Central Community College Accessibility Guidelines

All faculty and staff play a vital role in Central Community College's success to ensure the goals of Web Accessibility are met in a timely manner. Each department contributes by implementing web accessibility best practices and supporting efforts related to training, assessing and creating accessible web content. Ensuring all official college web-based information conforms to the Web Content Accessibility Guidelines 2.0 (WCAG)- Level AA is a priority of the institution.

***Purpose:**
The purpose of these guidelines is to provide guidance to the college community on Central Community College's commitment to equal access to information technology (IT). Following the guidelines helps to ensure that people with disabilities have access to the same services and content that are available to people without disabilities, including services and content made available using information technology. These guidelines apply to all web-based information and services which includes, but isn't limited to, websites, instructional materials, and online systems that are developed, hosted or maintained by CCC. IT procured, developed, maintained and used by the college should provide substantially similar functionality, experience, and information access to individuals with disabilities as it provides to others.

***Accessibility Defined:**
Accessible can be defined as "a person with a disability is afforded the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services as a person without a disability in an equally effective and equally integrated manner, with substantially equivalent ease of use. The person with a disability must be able to obtain the information as fully, equally, and independently as a person without a disability." (OCR Compliance Review No. 11-11-6002)

***College Implementation:**
CCC makes our top priority systems accessible to the most users with the highest regard given to public-facing systems and student-facing systems. The following areas have been identified as the major concentration of these accessibility standards:

1. Central Community College Website and Extension Sites ~~including, but not limited to, the Raider Athletic website.~~
2. Student course materials and documents.
3. Student and public facing technology and software.

Administrative Responsibilities

President
The President shall be directly responsible to the Central Community College Board of Governors (i.e., Board) for the overall administration of the College. His/her title shall be "President," Central Community College. The President's delegated duties include:

- Act on behalf of the Board during times the board is not in session.
- Meet with the Board or Committees of the Board for the purpose of reporting, advising, and recommending in all phases of operation of the College.
- Provide information to assist the Board in effective decision-making and sound policy formation.
- Recommend College policies and policy changes to the Board.
- Report, interpret, and implement policies and actions of the Board to all employees of the College and to the citizens of the 25-county area.
- Administer the business management of the College and direct the development and preparation of the annual budget for the College and the operation and maintenance of all College properties.
- Recommend educational, instructional, and physical plant changes.
- Evaluate and recommends changes to the programs and operations of the college to ensure board approved policies and state requirements are followed, and to avoid unnecessary duplication within the College operation.
- Recommend full-time instructional staff and College administrative staff at dean level and above for appointment, assignment, transfer, suspension, promotion, or dismissal.
- Create, reorganize or disband committees, divisions or organizational units as needed for efficient college operations.
- Appoint, assign, transfer, suspend, promote, or dismiss all employees other than those previously mentioned.
- Determine and approve job descriptions and titles for all staff.

Campus President – Columbus/Division Vice President - Acts as the chief executive officer of the Columbus Campus and is responsible for overall administration of assigned College-wide programs including ~~Academic Education and Extended Learning Services and Training and Development.~~Arts, Sciences & Business and Adult Education. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. Reports directly to the President regarding assignments of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Campus President – Columbus/Division Vice President represents the staff of the Columbus Campus as a voting member of the College Cabinet.

Campus President – Grand Island/Division Vice President - Acts as the chief executive officer of the Grand Island Campus and is responsible for overall administration of assigned college-wide programs including ~~Student Services and~~ Health Sciences and Nursing. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. ~~The~~ Reports directly to the President regarding assignments of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Campus President – Grand Island/Division Vice President represents the staff of the Grand Island Campus as a voting member of the College Cabinet.

Campus President – Hastings/Division Vice President - Acts as the chief executive officer of the Hastings Campus and is responsible for overall administration of assigned college-wide programs including Skilled ~~and~~ & Technical Sciences ~~and Business~~. The duties, responsibilities, and authority of this position are

delegated by the President following the policies of the College's Board of Governors. Reports directly to the President regarding assignments of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Campus President – Hastings/Division Vice President represents the staff of the Hastings Campus as a voting member of the College Cabinet.

Vice President of Community & Workforce Education - Acts as the primary administrator of the Kearney Campus and is responsible for overall administration of assigned college-wide programs including community education, early college, workforce training & development, and programming in Kearney, Lexington, Holdrege and Ord centers. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. Reports directly to the President regarding assignments of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Vice President of Community & Workforce Education represents the staff of the centers as a voting member of the College Cabinet.

Vice President of Innovation and Instruction – Serves as the College's chief instructional representative for all external affairs. Responsible for coordinating and assisting in the planning, developing, and evaluating instructional services, and designated supportive services of the college, including regional accreditation, institutional reports, college communications, and grants. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. Reports directly to the President regarding assignment of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Vice President of Innovation and Instruction is a non-voting member of the College Cabinet.

Vice President of Administrative Services - Coordinates the business and facilities operations of the College. Responsible for coordinating and assisting in the planning, developing, and evaluating information technology, purchasing, payroll, environmental health and safety, security and other areas and area facilities including annual audits and state fiscal reports. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. Reports directly to the President regarding assignments of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Vice President of Administrative Services is a non-voting member of the College Cabinet.

Vice President of Student Success & Enrollment Management - Coordinates the student success and enrollment services of the College. Responsible for coordinating and assisting in planning, developing, and evaluating student development, registration, admissions, financial aid, advising, residence halls, student conduct, veterans services and other related offices, services and functions including audit and compliance functions. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. Reports directly to the President regarding assignments of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Vice President of Student Success & Enrollment Management is a non-voting member of the College Cabinet.

Senior Director of Human Resources - Coordinates and leads the human resources services, systems, and policies of the College. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. Reports directly to the President regarding assignments of responsibility and for evaluation of performance of duties, and may act for the President during absences. The Senior Director of Human Resources is a non-voting member of the College Cabinet.

CCC Foundation Executive Director - Coordinates and leads the College's Foundation and reports directly to the CCC Foundation Board. The duties, responsibilities, and authority of this position are delegated by the President following the policies of the College's Board of Governors. Reports indirectly to the President regarding assignments of responsibility and for evaluation of performance of duties. The CCC Foundation Executive Director is a non-voting member of the College Cabinet.

Clothing Procedures

The College may provide personal clothing for employees as follows:

A. Rental of smocks, overalls, uniforms, shirts, and pants.
B. Purchase of t-shirts, ~~or~~ polo shirts, or jackets with the College/campus logo when associated with a College activity.
C. Purchase of uniforms for security personnel.
~~C.~~D. Standardized graduation regalia.

College Cabinet Policy

The College Cabinet is comprised of the President, Vice President of Innovation and Instruction, College Vice Presidents/Campus Presidents, Vice President of Administrative Services, Vice President of Community & Workforce Education, Vice President of Student Success & Enrollment Management, Senior Director of Human Resources, Foundation Executive Director, and a faculty and staff representative who shall meet approximately two weeks before each board meeting for the purpose of coordinating activities of the College.

Computer Usage Procedure

Each employee shall avoid sharing or allowing others access to individual computer passwords or user codes. If employees know or suspect their password is known by another individual, the employee must notify the Information Technology (IT) Department personnel immediately.

It shall be considered unauthorized access and/or a violation of the College's Technology Agreement and Neb. Rev. Stat. §§28-1343 to 28-1347 for an employee to:

A. Use of another employee's password and/or user codes;
B. Access a computer system or network without authorization or exceeding the limits of authorization;
C. Deprive or unlawfully obtain property or services;
D. Alter, damage, delete, or destroy programs or data; or
E. Obtain confidential information from a computer system.

Any employee who knowingly violates the Technology Agreement shall be subject to disciplinary action.

Administration
Board adopted 5/15/14

Diversity Policy

The College shall conduct workshops, seminars, make distribution of publications, and engage in other activities to promote understanding and benefits of diversity for employees.

The following community colleges endorse the *Statement in Support of Diversity in Higher Education* and remain strongly committed to taking steps, appropriate to their mission and circumstances that advance inclusion and pluralism in our institutions.

- Nebraska Community College Association Board of Directors
- Central Community College Area Board of Governors
- Metropolitan Community College Area Board of Governors
- Mid-Plains Community College Area Board of Governors
- Northeast Community College Area Board of Governors
- Southeast Community College Area Board of Governors
- Western Community College Area Board of Governors

Commented [AD1]: This is now part of the Civil Rights Policy

Drug and Alcohol Testing Policy

It is the policy of the College that the use, possession, or presence of alcoholic beverages or illegal drugs by employees while on duty and students, in a vehicle or on property owned or used by the College is prohibited. Employees or students shall not report for duty, be on College controlled property, or at a College activity under the influence of any alcoholic beverage or illegal drugs. Violations of this policy will be governed by the College Drug and Alcohol Testing Procedure.

For purposes of this policy, the term "illegal drug" means intoxicants and narcotics, marijuana, or any other controlled substance as defined by Nebraska or Federal law. The term "illegal drugs" does not include any medication, which has been lawfully prescribed to be used by the student or employee.

Violation of this policy shall be grounds for participation in an alcohol abuse program and/or the termination of employment or dismissal from the College.

Drug and Alcohol Testing Procedures

The results of any tests performed on the body fluid or breath specimen of a student or an employee, as directed by the College to determine the presence of drugs or alcohol shall not be used to deny any continued employment or administrative action unless the following requirements are met: (1) a positive finding of drugs by preliminary screening procedures has been subsequently confirmed by a method which has been or may be approved by the Nebraska Department of Health; or (2) a positive finding of alcohol by a preliminary screening procedure is subsequently confirmed by either: (a) gas chromatography or other method which has been, or may be approved by the Nebraska Department of Health; or (b) a breath-testing device operated by a trained and certified operator.

Types of Tests
The College may conduct drug and alcohol tests in three circumstances: (1) pre-employment for full-time and specified part-time positions, (2) to be in compliance with external entities that require a drug-screen (ex. clinical locations, etc.), and (3) for reasonable cause. Pre-employment testing shall be paid by the College.

Pre-Employment Testing
When required, applicants for employment must consent to a urine drug screen. The test shall be administered after a conditional offer of employment has been extended. If the applicant tests positive, the conditions for employment shall be deemed not to have been met and the applicant shall not be hired.

Compliance with External Entities Testing
When required, employees shall consent to a urine drug screen or breathe test per the requirements of external entities. The employee shall also be requested to execute a consent form authorizing the analysis of his or her urine for the purpose of determining the presence of illegal drugs and/or blood or breathe tests to determine alcohol content. The form shall authorize the release of the written results of such tests to the College. The refusal of an employee to submit a urine specimen, blood test, breath sample test, or execute a consent form when requested to do so shall be grounds for discharge or dismissal. If the employee tests positive for drug or alcohol use, the conditions for compliance with

external entities shall be deemed not to have been met which may result in disciplinary action up to and including termination.

Reasonable Cause

If the Senior Director of Human Resources for employees or the Campus President for students concludes that reasonable cause exists to believe that an employee is demonstrating characteristics of illegal drug use or alcohol use, the employee shall be requested to submit a test of his or her urine for the purpose of determining the presence of illegal drugs. A gas chromatograph, blood test, or other approved method shall be used to determine blood alcohol content. The testing shall be performed by a trained and certified operator under the supervision of the Senior Director of Human Resources, or by such other persons as may be designated by him/her. The employee or student shall also be requested to execute a consent form authorizing the analysis of his or her urine for the purpose of determining the presence of illegal drugs and/or blood or breathe tests to determine alcohol content. The form shall authorize the release of the written results of such tests to the College. The refusal of an employee or student to submit a urine specimen, blood test, breath sample test, or execute a consent form when requested to do so shall be grounds for discharge or dismissal.

Reasonable grounds for requesting that an employee or student submit to testing and execution of a consent form shall be deemed to exist when the employee or student manifests physical or physiological symptoms or reactions commonly associated with the use of a controlled substance or alcoholic beverages. Reasonable grounds include but are not limited to: the odor of alcohol on the breath; slurred or thick speech; apparent loss of coordination or unsteady gait; or uncharacteristic emotional behavior. Reasonable grounds shall also be deemed to exist whenever an employee or student is involved in an accident while on duty, which results in an injury to himself or herself or any other person, or which causes damage to the College property or the property of another individual.

Refusal to Test

Refusal to submit to the types of drug and alcohol test employed by the College shall be grounds for refusal to hire applicants, to terminate employment of existing employees, and to dismiss students. A refusal to test is defined to be conduct, which would obstruct the proper administration of a test. A delay in providing the urine, blood, or breath specimen could be considered a refusal. If an employee or student cannot provide a sufficient urine or blood specimen or adequate breath, he/she shall be evaluated by a physician of the College's choice. If the physician cannot find a legitimate medical explanation for the inability to provide a specimen (either urine or breath), it shall be considered a refusal to test. In that circumstance, the employee shall be subject to termination or the student to dismissal.

Drug Urinalysis

Drug testing shall be performed through urinalysis. Urinalysis shall test for the presence of drugs and/or metabolites considered to be a controlled substance, including but not limited to the following substances: (1) marijuana, (2) cocaine, (3) opiates, (4) amphetamines, and (5) phencyclidine (PCP); or a controlled substance as defined by the federal Controlled Substances Act (21 U.S. C§801 et. seq) or Nebraska Uniform Controlled Substances Act (Neb. Rev. Stat. §28-401 to §28-456.01 and §28-458 to §28-462), as such laws may from time to time be amended. The urinalysis procedure starts with the collection of a urine sample. Urine specimen shall be submitted to and all confirmatory tests shall be performed by a clinic, hospital, or laboratory which is licensed pursuant to the federal Clinical Laboratories Improvement Act of 1967, 42 U.S.C. 263a, or which is accredited by the College of American pathologists for testing.

As part of the collection process, the specimen provided shall be split into two vials: a primary vial and a secondary vial. A certified laboratory shall perform initial screenings on all primary vials. In the event that the primary specimen tests positive, a confirmation test of that specimen shall be performed before being reported by the laboratory to the Medical Review Officer (MRO) as a positive.

A written record of the chain of custody of the specimen shall be maintained from the time of the collection of the specimen until the specimen is no longer required.

All Laboratory results shall be reported by the laboratory to an MRO designated by the College. Negative test results shall be reported by the MRO to the Senior Director of Human Resources for employees or Vice President of Student Success for students. Before reporting a positive test to the College, the MRO shall attempt to contact the employee or student to discuss the test result. If the MRO is unable to contact the employee or student directly, the MRO shall contact the Senior Director of Human Resources for employees and Vice President of Student Success for students, who shall, in turn, contact the employee or student and direct the employee or student to contact the MRO. Upon being so directed, the employee or student shall contact the MRO immediately or, if after the MRO's customary business hours, then the start of the next business day. In the MRO's sole discretion, a determination shall be made as to whether a result is positive or negative.

An individual testing positive may make a request of the MRO to have the secondary vial tested. The employee or student may request that the secondary vial be tested by a different certified lab than that which tested the primary specimen. The individual making the request for a test of the second specimen must prepay all costs associated with the test. Request for testing of a second specimen is timely if it is made to the MRO within 72 hours of the individual being notified by the College of a positive test result.

Alcohol Tests

The College shall perform alcohol tests using an approved breath testing device. The College shall utilize the approved breath testing device provided by a vendor or agent. Employees or students shall report to the site of the approved breath-testing device as directed by the College. The approved breath-testing device shall be operated by a certified breath alcohol technician. The employee or student shall follow all instructions given by the certified breath alcohol technician. Employees or students with tests indicating a blood alcohol concentration in violation or the then-current state limit for driving or greater are considered to have engaged in conduct prohibited by this policy which may result in disciplinary action up to and including termination. All alcohol tests (except pre-employment) shall be performed just prior to, during or just after employee's work time.

The College shall insure supervisors or deans designated to determine whether reasonable suspicion exists to require an employee or student to undergo testing to receive training on alcohol misuse and training on controlled substance use. Training shall cover the physical, behavioral, speech, and performance indicators of probable alcohol misuse and use of controlled substances.

Confidentiality

The results of any ~~urinalysis~~ tests conducted under this policy shall be made available to the employee or student and the Senior Director of Human Resources for employees or Vice President of Student Success for students. Results for employee tests shall be maintained by Human Resources. The results of such tests shall not otherwise be divulged to any other person except when approved by the President. The College shall not be precluded, however, from divulging such test results upon request

from agencies of local, state, or federal government; in any administrative or judicial proceeding wherein the results of such a test are relevant to the issues involved; or when the College is required to divulge such test results by subpoena.

Administration
Board adopted 5/15/14
Cabinet adopted 4/2/14

Drug-Free Workplace Policy

The College affirms its responsibility and commitment to maintain a drug-free workplace as required by the Drug Free Workplace Act of 1988. The College also prohibits the possession, use, consumption, sale, dispensing, distribution or manufacture of alcohol or controlled substances while ~~unlawful manufacture, distribution, dispensing, possession, or use of controlled substances~~ on College property or while conducting College business off College premises. The College Board of Governors requires strict compliance to the Drug-Free Schools and Communities Act Amendment of 1989, Public Law 101-226, as the same may from time to time be amended.

Drug-Free Workplace Procedure

An employee needing help with drug or substance dependency is encouraged to seek assistance through the College's Employee Assistance Program, health insurance plan, or other substance use recovery programs. ~~(either through their health insurance plan or whatever is appropriate).~~ An employee voluntarily seeking such help shall not receive any type of reprimand and no mention of the issue shall appear in the employee's personnel record.

The College shall notify, as required by law or government regulation, any of its federal contracting or granting agencies of any criminal convictions of employees for illegal drug activity in the workplace within ten (10) working days of learning about the conviction. The term conviction is defined as ~~means~~ a finding of guilt (including a plea of nolo contendere) or imposition of a sentence or both, by any judicial body charged with the responsibility to determine violation of the federal or state criminal drug statutes.

All employees, as a condition of employment, shall report to their immediate supervisor any criminal drug conviction within five (5) working days after the conviction. This requirement is mandated by the Drug Free Workplace Act of 1988.

An employee violating this procedure or convicted of a criminal drug offense in the workplace is subject to appropriate personnel or disciplinary action to include satisfactory participation in a drug rehabilitation program and/or termination.

Fraud Policy

A fraudulent act may be an illegal, unethical, improper, or dishonest act including, but not limited to:

- An intentional or deliberate act
- To deprive the College or a person of something of value or gain an unfair benefit
- Using deception, false suggestions, suppression of truth, or other unfair means which are believed and relied upon
- Identity theft
- Embezzlement
- Misappropriation, misapplication, destruction, removal, or concealment of property
- Alteration or falsification of documents
- False claims by students, employees, vendors, or others associated with the College
- Theft of any asset including, but not limited to money, tangible property, trade secrets, or intellectual property
- Inappropriate use of computer systems, including hacking and software piracy
- Bribery, rebate, or kickback
- Conflict of interest, or
- Misrepresentation of facts

Any member of the campus community who has a reasonable basis for believing a fraudulent act has occurred has a responsibility to promptly notify one of the following:

- His\her supervisor
- The appropriate administrator
- Vice President of Administrative Services
- Office of the President

A. Protection of Involved Parties

The College shall use its best effort to protect employees against retaliation. The employee's identity shall be kept confidential unless:

1. The person agrees to be identified, or
2. Identification is necessary to allow college or law enforcement officials to investigate or respond to the report effectively, or
3. Identification is required by law, or
4. The person accused of fraud violations is entitled to the information as a matter of legal right in disciplinary proceedings.

College employees may not retaliate against another employee with the intent of affecting the terms of employment.

B. Student Handbook

In those cases where disciplinary action is warranted, the Vice President for responsibility for student services, legal counsel, or other appropriate office shall be consulted prior to taking such actions. Additionally, criminal or civil actions against students who participate in unlawful acts shall be forwarded to the appropriate agency.

The relationship of other individuals or entities associated with the College found to have participated in fraudulent acts as defined by this policy shall be subject to review, with possible consequences including termination of the relationship. In those cases where action is warranted, legal counsel or other appropriate office shall be consulted prior to taking such actions. Additionally, criminal or civil actions against individuals or entities associated with the College who participate in unlawful acts shall be forwarded to the appropriate agency.

C. Reporting

According to College policy, the following procedures shall be followed in reporting illegal acts (theft, fraud, etc.) to the office of the Campus President or Vice President of Administrative Services, and/or local law enforcement officials.

1. If an individual is suspicious that an illegal act has been committed, the Vice President of Administrative Services should be contacted immediately.
2. When the Vice President of Administrative Services is reasonably certain that an illegal act has been committed, the President shall be informed ~~before~~ while contacting the College legal counsel and/or appropriate law enforcement officials.

Identify Theft Procedure

Approval and Management; Program Administration; Training; Annual Report
The Vice President of Administrative Services shall be responsible for overall Identify Theft Program management and administration under the Red Flags Rule pursuant to sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act). The Vice President of Administrative Services shall be responsible for the provision of appropriate identity theft training for relevant College employees and for providing reports and periodic updates to the senior administration and to the Board ~~at least on an annual basis.~~as needed.

The ~~annual~~ report shall evaluate issues such as the effectiveness of the policies and procedures for addressing the risk of identity theft with respect to covered accounts, oversight of service providers, significant incidents involving identity theft and the College's response, and any recommendations for material changes to the program. As part of the review, red flags may be revised, replaced, or eliminated. Defining new red flags may also be appropriate.

Definitions
"Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

"Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

A. Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification;
B. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
C. Unique electronic identification number, address, or routing code; and
D. Telecommunication identifying information or access device (as defined in 18 USC 1029(e), as the same may from time to time be amended).

"Account" means a continuing relationship established by a person with the College to obtain a product or service for personal, family, household, or business purposes.
Account includes:

A. An extension of credit, such as the purchase of property or services involving a deferred payment, and
B. A deposit account.

"Covered Account" means:

A. An account that the College offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. Examples could include credit or debit card accounts if the cards are issued by the College, certain student loan accounts, and accounts for the payment of tuition, fees, or other charges over time; and
B. Any other account that the College or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

“Customer” means a person that has a covered account with the College.

“Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

“Service Provider” means a person that provides a service directly to the College.

Transactions at Risk

The College has reviewed its transactions and has determined that the following are "covered accounts" and thus subject to the identity theft prevention policy:

A. Student accounts utilizing the FACTS payment plan.
B. Campus deferment plans.

The College has reviewed the guidelines that contain potential red flags in Appendix A to part 681 of Title 16 in the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, and shall continue to do so as the same may from time to time be amended. The College already has existing policies, procedures, and other arrangements to ameliorate the risk to student and customers, with particular emphasis on those customers who are students or former students, of identity theft. The College intends to utilize those current policies in addition to the new requirements of this identity theft prevention program.

Risk Assessment

A. The College shall consider the following risk factors in identifying red flags for covered accounts, if appropriate:
    1. The types of covered accounts the College offers or maintains;
    2. The methods the College provides to open covered accounts;
    3. The methods the College provides to access covered accounts; and
    4. The College's previous experience with identity theft.
B. The College shall incorporate relevant red flags from sources such as:
    1. Incidents of identity theft that we have experienced or that have been experienced by other colleges and universities;
    2. Methods of identity theft identified by us or other creditors that reflect changes in identity theft risks; and
    3. Applicable supervisory guidance.
C. The College shall include relevant red flags from the following categories, if appropriate:
    1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
    2. The presentation of suspicious documents;
    3. The presentation of suspicious personal identifying information, such as a suspicious address change;
    4. The unusual use of, or other suspicious activity related to, a covered account; and
    5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
D. The College shall attempt to detect relevant red flags in connection with the opening of covered accounts and existing covered accounts, such as by:
    1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account.
    2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.
E. The College shall consider the following instances as red flags:
    1. Notifications or warnings from a consumer reporting agency
        a. A fraud or active duty alert is included with a consumer report;
        b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;
        c. A consumer reporting agency provides a notice of address discrepancy that informs the user of a substantial difference between the address for the

consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

(1) A recent and significant increase in the volume of inquiries;

(2) An unusual number of recently established credit relationships;

(3) A material change in the use of credit, especially with respect to recently established credit relationships; or

(4) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2. Suspicious documents
   a. Documents provided for identification appear to have been altered or forged.
   b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
   c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
   d. Other information on the identification is not consistent with readily accessible information that is on file with us.
   e. An application appears to have been altered or forged, or given the appearance of having been destroyed and reassembled.
3. Suspicious Personal Identifying Information
   a. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
      - The address does not match any address in the consumer report; or
      - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
   b. Personal identifying information is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the Social Security Number range and date of birth.
   c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College, such as;
      - The address on an application is the same as the address provided on a fraudulent application; or
      - The telephone number on an application is the same as the phone number provided on a fraudulent application.
   d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College, such as;
      - The address on an application is fictitious, a mail drop, or a prison; or
      - The telephone number is invalid, or is associated with a pager or answering device.
   e. The Social Security Number provided is the same as that submitted by other persons opening an account or is the same as other customers.
   f. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or is the same or similar to other customers.
   g. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
   h. Personal identifying information provided is not consistent with personal identifying information that is on file at the College.
   i. If the College uses challenge questions, the person opening the covered

account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. Unusual use of, or Suspicious Activity Related to, the Covered Account
   a. Shortly following notice of a change of address for the covered account, the College receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
   b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud, such as:

(1) A majority of available credit is used for emergency loans or merchandise that is easily convertible to cash, such as books; or
(2) The customer fails to make the first payment or makes an initial payment but no subsequent payments.

c. A covered account is used in a manner that is not consistent with established patterns of activity on the account, such as:
(1) Nonpayment when there is no history of late or missed payments;
(2) A material increase in the use of available credit;
(3) A material change in purchasing or spending patterns;
(4) A material change in electronic fund transfer patterns in connection with a cellular telephone account; or
(5) A material change in electronic funds transfers patterns in connection with a deposit account.

d. A covered account that has been inactive for a reasonably lengthy period of time is used. Determining what is reasonably lengthy should take into consideration the type of account, the expected pattern of usage, and other factors which may be relevant.

e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

f. The College is notified that the customer is not receiving paper Account statements.

g. The College is notified of unauthorized charges or transactions in connection with a customer's covered account.

5. Notice from Customers and Others Regarding Possible Identity Theft in Connection with Covered Accounts Held by the College

a. The College is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.

F. Response to Detected Red Flags

The program shall provide for appropriate responses to detected red flags in order to prevent and mitigate identity theft. The response of the College shall be commensurate with the degree of risk posed. Appropriate responses may include, but not be limited to:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the customer;
3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
4. Canceling the transaction;
5. Reopening a covered account with a new account number;
6. Not opening a new covered account;
7. Closing an existing covered account;
8. Notifying and cooperating with appropriate law enforcement; or
9. Determining no response is warranted under the particular circumstances.

G. Updating the Program

1. The program shall be re-evaluated and updated periodically to reflect changes in risks to customers or the safety and soundness of the College based on factors such as:

a. The experiences of the College with identity theft;
b. Changes in methods of identity theft;
c. Changes in methods to detect, prevent, and mitigate identity theft;

d. Changes in the types of accounts that the College offers or maintains; or
e. Changes in the business arrangements of the College, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

The reviews shall include an assessment of which accounts are covered by the program, and the risk of identity theft with respect to each type of covered account.

H. Oversight of Service Providers

It shall be the responsibility of the College to ensure that the activity of a service provider, who is engaged by the College to perform an activity in connection with covered accounts, is conducted with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program that is consistent with the policy of Central Community College and the federal law and regulations may be considered to be meeting these requirements.

Recycling Plan Procedure[AD1]

The College Recycling Plan shall:

A. Develop an educational program to explain why recycling is important to all. We need to change the College culture regarding the use and recycling of materials. Present information to the entire College community; including faculty, staff, and students.

B. Determine what materials (paper, plastic, aluminum, etc.) can be recycled and to where they can be recycled.

C. Determine which materials we can efficiently recycle this year at the College. We can (and will) then add on to the program in future years.

D. Determine what supplies (bins, etc.) are needed to accomplish our recycling goals. Secure funds to purchase supplies.

E. Determine the best locations for placement of recycling bins. Make sure safety is considered in the placement.

F. Inform the College community where the recycling bins are located and whether prepping or sorting is needed.

G. Coordinate facilities and supplies to ensure recycling will work efficiently. Answer the question: how do we get material from campus to a recycling center?

H. Develop an overall action plan based on data gathered from the above items. Present plan to College cabinet endorsement (approval).

I. Further educate the College community relative to the other “R’s” …. Reduce your use of materials; Reuse supplies; and more.

Registered Sex Offender Policy

Any person required by the state of Nebraska to register as a sex offender shall not be permitted to reside in any College residence hall.

Registered sex offenders who plan to attend classes at ~~on~~ any location ~~campus~~ of the College must register with the Associate Dean of Students Office or his/her designee ~~a campus counselor~~ within ten (10) days of enrolling or on the first day of class attendance, whichever is earlier. Failure to register within this time frame constitutes a basis for exclusion from the College. The College reserves the right to deny admission or continued enrollment to any student who may create an unreasonable risk of harm to the health, safety, welfare, or prosperity of CCC, members of its community, or themselves.

~~The College reserves the right to deny or place conditions on admissions of applicants, if the College determines that such person represents a safety risk to persons or property.~~

Anyone who disagrees with a decision made pursuant to this policy may appeal that decision to the Vice President of Student Success and Enrollment Management ~~Campus President~~, by making a request in writing for review within seven (7) calendar days of the date of any decision made pursuant to this policy.

The Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. Section 1232g does not prevent educational institutions from disclosing information concerning registered sex offenders provided under the Wetterling Act, October 25, 2000, including information made available under the Campus Sex Crimes Preventions Act (CSCPA) 42 U.S.C. 14071(j), amendment (October 28, 2002) to that Act, and as any of the foregoing statutes may from time to time be amended.

Social Networking Procedures

The College shall maintain an official presence on Facebook to support the College in accomplishing its mission and achieving it goals and objectives. Other social networking sites also may be used.

In the spirit of maintaining a positive environment to our site visitors, we reserve the right to remove any comments or wall postings from official College-sponsored pages that are inappropriate, inflammatory, or damaging to the College or any individual.

The College, its departments, and individuals in their capacity as College employees are encouraged to use online social networking media including Facebook and ~~MySpace~~ Instagram pages to enhance instruction; inform constituencies about College activities and developments; build online communities of interested constituents; and provide a way for constituents to keep informed about the College and share thoughts, ideas, and experiences through discussions, postings, photos, and videos. Constituencies may include but are not limited to current and prospective students, alumni, employees, potential donors, and members of the community.

The College Communications Office shall maintain a College-level Central Community College Facebook ~~fan~~ page. The senior director of college communications, marketing manager, media producer, and graphic design specialist shall be included as administrators for the page.

~~It is recommended that administrators be assigned and Facebook pages developed for the following: Columbus Campus, Columbus ELS Office, Grand Island Campus, Grand Island ELS Office, Hastings Campus, Hastings ELS Office, Holdrege Center, Kearney Center, Lexington Center, Training Programs, and Central Community College Alumni Office.~~

Other departments and College staff are encouraged to develop Facebook fan pages or other social networking media.

A. Employees must consult and receive approval from their supervisor prior to the use of their College e-mail account on social networking sites or pages on which they are representing the College in an official capacity (non-instructional).

B. Departmental social networking pages shall have a minimum of two administrators assigned. If an administrator leaves the College, he/she shall be removed as a page administrator and another person assigned in his/her place.

~~C. Administrators for College social networking pages agree to check their pages a minimum of twice a day during the normal workweek. It is recommended that pages be checked three times a day, every day.~~

~~D.~~C. The following types of content are prohibited from College social networking sites:

1. Derogatory language
2. Inflammatory language/Photos
3. Inappropriate language/Photos

D. The college communications department must be given the username and password to any of the college social media sites.

E. A college communications member must be given administrator rights to any college social media sites.

Technology Usage Policy

College technology is College property. College technology includes computers, hardware, software, data, e-mail, Internet access, network access, telephone, and voice-mail. College technology shall be used to support the College role, mission, and objectives. The College shall establish employee procedures and student guidelines for acceptable and non-acceptable usage of College technology.

Technology Usage Procedure ~~Guidelines~~ ~~(effective July 1, 2015)~~

Section 1: Purpose

~~The Central Community College Acceptable Use Procedures for Information Technology Resources are intended to serve as an acceptable use guide for users of College information resources.~~ College information resources consist of the computer devices, data, applications, and the supporting networking infrastructure. These technologies are critical to the multifaceted mission of the College, a mission that includes teaching, research, and public service. Information technology offers increased opportunities for communication and collaboration and has changed the way we conduct business as a College:

- All students, faculty, and staff use e-mail services
- All members of the College can obtain wireless connectivity
- Students submit assignments via the Internet

These are but a few of the many examples of how information resources are connected to many activities at the College. While these resources help the College function, they also require responsible use from every user. The actions of users on the Central Community College campus can affect people all around the world. Users must use these technologies responsibly and with respect.

~~This~~ These are the procedure~~s~~ that establish~~es guidelines for~~ acceptable use of information resources. It includes examples of what users may or may not do, and what rights users have. All of these ~~guidelines~~ procedures are based on the following underlying principles:

- Information resources are provided to support the essential mission of Central Community College.
- Central Community College policies, regulations, state and federal law govern users' use of information resources.
- Users are expected to use information resources with courtesy, respect, and integrity.
- The information resources infrastructure is provided for the entire campus. This infrastructure is finite and requires millions of dollars to maintain, and all users are expected to use it responsibly.
- Simply because an action is easy to do technically does not mean it is legal or even appropriate.

All guidelines in this document are based on these important principles. In many cases, they are similar to guidelines governing other forms of communication at the College.

Section 2: Audience

The Central Community College Acceptable Use Policy provides guidance for all individuals that have, or may require, access to the Central Community College information resources, including but not limited to all faculty, staff, students, contractors, visitors, and vendors using College information resources.

Section 3: ~~Authoritative Sources~~Responsible Administrator

~~Section 3.1 Policy~~

~~This policy that is the foundation this procedure is CCC's Equipment and Facilities Use Policy. A copy of this policy may be on WebCentral.~~

~~Section 3.2 Responsible Administrator~~

The authoritative source on this procedure and responsibility for its implementation rests with the Office of the Vice President of Administration.

Section 4: User Responsibilities

Just as everyone in the College community is expected to use physical resources at Central Community College responsibly, we are all expected to help protect information resources at Central Community College. ~~Protecting information resources is not the sole responsibility of IT administrators, any more than taking care of books is singularly the responsibility of librarians.~~

4.1. Protecting IT Resources from Physical Access

Users are responsible for the use of the College information resources they have been provided.

Users must control unauthorized use of their College information resources by preventing others from obtaining access to their computer, or to the network access port assigned for his or her exclusive use.

4.2. Protecting IT Resources from Electronic Access

Likewise, users are responsible for protecting their information resources from unauthorized electronic access by using effective passwords (or other access controls) and by safeguarding those passwords.

Although an individual may believe that the data they store on a Central Community College computer system need no protection from access, remember that an insecure account may provide an access point to other CCC IT services or data. Persons attempting to gain unauthorized access to a system do so through user accounts, and an individual's password may be the only safeguard against such access.

4.3. Using Electronic Communications Responsibly

All members of the College community are encouraged to use electronic communications for College-related activities and to facilitate the efficient exchange of useful information. ~~However, access to the College's electronic communications services is a privilege, and certain responsibilities accompany that privilege.~~ People who use College communication services (such as e-mail) are expected to use them in an ethical and responsible manner, following general guidelines based on common sense, common decency, and civility applied to the networked computing environment.

Electronic communications should meet the same standards for distribution or display as if they were

tangible documents or instruments. Users must identify themselves clearly and accurately in all electronic communications. Concealing or misrepresenting your name or affiliation to dissociate yourself from responsibility for your actions is never excusable.

Electronic communications to the "All CCC" distribution list shall be approved by the College President or a member of Cabinet prior to distribution. Electronic communications to the "All Campus" distribution lists shall be approved by the respective Campus President. Cabinet-level employees are exempt from these approval requirements.

All stored electronic correspondence belongs to somebody. It should be assumed to be private and confidential unless the owner has explicitly made it available to others.

Civil discourse is at the heart of a college community free of intimidation and harassment. It is based upon a respect for individuals as well as a desire to learn from others. While debate on controversial issues is inevitable and essential, bear in mind that it is an individual user's responsibility to do so in a way that advances the cause of learning and mutual understanding.

4.4. Using Limited Resources Responsibly, Efficiently, and Fairly

Users are expected to promote efficient use of network resources, consistent with the instructional, research, public service, and administrative goals of the College. Show consideration for others and refrain from engaging in any use that would interfere with their work or disrupt the intended use of network resources.

It is not responsible to use disproportionate amounts of information resources. Examples of disproportionate uses generally include activities such as the misuse of peer-to-peer (P2P) applications, streaming media at high bit rates, or serving a multi-user game.

4.5. Complying with the Terms of the User Agreement

As a member of the college community, users are expected to read, understand, and comply with the terms of this document. If you have questions, ask for clarification from the Vice President of Student Success and Enrollment Management or the College Information Technology Service Manager.

4.6. Complying with College Rules and Federal Laws

As a member of the college community, users are expected to comply with all applicable College regulations and federal and state laws. Central Community College reserves the right to terminate computing services of users who repeatedly violate College policy/rules or infringe upon the rights of copyright holders. If you have questions about whether you may be infringing on another's copyright, please go to http://www.cccneb.edu/Copyright/ or consult a member of the faculty for rules of use of academic intellectual property.

Section 5: Requirements

The information in this section is intended to assist users in decision making about how to utilize CCC Information Technology Resources.

5.1 Passwords and Access

The user who is granted access from the IT department is the only person who can use an information resource (such as an electronic identifier or an electronic mail account) that the College has provided for their exclusive use. **Never give your password to anyone else**, even people you trust, such as your friends or relatives/parents or someone who has offered to help you fix a problem. If you suspect someone may have discovered or guessed your password, change it immediately.

a. The user whose access is used in an online transaction of any type is responsible for all charges accrued using the computing account or computing resources assigned to them, even if a friend using their account without permission runs up the charges.
b. The user whose access is used will also be held responsible for destructive or illegal activity done by someone to whom they gave access.

Users may not give others access to College information resources unless they are authorized and authenticated to do so. Users may not extend access to College information resources to others without permission (e.g., proxy services, accounts for non-College personnel, etc).

5.2 Use of College IT Resources for Commercial Gain

Users may not be paid, or otherwise profit, from the use of any College-provided information resource or from any output produced using it. Users may not promote any commercial activity (for example promoting a private business) using College information resources. Examples include, attempting to sell football tickets or advertising a "Make Money Fast" scheme via a newsgroup or a distribution list. Such promotions are considered unsolicited commercial spam and may be illegal as well.

5.3 Illegal Activity

College-provided information resources may never be used to do something illegal, threatening, or deliberately destructive—not even as a joke. Campus Security and/or Student Services will investigate all complaints. The Office of the Vice President of Student Success and Enrollment Management and the Campus Associate Deans addresses complaints about students; the Senior Director of Human Resources addresses complaints about Central Community College faculty and staff. Violations can result in disciplinary action, criminal charges, or both. Law enforcement agencies will investigate violations of state or federal law.

a. Ignorance is no excuse. Read the Computer Crimes Law.
b. Never deliberately install any unauthorized or malicious software on any system.
c. Users cannot be exempt from the law because they are "just a student," "they were conducting research," or they were "just playing around."
d. If a user is a student with a part-time job at the College, they may be disciplined both as an employee and as a student, resulting in both professional and educational consequences.

5.4 Civility

Be civil. Do not send rude or harassing correspondence.

a. If someone asks you to stop communicating with him or her, you should. If you fail to do so, the person can file a complaint and you can be disciplined.

b. If you ever feel that you are being harassed, College staff members will assist you in filing a complaint. Please report the problem to the Title IX Coordinator at 308-398-7548 or email at titleixcoordinator@cccneb.edu. If you are concerned for your safety or feel that you are in danger, dial 911.

5.5 Guidelines for Using Limited Resources Responsibly, Efficiently, and Fairly

Use resources appropriately. Do not interfere with the activities of others or use a disproportionate share of information resources. Examples of inappropriate use of resources are shown below. These actions frequently result in complaints and subsequent disciplinary action.

a. Sending an unsolicited message(s) to a large number of recipients (known as "spamming the network").
b. Consuming an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications).
c. Deliberately causing any denial of service, including flooding, ICMP attacks, or the unauthorized automated use of a service intended solely for human interaction.

5.6 User Identity

All electronic correspondence must correctly identify the sender; the only exceptions to this rule are ones approved by College leadership (the Suggestion Box is an example of this). Never falsify your identity or enable others to falsify identity using College information resources. This type of forgery can result in serious criminal penalties and disciplinary action by the Office of the Vice President of Student Success and Enrollment Management or the Office Human Resources.

a. All electronic correspondence belongs to someone and should be treated as private communications unless the author has explicitly made them available to others.

5.7 Respect Copyright

Never infringe upon someone else's copyright. It is a violation of College policy and federal law to participate in copyright infringement. The College complies with all legal requests (e.g., subpoenas) for information and will not hesitate to report a student, faculty, staff or administrators use in response to a lawful request. Copyrighted materials include, but are not limited to, computer software, audio and video recordings, photographs, electronic books, and written material. If you share movies or music that you did not create, you may be infringing on another's copyright. Consequences of copyright infringement can include disciplinary actions by the College. In addition, copyright owners or their representatives may sue persons who infringe on another's copyright in federal courts. Such lawsuits average $750 per allegedly violated song in penalties or fines, for example. See CCC's Copyright Information web page for more information.

5.8 Unauthorized Access

Users may never try to circumvent login procedures on any computer system or otherwise attempt to

gain access other than what has been granted to him or her by IT Services. Users may never deliberately scan or probe any information resource without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences, including disciplinary action by the Office of the Vice President of Student Success and Enrollment Management, the College Information Technology Service Manager, or the Senior Director of Human Resources.

5.9 Information Disclosure

Users may not use or disclose data that is confidential or restricted without appropriate authorization. The Vice President of Administration must be consulted prior to any release of information to a third party without specific written student authorization.

a. Make sure any individual with whom you share confidential data is authorized to receive the information.
b. Do not share confidential data with friends or family members.
c. Do not share College business data that may be classified as confidential, such as the status of negotiation or the terms of contracts.
d. Comply with the College's agreements to protect vendor information such as software code, proprietary methodologies, and contract pricing.
e. If your office routinely receives requests for confidential information, work with the Vice President of Administration to develop formal processes for documenting, reviewing, and responding to these requests.
f. If you receive a non-routine request for confidential information from a third party outside of the College, check with Vice President of Administration to make sure the release of the data is permitted.
g. Report violations of College policies regarding use and/or disclosure of confidential or restricted information to the Senior Director of Human Resources.

Section 6: Privacy Expectations

As a user of information resources at the College, there are certain things you can expect.

6.1. Email Privacy

In general, electronic communications transmitted across a network should never be considered private or confidential. When you are considering the safety and security of a communication, it is best to think of e-mail and instant messages like postcards—viewable by anyone with access.

6.2. File Privacy

The College respects the contents of your files and monitors the College network in accordance with the Central Community College Network Monitoring Standards. Additionally, Information Technology (IT) administrators may become aware of file content while dealing with specific operational problems. Usage logs are frequently kept to diagnose such problems. Furthermore, the College will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance has included providing, when required, copies of system files, e-mail content, or other information ordered by the court.

The College does not monitor personal Web pages for the purpose of determining content. However,

when credible evidence of illegal or otherwise impermissible activity is reported, appropriate action will be taken.

The College does not review electronic communication for the purpose of determining whether impermissible activity is occurring. However, in the course of assuring the viability of the College's network, IT administrators may become aware of activity that poses a risk to the network's proper operation. In such cases, IT administrators may need to disable or block access to the services or systems involved if they are deemed to pose a risk to the network's optimal performance. Also, during the process of diagnosing potential problems involving the proper function of the network, any information obtained that indicates possible unauthorized distribution of copyrighted materials may be referred to College Security or Student Services for further investigation and potential imposition of sanctions.

6.3. First Amendment Rights

As an academic institution, we place great value on freedom of thought and expression. The College community encompasses a wide array of opinions, views, approaches, and temperaments. Ideally, we would like all those associated with the College to exercise their freedoms in a mature, responsible, and respectful manner, and we encourage them to do so. We do not punish or prevent expression that may be offensive but that violates no specific law or College regulation.

Section 7: Disciplinary Actions

7.1. What are the consequences for violating the ~~guidelines~~ procedures listed in this document?

Punishment for infractions includes, but is not limited to:

- Verbal warnings
- Revocation of access privileges
- Disciplinary probation
- Suspension from the College
- Criminal prosecution

If a user's activity breaks the law, he or she can be prosecuted. Even if an individual is charged criminally, he or she can also be placed on probation, suspended or dismissed/terminated from the College.

The College reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

If you are unsure whether an action you are considering is an acceptable use of electronic resources, please contact the Vice President of Student Success and Enrollment Management or the Information Technology Service Manager.

7.2. What is NOT against law or policy?

Some things a user might think violate Central Community College policies may not be violations. Before you report what you believe is an incident of misuse, please read this section carefully. It is written primarily for those planning to report what they believe to be an infraction of law, policy or the rules contained within this document.

7.2.1. First Amendment Rights

In general, expressions of opinion by members of the College community that do not otherwise violate state and federal laws or College rules are protected as "free speech." This is true even though the opinions expressed may be unpopular or offensive to some. The Central Community College community encompasses a wide array of opinions and views. We encourage all those associated with the College to exercise their constitutional rights and freedoms responsibly. We do not, however, punish people who express views that may be unpopular or offensive, but who break no laws or College rules while doing so.

7.2.2. "Spam

“Spam” is unsolicited and unwanted e-mail, and other junk mail from a source outside Central Community College.

Many people are annoyed by junk mail such as "spam" and other kinds of unsolicited or unwanted e-mail. If the offending e-mail is against Central Community College rules, IT staff will investigate. Please send reports of “spam” to IT via the student or employee helpdesk located in WebCentral.

It is not unusual, though, for junk mail to originate from a source outside the College. In most such cases, the College has little control. A user, however, as the recipient has a great deal of control. He or she may ignore or delete the junk mail.

Users may write the administrator of the Internet service provider from which the e-mail was sent, as described later in this section. Responsibly administered mailing lists will remove your name from their subscriber list if you ask them to do so. Not all lists, however, may honor or even acknowledge receipt of your request.

ITS uses robust hardware and software to control spam on all e-mail services provided centrally by ITS. Specific questions about spam can be addressed to the ITS Help Desk.

Repeated incidents involving offensive e-mail may become harassment. If you feel this is occurring, contact the Senior Director of Human Resources. If you feel threatened, contact Campus Security or dial 911.

7.2.3. Breaches of "netiquette"

Disagreements between people, even heated arguments, unless threatening or otherwise unlawful, are not considered violations. Central Community College does, however, strongly encourage all its users to be polite and courteous.

A well-known problem with e-mail, blogs, and social networks is that it's easy to fire off a quick, angry

response that you'll later wish you hadn't sent. In doing so, should you cross the line beyond merely being rude or stating an unpopular, offensive view, you may run the risk of violating criminal laws or inviting an action in civil court. "Counting to ten" before saying something you may later regret applies in cyberspace too.

7.2.4. Off-topic postings

Off-topic postings to blogs, social networks, etc., are breaches of network etiquette, but are not against College rules unless the content of the posting itself is a violation. Find out what is appropriate for each group before you post messages. If someone else posts an off-topic message and you decide to write them about it, be polite. Many such postings are not intentional.

7.3. How do I report an incident?

Note: Before you report an incident involving what you believe to be a misuse of information resources, please reference Section 4: Responsibilities that lists activities that do not violate laws or policies.

How you report an incident involving the misuse of IT resources depends upon the nature of the incident:

- If you believe that your personal safety is threatened, call 911 or contact Campus Security.
- For other incidents, contact the IT helpdesk using either the student or employee links in WebCentral.
- For reporting problems with "spam" or unsolicited mail, you may want to notify the Internet service provider (ISP) from which the mail was sent. Send a simple, polite note to the ISP, including a complete, unaltered copy of the spam (including the e-mail headers) for them to analyze. Don't expect a personal reply, because the ISP will probably be awash in complaints just like yours.

Section 8: Contact information for CCC officials/offices mentioned in this document

- **CCC Security**
  Columbus Security – 402-910-6665
  Grand Island Security – 0 (or 911)
  Hastings Security – 402-469-2421

- Senior Director of Human Resources/Title IX Coordinator
  Pennie Morgan
  (308) 398-7325
  penniemorgan@cccneb.edu

- Title IX Coordinator
  Lauren Slaughter
  (308) 398-7548

laurenslaughter@cccneb.edu

- Information Technology Service Manager
  Mr. Tom Peters
  (308) 398-7365
  tpeters@cccneb.edu

- Vice President of Student Success and Enrollment Management
  Dr. Beth Przymus
  (402) 562-1284
  bprzymus@cccneb.edu

- Vice President of Administration
  Mr. Joel King
  (308) 398-7315
  joelking@cccneb.edu