.

Managing and Protecting Confidential Information

Employees are prohibited from accessing confidential information as defined in the Data Classification Policy unless such access is related to the employee's duties. For all confidential information such authorization may be granted to a specific individual or to all individuals serving in a specific job function. For College employees, access to confidential information is determined by business process. For non-College employees, access shall be determined by the appropriate manager in conjunction with the General Counsel’s office and OITS. All access to confidential information will be evaluated on a periodic basis to ensure access levels are still appropriate.

For confidential information, the following procedural and system-level controls must be in place:

- Departmental procedures must be in place to ensure that all individuals are aware of the sensitivity of the information to which they have access and understand their responsibilities to protect that information appropriately.
- Tangible records (e.g., memos, reports, paper documents) containing confidential information must be stored in a locked facility, cabinet, or drawer when not in use. Documents must be physically shredded/destroyed when no longer needed.
- Procedures must be in place to control physical access to electronic devices that store confidential data as well as the above mentioned hard copies.
- Employees who store or transmit information classified as confidential must encrypt both the stored data and its transmission.

Confidential information will not be stored locally on computers, flash drives, smart phones, or other devices that are easy to carry away. If it is absolutely necessary to store sensitive or confidential information on such a device due to a business requirement, the information must be encrypted to protect it from view should the device fall into unauthorized hands. **The necessity to store such**

information outside of the College maintained Network or approved Cloud Computing Service must be reviewed and approved by OITS, College Counsel, and the appropriate Vice President.

Employees who store or transmit confidential data on portable devices are responsible for ensuring that the information is backed up regularly in a form that permits ready retrieval.

In the event of unauthorized access to College data, whether through theft or loss of portable devices such as USB drives, laptops, smart phones or other devices, or any other kind of breach of security, the individual who is responsible for the device or who learns of a potential breach must notify the Information Security Director and assist with the College's data breach response. In case of theft of College-owned equipment, this individual must also contact Police to file a police report and notify the Information Security Director.

College-endorsed encryption products or protocols must be used confidential data. Employees should consult OITS for an appropriate product or protocol and to obtain assistance with implementing this requirement.

Data Security Practices and Requirements

All Employees:

1. Must ascertain and understand the classification level of information (reference Data Classification Policy) for which they have been authorized to access.
2. Must adhere to College's requirements for protecting any computer used to conduct College business regardless of the sensitivity level of the information held on that system
3. Must protect the confidentiality, integrity and availability of the College's information wherever the information is located (e.g., physical documents, storage media, telecom system or data networks).
4. Must safeguard any physical key, ID card or computer/network accounts that allow them to access College information.
5. Must destroy or render unusable any confidential information contained in any physical document or any electronic, magnetic or optical storage medium (e.g., USB drive, CD, hard disk, magnetic tape, or diskette) before it is discarded.
6. Must report any activities that they suspect may compromise sensitive information to their supervisor and the College Information Security Director.
7. Must protect sensitive information even after leaving the College.
8. Must consult General Counsel upon receiving investigative subpoenas, court orders, or any other requests for confidential information.
9. Must exercise caution in not posting sensitive or confidential information in forums, newsgroups, or other public mediums that may risk the integrity of College data.

Additional Responsibilities for Supervisors and Managers:

In addition to complying with the requirements listed above for all College employees, managers and supervisors should:

1. Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the Information Security Director or appointee, and that those procedures are followed.

2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
3. Ensure that each employee understands his or her information security-related responsibilities.
4. Ensure that the requirements for confidentiality, integrity and availability are satisfied within their environments by:
    - Developing, implementing, operating and maintaining a secure technology environment
    - Ensuring that employees are trained on proper procedures for the classification and handling of data and the measures used to secure it.

Additional Responsibilities for OITS Employees:

OITS maintains and operates both internal and external resources that house, transmit, and create user information and data. As such, OITS has developed appropriate safeguards and security related procedures.

OITS will perform bi-annual review of these internal and external resources. These reviews will include, but are not limited to, the following:

- Appropriate administrator access level for each OITS staff position
- Firewall configuration review of systems and network resources
- Log reviews
- Service patches, anti-virus, malware protection review
- System load and performance review
- Disaster recovery procedures review
- Backup status/location
- Verification of backups

Cloud Computing Considerations:

This pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

If you are not sure whether a service is cloud-based or not, please contact OITS.

- Use of cloud computing services for work purposes must be formally authorized by the business owner, VP, and appropriate commitee. These entities will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by counsel.
- The use of such services must comply with the College's existing Acceptable Use Policy.
- Employees must not share log-in credentials with co-workers.
- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by Excelsior College.

- The business owner, VP, and appropriate committee willdecide what data may or may not be stored in the Cloud.
- Personal cloud services accounts may not be used for the storage, manipulation or exchange of confidential data. This includes personal email, Dropbox[1], twitter, facebook, and any other non Excelsior College implemented cloud technology.

Exceptions to the AUP

When it is technically unsupported or a business process has a need for an exemption to any requirements of this Acceptable Use Policy they must request an exemption. These requests will be reviewed by the VP- Information Technology and the Information Security Director. If approved they will be documented as an approved exception to the Acceptable Use Policy. Acceptable Use Policy exceptions will be evaluated by OITS on a yearly basis to ensure they are still required.

[1] Dropbox and other file sharing **for non confidential information** will be allowed until such time as Excelsior College implements a technology to replace it.