CNU

INFORMATION TECHNOLOGY SERVICES

Information Technology Policy Guide

September 18th, 2014

Prepared By ITS & CNU Partner Communities

Table of Contents

Introduction

This guide is the collection of policies that govern the use of Information Technology (IT) at Christopher Newport University (CNU). All users of computing, voice and data systems owned and/or operated by CNU may use any system for which they have been authorized, subject to and within the parameters set forth in this guide. This guide is not meant to be an all inclusive representation of every federal, state and local policy, guide and standard, yet a document that houses information of particular value to CNU faculty and students.

CNU values the productive use of all IT systems. Use that promotes the positive image of the university, furthers professional and academic growth, facilitates the performance of employees' duties and contributes to a beneficial quality of life for residents is encouraged.

Violation of any policy must be reported to the Information Security Officer. The enforcement of any policy will be the responsibility of the supervisor, department head, Information Security Officer, Campus Police, Human Resources personnel or any combination thereof, depending on the circumstances of any given violation. Violations or illegal activity may result in disciplinary action, including but not limited to termination of employment in addition to legal courses of action.

These policies are written to primarily support and protect four vital interests:

- Quality of Life
- Academic Freedom
- Confidentiality, Integrity & Availability (CIA Model)
- Forensics

Quality of Life

The lives of students, faculty, staff and residents are all affected by IT systems. Residents deserve an environment that allows them to pursue academic and personal interests. These are ensured by policies that prohibit activities that would hinder their productivity in the classroom and enjoyment in their dormitories and apartments, while balancing the needs of all students through the regulation of bandwidth and management of network traffic.

Faculty interests are accounted for by implementing policies that shape the use of technologies in the classroom and ensure the issuance of new technologies on a regular basis. For administrative staff, technology replacement cycles and methods provide state-of-the-art equipment for the performance of their duties.

Overall, these policies ensure all users of IT systems have access to available services while preventing undue impact to others, govern productive use of campus technologies and create adaptable guidelines for a changing environment.

Academic Freedom

CNU subscribes to the principals of academic freedom as defined in the *University Handbook 2013–2014 Edition* Section II Board of Visitors - Academic responsibility implies the faithful performance of professional duties and obligations. Faculty members have the obligation, as a member of a learned profession and employee of the University to attempt to be accurate, to exercise appropriate restraint, to show respect for the opinions of others, and to make every reasonable effort to indicate that the faculty member is not an institutional spokesperson. Faculty members will be guided by academic ethics and professional standards.

A misapplication of academic freedom will not be justification for unreasonable or irresponsible uses of CNU IT systems, the violation of IT policy, or inhibiting the creation of any reasonable policy.

All ITS policies serve to protect the interests of CNU, staff, faculty and students. Specific to academic freedom, these policies serve to further the knowledge, truth-finding pursuits, academic endeavors and research performed by members of the faculty. These policies are written to protect those freedoms, as well as the personal and confidential information of each faculty member, staff member and student. Some polices or portions thereof may conflict with the ideals of academic freedom.

Confidentiality, Integrity & Availability

In accordance with the Department of Human Resource Management Policy 1.75, "Use of Electronic Communications and Social Media" no user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth's equipment and/or access. CNU maintains the right to monitor any and all aspects of electronic communications and social media usage to maintain the integrity and availability of university information and data. Such monitoring may occur at any time, without notice, and without the user's permission. In addition, except for exemptions under the Act, electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore, available for public distribution.

Prevention and Forensics

ITS is committed to preventing the use of IT systems for illegal activities and activities that violate the confidentiality of personal data. Since not all activities can be prevented, the need to gather and analyze forensic information is also required.

ITS will employ systems that gather and analyze data in the effort to support investigations, assist law enforcement efforts and protect confidential and valuable information. Such information will only be used for such purposes and will never be shared, disseminated or otherwise made available to others who are not directly involved in the investigation.

Acceptable Use of Computing Resources Policy

CNU Policy 1000 (Security Policy)

All traffic and the contents thereof which traverse the CNU computer network, all CNU-supplied computers and related technologies and all correspondence including but not limited to files, e-mail and respective attachments, instant messaging, text messaging, voice and video calls are subject to the rights reserved by CNU to manage to the extent deemed necessary any communication or the contents thereof.

Upon termination, resignation, withdrawal or status change of an employee or student, these materials remain the property of CNU, and shall be relinquished as such. ITS reserves the right to require the removal of any computing device or technology that does not meet the minimum specifications as defined on the ITS web site, which also includes devices (hardware & software) that pose a risk to test, development and production systems, either by creating vulnerabilities in the environment, exploiting software that would allow unauthorized access or creating undue network traffic to exist.

Members of the general public and/or people unaffiliated with CNU may use computing resources as available and authorized for such a purpose by the Information Technology Services department. Such use shall be restricted to accessing the Internet and any CNU resources intended for use by the public.

The CNU community may use Christopher Newport University (CNU) systems for authorized purposes. Unauthorized access to or use of any system is prohibited.

The following activities are expressly prohibited:

- Installing, copying, distributing, sharing or otherwise making available or using software , files or content of any kind in violation of any local, state or federal law, copyright law and/or End User Licensing Agreement.
- Altering system software or hardware or disrupting or interfering with the delivery or administration of system resources.
- Misuse of computing resources directed toward people or entities outside of CNU.
- Attempting to circumvent or subvert any security measure.
- Accessing or attempting to access or facilitating access to another user's account, server, workstation, computing device, files, voice mail or e-mail without the owner's permission.
- Sharing personal information, including but not limited to account information, user credentials and/or access to university systems (see **User Credentials** policy).
- Misrepresentation of identity in electronic communication.
- Engaging in conduct or the use of computing resources which interferes with others' use of IT systems, the activities of other users or otherwise impedes workplace productivity.
- Using computing resources unrelated to one’s position at the university for commercial interests, profit-making purposes and/or personal gain without written authorization from CNU.
- Failing to adhere to individual department and/or CNU policies, procedures, protocols or using systems in a manner contrary to their intended use.
- Acts of vandalism, theft or tampering with computer resources.
- Using ITS resources for any activities CNU, the state of Virginia or federal law have determined illegal, inappropriate or unacceptable. Such activities may include but are not limited to:

    - Identity theft
    - Pornography
    - Threats
    - Harassment, including sexual harassment
    - Theft
    - Terrorist activities
    - Violence
    - Unauthorized access

- Installation, implementation or use of any unauthorized computing device or protocol, which includes but is not limited to:
    a. Routers
    b. Wireless Access Points
    c. Switches/Hubs
    d. DHCP servers
    e. DNS servers

- The propagation of computer viruses, worms or other similar programs.

Systems & Mobile Devices with Sensitive Data
ITS Policy 1100 (Systems with Sensitive Data)
ITS Policy 1510 (Data Transport Policy)
COV ITRM Guideline SEC 507-00

All user information that is protected under local, state and federal law is confidential and is to be stored in a secure manner. Information not protected by law is sensitive and shared accordingly. Confidential information is only shared between and disseminated to others in the necessary performance of job duties. When required to support the investigation of prohibited activity, such information may be shared with the appropriate agencies to help further such an investigation. Information will also be disclosed to relevant parties in order to fulfill any requirements pursuant to a subpoena issued for such a purpose under the direction of the ISO, any Vice President or the President. Such sharing will be limited to only those people, whose efforts are required, and such personnel shall respect the sensitive, confidential nature of such an investigation and the information and individuals involved.

All sensitive information, data, and/or files containing sensitive data must be stored in an ITS approved secure location.

- Shared drive
- Secure database
- Encrypted media

Mobile storage media includes any data storage medium, which may be easily transported by an individual without any special equipment which includes but not limited to:

- Portable External Hard Drives
- Laptops, tablet PCs
- Smart Phones and Personal Digital Assistants (Android, iPhone, Blackberry, Etc.)
- Compact and Digital Video Disks (CDs/DVDs)
- Flash Drives (memory stick, USB drive, SD Cards, Etc.)

Such information shall only be shared between and released to authorized parties with a need to know and as necessary to execute job-related duties. No person identifiable information or sensitive data may be transported off of CNU's campus by any means except with the written permission of the appropriate Department head or Vice President. This information includes any of the following:

- Private Information (Social Security Number, Date of Birth, Driver's License Number)
- Health Information Portability and Accountability Act (HIPPA)
- Federal Educational Rights Privacy Act (FERPA)
- Student identification number (ID#)
- Bank account numbers
- Credit or debit card numbers
- Other banking information in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Any Personally Identifiable Information transported off campus via electronic means (laptop, pda, smart phone, flash drive, backup tape, cd, etc) must be protected with the following means:

- The data and device must be encrypted and locked with a password
- The data may only be stored for the specific time period during which it is being used
- The data must be deleted immediately after use
- Only the minimum amount of information needed for the current purpose should be stored
- The computer on which the information is used must have current anti-virus protection
- The computer on which the information is used must have current vendor patch levels, with automatic patching enabled where available
- The computer on which the information is used must have a firewall installed and enabled

In an effort to minimize the amount of sensitive or private information on systems in the CNU environment, a product named Identity Finder has been purchased to identify the exact location of this information. It is faculty and staff responsibility to eliminate or redact this information if it is not needed. There are only a few departments that must have access to this data. To eliminate or minimize the risk for significant fines levied against the university, faculty and staff should use the Identity Finder tool to identify, eliminate or redact this information as quickly as possible.

Electronic Document Retention & Destruction
Library of Virginia ~ Electronic Records Guidelines
Virginia Public Records Act (Code of Virginia, 42.1 ~ 76-91)
Virginia Uniform Electronic Transactions Act (59.1 ~ 479-498)

The Library of Virginia has an extensive list of requirements for document retention as well as established procedures for the destruction of those documents. These guidelines now extend to electronic documents and email. It is each person's (Faculty and Staff) responsibility to ensure they keep documents for the prescribed timeframes as well as removing them within a timely manner for records scheduled for destruction. Keeping electronic documents past their prescribed timeframes subjects them to the Virginia Freedom of Information Act and the Privacy Act.

Some suggestions include creating a naming convention and filing system to store electronic documents so documents can be quickly found when needed. Email can quickly become unruly if not continually managed. Some suggestions include:

- Delete email that doesn't need to be retained as public records
- It is not always necessary to retain email, which you are not the primary recipient. Internally generated and sent to a primary recipient within the agency, the email should be maintained by the primary recipient.
- Sort messages by sender and purge personal correspondence.
- Retain only the final email in a thread
- Permanently delete items in your deleted items folder on a regular basis.
- File your email regularly.

E-mail / Portal Use Policy

CNU Policy 4000

Access to the Christopher Newport University Network is not a right but a privilege granted to individuals in designated categories. The CNU e-mail system shall be used for purposes that further university goals. This policy covers appropriate use of any e-mail sent from a CNU e-mail address and applies to all employees, vendors, and agents operating on behalf of the University.

Pursuant to the CNU Acceptable Use Policy, all traffic and the contents thereof which traverse the CNU computer network, all CNU-supplied computers and related technologies and all correspondence including but not limited to files, e-mail and respective attachments, instant messaging, text messaging, voice calls and video calls are subject to the rights reserved by CNU to manage to the extent deemed necessary any communication or the contents thereof.

Persons may not use e-mail in inappropriate ways or in violation of CNU policy or local, state or federal laws. This includes, but is not limited to:

- Stalking, harassment including sexual harassment, hate speech, or other unlawful activity.
- Sending or forwarding private or sensitive information (e.g. social security numbers, credit card information, user credentials) in an unencrypted format (see the **Sensitive Data** Policy).
- Fraudulent acts, including the use of a deceptive alias to disguise one's true identity.
- Intentional distribution of viruses (real or simulated) or otherwise destructive software using E-mail.
- Any use of CNU resources for personal commercial gain, solicitation for self or other promotion except in cases of officially sanctioned University activities.
- Participation in chain-letters.

Any communications may become the subject of litigation. As such, disclosure shall be granted pursuant to any subpoena filed for such a purpose upon direction from the CIO, any Vice President or President.

E-mail containing official business of CNU shall be addressed to an official university e-mail address and should not be addressed to alternative addresses. Such e-mail shall not be automatically forwarded to an external address. CNU employees shall only use CNU e-mail systems for conducting official university business. The use of private or third-party e-mail systems for official business is prohibited.

University officials and supervisors shall be permitted to read any e-mail when written permission has been granted by the Chief of Staff, CIO, or Vice Presidents. E-mail accounts will be accessed by system administrators for the purposes of maintenance, forensics, and/or to support investigations. ITS reserves the right to filter, reject and/or remove any e-mail that is suspected to contain viruses, phishing attempts, spam or other harmful or inappropriate content

Upon employee termination, resignation, or withdrawal, these materials remain the property of the University and any associated e-mail account(s) will be terminated. All information not retained by CNU will be deleted. Exceptions to this policy may be granted for individuals who maintain a continued relationship in good standing with CNU and who actively use their accounts.

User Credentials Policy
ITRM Standard SEC501-06
ITS-1600 (Password Management)

User credentials consist of a combination of a username and password, which together permit access to individual accounts and the resources for which that user is authorized. The safekeeping of each credential is the responsibility of the user. This policy applies to all university owned, maintained and managed devices as well as personally owned devices (computers, mobile devices, etc.) used to gain access to university data.

Users must never disclose or share credentials with anyone!

Passwords must be sufficiently complex in order to deter certain types of guessing or brute force attacks. Therefore, all passwords must conform to the convention mandated by the Commonwealth and ITS Standards:

- Must be a minimum of 8 characters
- Combination of Upper and Lower Case letters
- Numbers
- Special Characters
- Must be changed every 90 days
- Must not be reused for at least the last 22 passwords

Passwords must be changed upon first login and at least every 90 days thereafter. In the event a user discloses his or her credentials to an unauthorized party, the password must be changed immediately. Due to the complexity requirements in conjunction with the number of passwords a user has, people may wish to use an ITS authorized password safe. Users should refrain from posting passwords on computer monitors, hiding pieces of paper under keyboards or other similar methods.

Server and System Level Passwords
All server/system-level passwords must be changed from vendor defaults and/or after an employee with whom the account was shared is no longer authorized to access the account(s). All server/system-level passwords must be no less complex than standard user passwords.

Password Protection
All passwords are confidential. If an account or password is suspected to have been compromised, report the incident to the Information Security Officer and immediately change the password(s) affected.

Since all users are responsible for the safekeeping of their passwords, they may be held responsible for activity from systems that are accessed with their credentials.

New Account Creation
All authorized users shall be issued credentials using a process defined by ITS. For new hires, this process shall be defined and agreed upon by ITS and Human Resources. Additional authorizations and/or credentials shall be issued as appropriate to any user requiring access to resources not accessible using their standard credentials.

For employees, such authorizations shall be modified as required by the user's job responsibilities. Access shall be de-provisioned and/or modified upon any change in the user's relationship with CNU.

Workstation Security
All employee workstations must be locked when not attended by the user. This will be systematically applied after 15 minutes of inactivity or should be imposed immediately by all faculty and staff when leaving their work areas.

Use of Electronic Communications and Social Media

Department of Human Resource Management Policy 1.75

On an annual basis, Faculty, Staff and Contract staff will electronically acknowledge the Use of Electronic Communications and Social Media while using electronic resources at CNU. Use of these systems carries heavy penalty if not used appropriately and for official use only. The statement reads as follows:

> ***I have been given a copy of Department of Human Resource Management Policy 1.75, "Use of Electronic Communications and Social Media" and I understand that it is my responsibility to read and abide by this policy, even if I do not agree with it. If I have any questions about the policy, I understand that I need to ask my supervisor or the agency/institution Human Resource Officer for clarification.***
>
> ***I understand that no user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth's equipment and/or access. Agencies have a right to monitor any and all aspects of electronic communications and social media usage. Such monitoring may occur at any time, without notice, and without the user's permission.***
>
> ***In addition, except for exemptions under the Act, electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore, available for public distribution. If I refuse to accept and comply with the responsibility, my supervisor will review this statement with me and will be asked to initial this form indicating that a copy has been given to me and that this statement has been read to me.***

Purchasing Questionnaire

For any hardware, software or cloud based service purchase where CNU data will be used in or part of, the following questionnaire will be required and should be attached to all requisitions within eVA. If the purchase is a credit card purchase, please contact IT Services prior to completing the purchase to discuss various aspects of the project. This form will aid in mitigating the risk of losing CNU sensitive or private data. Failure to provide complete detail of purchases prior to completing them stands to cause significant risk to CNU if this data is put on systems that are found to be unsecure.

Purchasing & IT Services

Data Classification & Security Questionnaire

Please complete this document in combination with any purchase you or your department may be considering where CNU data may be contained. This includes but is not limited to purchases where Faculty, Staff or Student data may be housed (server, computer, storage device, etc.) or placed in a vendor environment (cloud storage, vendor database, etc.). There are many risks associated with storing CNU data in external systems. The overarching risk is the loss or breach of this data by unauthorized parties whose main intent is to use it for illegal purposes. While not the intent of most of our vendors, the intent of this questionnaire is to protect the confidentiality and integrity of the data, ensure data is not leaked or breached and maintain authoritive sources for access in accordance with Virginia and CNU policies and guidelines.

Please complete the questionnaire with as much detail as possible. If you are unsure about a particular question, please contact purchasing or IT services.

- -

Will the technology or service you are procuring house CNU data (Faculty, Staff, Student, Alumni, Other)? ______________________ If yes, please attach all supporting documentation (contract terms & conditions, quote, estimated implementation date, vendor points of contact). **If CNU data will not be stored; stop here.**

What data will be stored (name, social security, address, course data, student class data, health information, etc.). A determination of risk will be assessed dependent on the type of data (Ferpa, Hippa, Sensitive), where it will be stored and who has access to it. Dependent on the risk, data may or may not be allowed to be housed on these systems.

Who will administer the system (Vendor, CNU Employee) ?

What expectation is there for departments to develop customized interfaces to access data?

What on-going expectation is there to maintain data, and who will complete the updates?

Additional information you feel to be critical to this request?

It is our hope the information contained in this document helps in defining your responsibility in keeping CNU data and information systems secure. Any questions or comments can be directed to Stephen Campbell, Information Security Officer/Information Security Officer; (757) 594-7663 or sc@cnu.edu.