DAKOTA COLLEGE AT BOTTINEAU

RISK MANAGEMENT HANDBOOK

REVISED: August 2013

Table of Contents

DAKOTA COLLEGE AT BOTTINEAU
Communication With Media And The Public
For Risk Management Events

All communication to external sources will come from the Campus Dean or his/her designee during risk management events. The Dean or designee will work cooperatively with the appropriate officials to release statements about emergency events that occur on campus.

If questioned about an event, an appropriate response would be, "I am not aware of the details. I will ask the Campus Dean to call you as soon as possible." Also, avoid speculation about the following, as it relates to information requests:

- Financial estimate of damage
- Insurance coverage
- Cause of the incident
- Allocation of blame
- Anything "off the record"
- Injuries

DAKOTA COLLEGE AT BOTTINEAU
Referral Numbers

Note: This manual provides a written account of how certain activities are performed and is designed to guide and assist staff in performing their functions. When appropriate, there may be deviations from these written procedures due to changes in personnel, policies, interpretation, law, experimentation with different systems, or simply evolution of the process itself. This manual may be changed at any time. Staff are encouraged to review this manual periodically and suggest changes in the manual to keep it current and to minimize differences between the manual and actual practices.

Referral Numbers

When using the on-campus phone system, any emergency requiring immediate police, ambulance, or fire department service: DIAL 9-911

The campus phone system runs on a T-1 Internet line. If that network line were to go down for some reason, DIAL 8-911 for emergency services.

Associate Dean for Student Affairs	228-5451
Bottineau County Sheriff	228-2740
Campus Health Service	228-5460
Director of Business Affairs	228-5432
Family Crisis Center	228-2028
Housing Director	228-5621
ND Poison Control	1-800-222-1222
ND Helpline for Crisis and Referral	1-800-472-2911 or 211
St. Andrews Health Center (hospital)	228-9300
St. Andrews Clinic	228-9400
Suicide Prevention & Survivors of Suicide	1-800-472-2911 or 211

DAKOTA COLLEGE AT BOTTINEAU
Fire Evacuation Procedures

_____ Remain calm.

_____ Activate the nearest fire alarm station.

_____ If the alarm fails to operate, warn others by knocking on doors and shouting warnings; solicit others to help spread the warning, ***if it can be accomplished without risk to yourself.***

_____ Assist any person in immediate danger to safety, ***if it can be accomplished without risk to yourself.***

_____ Dial 9 for an outside line, (if you are not calling from a residence hall telephone,) then 9-1-1 for emergency services. Identify yourself and describe the nature and location of the fire.

_____ Attempt to extinguish the fire only if it is very minor, you know how to use a fire extinguisher and ***if it can be accomplished without risk to yourself.***

_____ Evacuate the building following the evacuation route nearest your location. Keep to the right and walk, ***DO NOT RUN AND DO NOT USE THE ELEVATOR***. Stay in a single file in stairways so as to provide a lane for fire fighters. If smoke, heat, or fire block your exit, go to an alternate exit.

_____ If smoke is present, keep low to the floor. Take short breaths.

_____ The person in charge of the area being vacated will close all windows and doors, ***if it can be accomplished without risk to yourself.***

_____ The college staff present makes sure all occupants are evacuated.

_____ Those being evacuated will move away from the building so they do not block exits and are not in danger from falling debris or from an explosion. Never re-enter the building without permission from the fire department.

_____ Report the fire to the college administration.

_____ All those affected by the fire will meet in the Thatcher Hall Gymnasium, if it is available. If it is not available, the meeting will be held in NSC 125. A headcount will be taken.

_____ If injuries occur that require the attention of a physician at a clinic or hospital, arrange for a staff member to act as a liaison. However, official injury reports should only be provided by the health care facility.

_____ Provide for the following as required:
- clothing and personal items
- telephones
- counseling services
- emergency housing accommodations
- ease disruption of academic life
- Red Cross assistance

_____ As soon as possible, convene the Dean's Council to review student and staff needs, assess the situation, and provide an official version of events.

If You Cannot Evacuate

_____ Close the doors between you and the fire.

_____ Open the window.

_____ If communication is available, **call 911 (9-911 from a campus extension)** and advise them of your situation

_____ Shout for help.

_____ Hang clothing from a window to alert emergency response personnel to your location.

_____ Seal cracks around the door with towels, tape, bed clothing, or similar items to keep out the smoke.

Training/Inspections

_____ Conduct fire drills annually.

_____ Test fire alarm systems annually.

_____ Inspect fire extinguishers annually.

_____ Post evacuation routes.

_____ Test emergency lighting monthly.

_____ Conduct training on the use of fire extinguishers bi-annually.

_____ Test sprinkler systems annually.

_____ Make sure all exits are free of obstructions.

_____ Make sure all flammable materials are properly stored.

_____ Check all exit lights for burned out bulbs.

_____ Conduct inspections by State Fire Marshall as required by statute.

_____ Faculty and staff should be aware of the location of fire extinguishers in their building.

DAKOTA COLLEGE AT BOTTINEAU
Hazardous Materials Procedures

1. _____ Call 9-911.

2. _____ First responder (sheriff's or fire department) will determine the type of spill and assess the threat to students, faculty and staff.

3. Noxious Fumes:

a. If evacuation is possible, the persons in charge will determine the safest route to evacuate.

b. If evacuation is not possible and
   i. If inside:
      1. _____ Faculty and staff will close all doors and windows and turn off ventilation systems.
      2. _____ Cover mouth and nose with fabric (preferably wet) and take shallow breaths.
      3. _____ Wait until the command to evacuate is given or the all-clear is given.

   ii. If outside:
      1. _____ Faculty and staff will move everyone into a building if possible.
      2. _____ If it is not possible to move into a building, direct everyone to move perpendicular so that the wind is blowing at the side of the body.
      3. _____ Staff, faculty and students will avoid stepping in spilled material.

4. Explosives

a. _____ Evacuate the building using the evacuation route posted in the building.

DAKOTA COLLEGE AT BOTTINEAU
Missing Persons Procedures

Document all steps taken.

_____ (1) Contact the Associate Dean of Student Services at 228-5451 if a student is believed to be missing.

_____ (2) The Associate Dean of Student Services will consult the Director of Housing, roommates, parents, guardians, or spouse, if appropriate, to determine whether or not an investigation should be initiated.

_____ (3) The Associate Dean of Student Services will inform the Campus Dean about the details of the situation; additional support may be necessary in order to coordinate a response to the incident.

_____ (4) If there is substantial reason to believe the student is missing, the Campus Dean will inform the local sheriff's department at 228-2740.

After step 4, the Associate Dean for Student Services will also contact the following:

_____(5) The parents, spouse, or guardian; this office will serve as the official liaison with the family in this matter.

_____(6) The Associate Dean of Academic Affairs, who will inform the student's instructors of the situation.

_____(7) The Campus Dean, who will coordinate public information for the media.

_____(8) The Business Office who will in turn notify the campus employer, if the student is employed on campus.

_____(9) The Campus counselor, Housing Director, and any other offices that are deemed appropriate so that they can provide support to roommates, friends, and anyone else affected by the disappearance.

When the student is located:

_____(10) Notify the Associate Dean of Student Services so that office, in turn, notify all others who had been informed initially.

_____(11) The Associate Dean of Student Services will coordinate a follow-up meeting to assess the handling of the particular incident.

DAKOTA COLLEGE AT BOTTINEAU
Severe Weather Procedures

Tornadoes

_____ Remain calm.

Tornado Watch

_____ The Business Office will monitor local radio for updates in the weather conditions and will attempt to notify someone in each building.

_____ Know where areas of safety are located and be prepared to move to them, e.g., the lowest level of the innermost part of the building, the utility tunnel under Thatcher Hall and the New Addition (the Business Office has the key to gain access to the area).

Tornado Warning (City siren will be activated by the Sheriff's Department.)

_____ Seek shelter immediately.
Indoors:
- _____ Go to the **lowest level** of the **innermost part** of the building.
- _____ Stay away from windows and areas with a large expanse of glass.
- _____ Stay away from load-bearing walls on the south and west sides.
- _____ Avoid the gymnasium and other large rooms with free-span roofs.
- _____ Assist personnel who are physically unable to move to a safe area.
- _____ Close all doors, including main corridors, making sure they latch.
- _____ Crouch near the floor or under heavy, strong support objects, and cover your head.
- _____ Do not leave the shelter until a verbal "all clear" announcement is made by supervisors.

Outdoors:
- _____ Move to the nearest building and area of safety.
- _____ If insufficient time to reach a safe area, sit down with your hands over the back of your head with your head facing down.

_____ The Campus Dean or Dean's Council member will stay abreast of official weather reports and notify supervisors when the severe weather has passed or been down-graded.

_____ Once an "all clear" announcement is made, Supervisors/Faculty account for employees/students.

_____ Use caution in entering or working in buildings that may have been damaged or weakened. Be aware of the possibility of gas leaks or electrical short circuits.

_____ The Director of Physical Plant will call safety officials (gas company, electric company, police, fire department) fro inspection if damage seems to have occurred.

Electrical Storms

_____ Continue indoor classes.

_____ Move outdoor classes/activities indoors or cancel the activities.

_____ Unplug or turn off all electrical equipment.

Snowstorms

_____ The Campus Dean (or designee) monitors the local weather and road conditions and determines if the campus will be closed and classes/activities cancelled. The Campus Dean or designee will notify the media of closure.

_____ Students and employees should listen to SUNY 101.9/KBTO radio or KXMC-TV and/or KMOT for storm-related information. (Decisions generally will be made by 7:00 AM.)

_____ If campus is closed; only "key personnel" will be required to report. The Campus Dean and Associate Dean of Business Affairs will designate key personnel.

_____ If a decision to close the campus occurs on the day, previous to the actual closure event, the Campus Dean will notify the Dean's Council who will in turn notify supervisors. Supervisors will let employees know of the closure. Faculty signatories will be called by the Associate Dean of Academic Affairs; the signatories will in turn call the faculty in the department.

_____ The use of the term "Campus Closure" means that classes and activities are cancelled and that faculty and staff with the exception of "key personnel" are not to report for work. If circumstances require that we vary from this procedure, that change will be made clear in the media announcement.

Because of the variety of methods, locations, and times the college utilizes to deliver instruction, it is not possible to prescribe a storm closure policy for all of them. However, the following guidelines will be used:

If classes are cancelled on the Bottineau Campus

Dakota College at Bottineau classes delivered via the interactive video network (IVN) will be cancelled at all distance sites whether the instructor intended to teach from the Bottineau or Minot studio (see Nursing exception below). Face-to-face classes scheduled at off-campus sites will be considered on an individual basis.

If classes are cancelled on the Minot Campus but not the Bottineau Campus

Dakota College at Bottineau classes delivered via interactive video network (IVN) or taught face-to-face on the Minot Campus will be cancelled. In addition, IVN classes cancelled at the Minot Campus will be cancelled at the Bottineau Campus and other distance sites.

Classes cancelled at MAFB by Minot State University

Dakota College at Bottineau classes at MAFB will not be held.

Dual Credit classes

If area high schools have cancelled classes, but Dakota College at Bottineau has not, classes delivered via interactive video will be held at high schools that are not closed.

Classes cancelled at Bismarck State College

Any interactive video classes that are delivered by Dakota College at Bottineau to Bismarck State will be cancelled, but these classes will not be cancelled at other sites receiving Dakota College at Bottineau interactive video classes.

Nursing IVN classes

These classes will always be held when at all possible because of the number and location of receiving and sending sites.

SEVERE WEATHER
Key Personnel

Snowstorms

The following staff needs to report to work when we have made an announcement regarding campus closure due to severe weather conditions. These individuals are not expected to report to work if doing so risks their health and safety. They are responsible for judging health and safety risk.

- Stuart Oien -- Snow Removal

- 1. Howard Prouty – Plumbing, heating, snow removal
  Or
  2. Blayne Graber – Plumbing, heating, snow removal

- 1. – Custodial services
  Or
  2. – Custodial services

- 1. – Telephone/Information services
  Or
  2. – Telephone/Information services

- Zelda Buelow – Food Services (*Zelda will work with her staff regarding staffing requirements during snowstorm closures.)*

If the first person on these listings is unable to report to work, he or she is responsible for contacting the second person on the respective listing. The Campus Dean or the Director of Financial Affairs will decide if conditions require additional staff to report to work. This information will be provided as soon as possible to those affected.

Tornadoes/Electrical Storms

Conditions will dictate the need for key personnel to report to work should these severe weather events cause campus closure. The Campus Dean and the Director of Financial Affairs will decide which staff needs to report. This information will be provided as soon as possible to those affected.

DAKOTA COLLEGE AT BOTTINEAU
Harassment Policy

Policy and Definition:

It is the policy of Dakota College at Bottineau (DCB) that there shall be no discrimination against persons because of sex, gender, sexual orientation, race, ethnicity, color, religion, national origin, pregnancy, age, marital status, veteran's status, political beliefs or affiliation, or physical or mental disability. Harassment is a form of discrimination that creates a hostile environment in the workplace and the classroom and, therefore, DCB will not tolerate harassment in any form. The behavioral standard of this policy applies to faculty, staff, and students, as well as persons conducting business with or visiting the Campus. This policy contains a definition of harassment, procedures for reporting allegations of harassment, procedures for investigations and resulting disciplinary matters, and discussions concerning consensual relationships and retaliation. Appendices A and B contain further discussion for understanding the practical definition of harassment. This policy implements the State Board of Higher Education Policy 603.1, Harassment.

Definition:

Harassment is defined as verbal, nonverbal, or physical conduct towards another person or identifiable group of persons that is severe, persistent, or pervasive and has the purpose or effect of:

a. Creating an intimidating or hostile education environment, work environment, or environment of participation in a Campus activity;
b. Unreasonably interfering with a person's educational environment, work environment, or environment of participation in a Campus activity; or
c. Unreasonably affecting a person's educational or work opportunities or participation in a Campus activity.

Sexual harassment is defined by unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature that constitute sexual harassment when:

a. submission to such conduct is made either explicitly or implicitly as a term or condition of an individual's employment or education requirement;
b. submission to, or rejection of such conduct by an individual is used as the basis for employment decision, educational decision (grades, etc.) affecting such individual;
c. such conduct has the purpose or effect of substantially interfering with an individual's work or learning performance or creating an intimidating, demeaning, or hostile offensive working/classroom environment.

Reporting Procedures (Students):

Any and all complaints alleging any form of harassment may be reported to the Associate Dean for Student Affairs or the Director of Financial Affairs; however, in an effort to satisfy a complaint and solve problems at the lowest level possible, students should also consider the following report methods:

a. Complaints alleging any form of harassment related to **employment** should be reported to the student's supervisor or to someone in the supervisory line.
b. Complaints alleging any form of harassment related to the **classroom environment** should be reported to the classroom instructor or Associate Dean for Academic Affairs.
c. Complaints alleging any form of harassment related to **non-classroom environments** should be reported to the Associate Dean for Student Affairs or the Director of Student Life.

Reporting Procedures (Faculty and Staff):

Any and all complaints alleging any form of harassment may be reported to the Campus Dean or Director of Financial Affairs, however, in an effort to satisfy a complaint and solve problems at the lowest level possible, faculty and staff should also consider the following report methods:

a. Complaints alleging any form of harassment from **employees** should be reported to the employee's supervisor or to someone in the supervisory line.
b. Complaints alleging any form of harassment from **students** should be reported to the Associate Dean for Student Affairs or Associate Dean for Academic Affairs.
c. Complaints alleging any form of harassment from other campus **visitors** should be reported to your supervisor or to someone in the supervisory line.

Formal and Informal Reporting of Complaints:

Anyone with knowledge concerning allegations of harassment should report such behavior or incidents. Timely reporting of harassing behavior is essential to the investigation that will follow, though there is no deadline for reporting such behavior.

All reports will be referred to as "formal" or "informal." A formal complaint refers to complaints made in writing. Formal complaints must include a description of the allegation, the name of the alleged offender, and the name and signature of the complainant. An informal complaint refers to complaints made orally.
All complaints, formal or informal, will be acted upon; however, an informal complaint may limit DCB's ability to effectively resolve the complaint.

While DCB respects the complainant's potential need for confidentiality, anonymity or confidentiality cannot be guaranteed. In the case of informal reports the complainant's name will not be used during investigations at any level; however, the nature of the specific issue may reveal the person's identity.

(See Appendix A)

Investigations:

Anyone receiving a complaint should contact the Director of Financial Affairs to coordinate a plan for investigating the complaint. The Director of Financial Affairs will either assign the complaint to an investigator or perform the investigation him/herself.

While an investigation should happen as expeditiously as time permits, it is expected that an investigation will be completed within 30 calendar days. This time line may be extended to a maximum of 120 days due to particular difficulties or unforeseen circumstances.

Each investigation will conclude with a "Report of Investigation" and will include at a minimum the background of the allegation, finding from the investigation, and a recommendation based on the finding. The finding will be a determination by the investigator whether DCB's policy on harassment was violated. Copies of the report will be provided to the complainant, the accused party, and other parties who will need to act upon the recommendation. The Business Office will serve as the office of record for the original report of investigation.

In the event the report of investigation finds that DCB's policy on harassment was not violated, the complainant may appeal the finding. The appeal must be filed in writing and delivered to the Campus Dean within thirty days of the date of the report. The appeal may be filed on any basis, though bringing to light new or missed information or mischaracterizations in the reports will probably be more effective. The Campus Dean has 30 days to review the Report of Investigation and to render a judgment.

Disciplinary Matters:

If a recommendation from the report of investigation calls for disciplinary action, the appropriate administrator is not bound by the recommendation. The administrator may discuss the report with the investigator and others in the supervisory chain to make a determination concerning the recommendation. Disciplinary action need not be progressive. Actions will be determined on the basis of the severity of the harassment and may include anything from a verbal warning to a dismissal, inclusively.

If the administrator takes disciplinary action against a member of the faculty or staff, the action will follow North Dakota Century Code, State Board of Higher Education Policies, NDUS Human Resource Policies and local policies including those contained in the Faculty Handbook as appropriate.

a. Any documented disciplinary action will include an opportunity for the recipient to acknowledge receipt of the document without discussion of agreement and to attach any comments to the document that will become a permanent part of that document. The right of the recipient to attach comment is without deadline, though three to five days should be provided the recipient prior to filing. (NDCC 54-06-21, State Government – General Provisions).

b. The recipient of disciplinary action may appeal the action or grieve the policy, practice, or procedure through the Faculty Rights Committee or Staff Personnel Board as appropriate. (SBHE 605.4, Hearings and Appeals; NDUS HR Policy 27, Appeal Procedures).

The Associate Dean for Student Affairs oversees disciplinary action against a student and ensures the action conforms with North Dakota Century Code, State Board of Higher Education Policies, and local policies contained in the Student Handbook, specifically, the Student Conduct Policy.

Non-Retaliation:

This policy seeks to encourage the timely reporting of allegations of harassment to subsequently provide for the timely resolution of the allegations. Retaliation against faculty, staff, or students for reporting complaints of harassment or enforcing this policy is strictly prohibited. Anyone involved in overt or covert acts of reprisal, interference, restraint, penalty, discrimination, or harassment against an individual or group for reporting an allegation of harassment or participating in an investigation under this policy will be subject to prompt disciplinary or remedial action.

Student-Faculty Relationships:

Any intimate, dating, or sexual relationship between faculty and students is explicitly prohibited. Any form of sexual harassment toward students is explicitly prohibited. Relationships between faculty members and students beyond the academic scope create a potentially threatening situation within the context of harassment and may create conflicts of interest in other areas as well.

Appendix A

Dealing with Harassment

People who harass will have no reason to stop unless they are challenged. Therefore, it is imperative to support and encourage people who are targets of harassment to come forward. Indeed, supervisors have an institutional and legal responsibility to respond to these concerns appropriately. However, many people do not report their experiences.
They are afraid they will not be believed or that others will say, "They asked for it." It's natural in such circumstances to feel uncomfortable and worried. Yet, ignoring or minimizing the problem will not make it go away. Remember, too, that oftentimes harassment is not blatant or obvious; it can be subtle. In fact, sometimes it is so subtle that it may be only after a series of incidents that a person may begin to feel that harassment is occurring. Individual incidents, taken in isolation, may not constitute harassment. However, when these incidents constitute a series of ongoing offenses, he or she may well conclude that a pattern of harassment exists.

Sometimes harassment can be stopped by taking direct action. Anyone who believes they are being, or have been, harassed should first point out the harassing behavior to the other individual. Be direct and clearly communicate your disapproval of the behavior that makes you uncomfortable and that you consider harassing. Sometimes the other individual simply needs to be made aware of their behavior and that it has crossed the line into harassment. If the behavior persists, then the matter should be reported formally or informally as discussed in the policy section on "Reporting Procedures."

Appendix B

Types of Harassment

Racial/Ethnic Harassment: In addition to being a violation of DCB policy, racial and/or ethnic harassment is a form of discrimination and is a violation of Federal, State, and local law. The U.S. Department of Education, Office of Civil Rights, has interpreted Title VII of the Civil Rights Act of 1964 as prohibiting racial and ethnic harassment. Similarly, the Equal Employment Opportunity Commission interprets Title VII as prohibiting racial and ethnic harassment.

Recognizing Incidents of Racial or Ethnic Harassment: The following are some incidents that may constitute racial or ethnic harassment and may result in disciplinary sanctions under DCB policy. (To make an accurate judgment as to whether these incidents constitute racial or ethnic harassment, the full context in which these actions were taken or statements made must be considered.)

- Several Asian-American students are called names that are racially and ethnically vilifying as they cross the campus.
- An advisor tells an African-American student not to take a certain course because the advisor says that other African-American students have had difficulty in the course and so African-Americans are, therefore, not suited for this particular course.
- A DCB official requests that a group of Latino students display their student IDs as they enter their residence hall while white students are not required to display their IDs. The official cannot explain why the Latino students were stopped and asked to display IDs.
- A student group discovers that swastikas have been painted on the door of a room often used to prepare for the observance of the Jewish Sabbath.
- A male student approaches an Asian Pacific-American female student on several occasions and makes statements implying that certain sexual practices are common within her ethnic group.
- A supervisor assigns only menial tasks to a Hispanic staff member and writes on an evaluation that the staff member could not expect to be promoted because he is an "affirmative action" appointment.
- Several female students of color receive anonymous phone calls in which the caller uses language that is both obscene and racist.

Disability Harassment: In addition to being a violation of DCB policy, harassment based on physical ability is a form of discrimination and is a violation of Federal, State, and local laws. Section 504 of the Rehabilitation Act of 1973, as amended, prohibits job discrimination because of disability and requires affirmative action to employ and advance in employment qualified individuals with disabilities who, with reasonable accommodation, can perform the essential functions of a job. The Americans with Disabilities Act of 1990, as amended, protects qualified applicants and employees with disabilities from discrimination in hiring, promotion, discharge, pay, job training, fringe benefits, classification, referral, and other aspects of employment on the basis of disability. The law also requires that covered entities provide qualified applicants and employees with disabilities with reasonable accommodations that do not impose undue hardship.

Recognizing Incidents of Disability Harassment: The following are some incidents that may constitute disability harassment and may result in disciplinary sanctions under DCB policy: (To make an accurate judgment as to whether these incidents constitute racial or ethnic harassment, the full context in which these actions were taken or statements made must be considered.)

- A visually-impaired student is told to "get new glasses" when the student requests a seat closer to the board.
- A student with a physical disability requests a classroom change to an area with fewer stairs and is denied outright.

Sexual Harassment: In addition to being a violation of DCB policy, harassment based on physical ability is a form of discrimination and is a violation of Federal, State, and local laws. EEOC Guidelines on sexual harassment (as an amendment to the Guidelines on Discrimination Because of Sex, 29 CFR part 1604.11, 45 FR 25024), Title VII and Title IX provide the basis for the DCB's policy. In brief, unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment. Incidents may be defined as sexual harassment as follows:

a. Submission to or rejection of such conduct is made either explicitly or implicitly a term or condition of an individual's employment, advancement, evaluation, or participation in a DCB program or activity. This is referred to as *quid pro quo*, and one such incident is unlawful.
b. Unwelcome conduct that is severe, persistent, and pervasive with the purpose or effect of unreasonably interfering with an individual's work performance, or creating an intimidating, hostile, abusive, or offensive working or educational environment, or hindering participation in or benefits from a DCB program or activity. This known as a *hostile environment*. A hostile environment is generally created by a series of incidents; however, a single incident may be so egregious as to also create a hostile environment.

It is important to remember that both men and women can be targets of sexual harassment, and that sexual harassment can occur between individuals of the same sex.

Recognizing Incidents of Sexual Harassment: The following are some incidents that may constitute sexual harassment and may result in disciplinary sanctions under DCB policy: (To make an accurate judgment as to whether these incidents constitute racial or ethnic harassment, the full context in which these actions were taken or statements made must be considered.)

- A student phones and sends email messages to someone s/he has a crush on, even though this person has clearly indicated no interest in him/her.
- A supervisor regularly makes sexually suggestive remarks in front of his/her staff. Several staff members have asked the supervisor to stop, but the behavior continues.
- A student dated his/her instructor at the beginning of the semester. S/he now believes the final grade for this course is not an accurate reflection of the work, but is an act of retaliation for ending the relationship.

- From time to time, a group of students hang out in front of the dining hall and rate other students from 1 to 10 as they leave the building. Some students avoid that dining hall because of this behavior.
- Two members of a student association or club persistently ask a prospective member to talk about favorite sexual fantasies. When the prospective member refuses and walks away, one member yells, "You won't get in this club if you don't know how to take a joke!"
- An employee sends unsolicited pornographic material and obscene messages to another employee via e-mail.
- An individual refuses to participate in sexually explicit conversations, and is called "gay" or "lesbian" for his/her refusal.

Distinguishing Between Sexual and Gender-Bias Harassment: Title VII of the Civil Rights Act of 1964 and the Civil Rights Act of 1991 provide protection against gender as well as sexual harassment. Gender harassment is a form of sexual harassment that consists primarily of repeated comments, jokes, and innuendoes directed at persons because of their gender or sexual orientation. It also occurs when attitudinal or organizational workplace barriers are maintained to deprive people of singled-out genders from competing and achieving at their highest potential. This behavior may or may not be aimed at eliciting sexual cooperation from those addressed, but it contaminates learning and work environments. Gender harassment closely resembles racial and ethnic slurs.
Gender harassment may include:

- Disparaging women's seriousness about academics
- Using sexist humor as a classroom teaching technique
- Turning a discussion of a woman's work into a discussion of her physical attributes or appearance
- Opening a meeting with remarks about a colleague's appearance, and continuing to make references to it throughout the discussions
- Disparaging scholarly works by or about women
- Ridiculing specific works because they deal with women's perception or feelings
- "Bashing" male students for being "pigs" or "chauvinists" in a Women's Studies class
- Holding allegedly social events at which workplace issues are discussed or decided at venues or locations where women are excluded by either policy or habit
- Referring to women as "girls," "princess," "chicks," or other diminutive terms.
- Any of the above actions directed toward lesbians or gays

DAKOTA COLLEGE AT BOTTINEAU
Student Death Procedures

Notify the Associate Dean of Student Affairs if you become aware of a student death. He or she will be responsible for confirming the death.

Direct all questions to the Associate Dean for Student Affairs.

The Associate Dean for Student Affairs or his/her designee will be responsible for the following:

_____ Confirm the death. Be very careful about providing information about the cause, especially labeling any death a suicide.

_____ Have medical personnel or law enforcement make the first contact with parents in regard to the death.

_____ If the student is from out-of-state, assist with any arrangements that might need to be made to return the body home.

_____ Inform faculty and staff of the death via campus mailboxes, and also inform them of the availability of counselors.

_____ Have the Associate Dean of Student Affairs contact the family to offer assistance and inform them of how the college intends to respond.

_____ Contact the Ministerial Association to provide grief counseling. Provide them a space where students may voluntarily stop by to visit. Also contact our campus counselor to set up a situation where students can drop by her office to visit.

_____ Identify those on campus who are most effected by the death and provide support for them if needed or requested. Follow up after a couple of days, with people on campus who seem to be having exceptional difficulty with the death – especially roommates – to see how they are doing.

_____ Direct all questions to one individual – the Associate Dean of Student Services or his designee.

_____ Ask instructors to provide for a campus-wide moment of silence (30 seconds) in their classes at a specified time, on a specified day (perhaps the day of the funeral), in remembrance of the deceased student.

_____ Provide details of the funeral to each room, also post the details at the Student Services Office and Business Office. Also, give details to the Director of Housing so he/she can verbally disseminate information.

_____ With permission and/or the request of family, set up a time for the college community to come together to "mark" or "signify" the student's death. Ask parents if they would like to come. Begin the event with help from clergy or counselors, have a college representative say a few words, then open it up. Keep it as informal as possible. Serve refreshments. Respect family's wishes in regard to this type of gathering.

_____ Contact family to ask if they would like to have roommates/friends or housing staff pack the deceased student's belongings so it is ready for the family to pick up.

_____ Ask parents if they would like privacy when they pick up the deceased student's gear – or if they mind if roommates/friends are in the vicinity at that time. Do what the parents prefer. Set up a time and date for the parents and have a counselor or minister there. Also ask several RA's to be there to help carry materials.

_____ Send a sympathy card from each residence hall, signed by students.

_____ Ask the Dean of the College to send a letter of condolence to the family on behalf of the college.

_____ Have the Foundation send flowers.

_____ If at all possible, have representation at the funeral from faculty and staff.

_____ Fly the flag at half-mast on the day of the funeral.

_____ Process any applicable refunds.

_____ Amend the student's records (registrar, business office, library, housing) appropriately.

_____ Several weeks after any student death, the Associate Dean of Student Services will convene a meeting to review Dakota College at Bottineau's response to the death.

DAKOTA COLLEGE AT BOTTINEAU
Threatening Call Procedures

A. **IF YOU RECEIVE A THREATENING CALL** (bomb, other physical harm, etc.):

1. **Do not hang up**. Have someone else call the Police at (9) 911 from another extension if possible. The caller should give the police their name, location and nature of the threat
2. Try to engage the caller in a conversation and obtain as much information as possible -- use **Threatening Call Report** form to record information and observations.
3. Notify the Campus Dean for a decision to evacuate. If he is not available, the net contact person is the Director of Financial Affairs, followed by the Associate Dean for Student Affairs, and Associate Dean for Academic Affairs.

B. **EVACUATION**: The decision will include the best method of notification (e.g. activating the fire alarm or messenger). Personnel will also be assigned to check restrooms, storage rooms and other areas where the evacuation order may not have been heard.

C. **EVACATION PROCEDURE:**

1. Follow the emergency evacuation (fire) routes.
2. Try to remain calm and walk (don't run).
3. All personnel should proceed to their assigned area. You should be at least 300 feet away from the threatened building. A headcount should be made and any missing personnel should be reported to the police.
4. All personnel should take their personal belongings with them.
5. Employees with knowledge of the contents and layout of the building may be asked by the authorities to assist in identifying any unusual items.
6. Assist students, visitors and persons with mobility difficulties to safety.
7. No one will re-enter the area until emergency personnel give permission.

D. **IF A BOMB IS FOUND**: Do not move, jar or touch the object or anything attached to it. Leave this to the professionals.

E. **IF A SUSPICIOUS LETTER OR PACKAGE IS RECEIVED**:

1. Inform you supervisor immediately.
2. Do no open it.
3. As co-workers if anyone can identify the package.
4. Contact the police by calling 9-911
5. Give the dispatcher a description and location of the package.

6. Follow the instructions given by police.
7. Instruct staff to evacuate if told to do so by the Campus Dean or designee.

THREATENING CALL REPORT

Time call received:	**Time cal terminated:**

Exact Words of the Caller:

Nature of Threat:

Person receiving call:	**Call received at extension:**
Date received:	

QUESTIONS TO ASK FOR BOMB THREAT

1. **When is the bomb going to explode?**
2. **Where is the bomb located? Building_____ Floor_____ Area _____**
3. **What does it look like?**
4. **What kind of bomb is it?**
5. **What will cause it to explode?**
6. **Did you place the bomb?**
7. **Why kill or injure innocent people?**
8. **What is your address?**
9. **What is your name?**

QUESTIONS FOR OTHER THAN BOMB THREAT

1. **Why?**
2. **From where are you calling?**
3. **What is your address?**
4. **What is your name?**

DESCRIBE THE CALLER'S VOICE (Circle)

FEMALE /MALE	**CALM**	**DISQUISED**	**NASAL**	**ANGRY**	**BROKEN**	**STUTTER**
SLOW	**SINCERE**	**LISP**	**GIGGLING**	**RAPID**	**DEEP**	**CRYING**
SQUEAKY	**EXCITED**	**STRESSED**	**ACCENT**	**LOUD**	**SLURRED**	**NORMAL**

BACKGROUND SOUNDS (Circle)

STREET	**FACTORY**	**VOICES**	**CLEAR**	**MOTOR**
OFFICE MACHINES	**HOUSE NOICES**	**LONG DISTANCE**	**PA SYSTEM**	**MUSIC**
ANIMAL NOICES	**STATIC**			

OTHER INFORMATION:

DAKOTA COLLEGE AT BOTTINEAU
Workplace Violence Policy and Procedures

Policy:
Dakota College at Bottineau is committed to providing a work environment that is free and/or protected from violent and aggressive behavior. Behavior that threatens the safety of its employees, students and/or visitors will not be tolerated.

Purpose:
The purpose of this policy is to recognize that workplace violence and abusive/threatening behavior is an occupational safety hazard. This policy and corresponding procedures have been developed as a guide for prevention.

Implementation:
Dakota College at Bottineau recognizes that creating a violence-free work environment requires a multi-faceted approach. To this end the College will:

a. Maintain a relevant policy - the Dean's Council in cooperation with the Administrative Council will develop, modify and amend current policies and procedures as needed on an annual basis.
b. Modify workplaces as required to make them safer – Administrative Council will develop site-specific action plans to eliminate, or at least minimize, threats of workplace related violence. These action plans may include, but are not limited to, modification of the work-site, change in environmental conditions such as lighting, means of egress, etc.
c. Ensure that follow-up procedures are adhered to – the Dean's Council is responsible for taking immediate and appropriate action upon learning of a workplace related threat to their employees. This also may include, but is not limited to, violence prevention education and/or work site modification.

Definitions:
Violence in the workplace is defined as the attempted or actual exercise by a person of any physical force to cause injury to a worker. This includes any threatening statement or behavior which give a worker reasonable cause to believe that the worker is at risk of injury.

Procedures:

A. Acts of Violence:

When an employee observes an act or behavior that may be violent or threatening in nature, and they believe there is a threat to their personal safety or the safety of others, the following procedures will apply:

1) Move to a safe location and alert those around you.

2) Call 9-911
   a) State clearly that immediate assistance is needed
   b) Provide your location and complete details of the situation.

3) If the individual attempts to leave, do not block their way. Be prepared to give the Sheriff a description of the subject and all available information.

4) As soon as you are able, report the incident to your supervisor. The supervisor will notify the Campus Dean as soon as practicable.

5) Employees involved in the incident will complete a Workplace Violence Incident Report within 24 hours

6) Support services will be offered to the affected employee(s) immediately.

7) The Campus Dean will conduct a follow-up assessment of the situation and make required changes to the environment or to the procedures as soon as practicable.

Abusive Language or Threatening Manner:

1) In a polite but firm service manner inform the person that if they wish to continue the interaction their behavior will need to change.

2) If the person persists, advise the subject you will have to terminate the interaction.

3) Inform the person that they may reschedule the interaction for another time.

4) Maintaining a firm, courteous service manner, ask the person to leave the area immediately.

5) If the person refuses to leave, notify your supervisor and monitor the situation if your safety is not in jeopardy.

6) If at any time you feel the situation has escalated to the point that you sense you, or anyone else, is in danger call the Sheriff (9-911) and request assistance. Notify your supervisor if the supervisor is not already involved. The supervisor will notify the Campus Dean as soon as possible.

7) Do not block the individual if they decide to leave. Be prepared to give the Sheriff a description of the subject and all available information.

8) If the abuse is over the telephone, the conversation is to be terminated in the same manner, giving the person your supervisor's telephone number. Advise your supervisor of all of the details.

9) If you feel that a person who has been abusive or threatening might go directly to another office on Campus, notify that office and advise your supervisor.

10) Employees involved in the incident will complete a Workplace Violence Incident Report with 24 hours.

11) Support services will be offered to the affected employee(s) immediately.

12) The Campus Dean will conduct a follow-up assessment of the situation and make required changes to the environment or to the procedures as soon as practicable.

DAKOTA COLLEGE AT BOTTINEAU
Anthrax and Suspicious Mail

WHAT TO DO IF A POSSIBLE ANTHRAX EXPOSURE OCCURS

1. Do not shake or empty the contents of any suspicious envelope or package; DO NOT try to clean up powders or fluids.

2. Set down the envelope or package, LEAVE the room and CLOSE the door, or section off the area to prevent others from entering.

3. WASH your hands with **soap and water** to prevent spreading any powder to your face or skin.

4. Report the incident to local police; notify your building security official or an available supervisor to shut down the ventilation system.

5. Remove clothing and place in a plastic bag to store until you receive further guidance.

6. As soon as possible, shower with soap and water. Do not use bleach or disinfectant on your skin.

7. If possible, LIST all people who were in the room or area when the suspicious letter or package was recognized. Give this list to both the local public health authorities and law enforcement officials for follow-up investigations and advice.

ANTHRAX FACT SHEET

Description: Anthrax is an acute infectious disease caused by the spore-forming bacterium *Bacillus anthracis*. Anthrax most commonly occurs in hoofed mammals and can also infect humans.

Symptoms: Symptoms of disease vary depending on how the disease was contracted, but usually occur within 7 days after exposure. The serious forms of human anthrax are inhalation anthrax, cutaneous anthrax, and intestinal anthrax.

Initial symptoms of inhalation anthrax infection may resemble a common cold. After several days, the symptoms may progress to severe breathing problems and shock. Inhalation anthrax is often fatal.

Infection: The intestinal disease form of anthrax may follow the consumption of contaminated food and is characterized by an acute inflammation of the intestinal tract. Initial signs of nausea, loss of appetite, vomiting, and fever are followed by abdominal pain, vomiting of blood, and severe diarrhea.

Direct person-to-person spread of anthrax is extremely unlikely, if it occurs at all. Therefore, there is no need to immunize or treat contacts of persons ill with anthrax, such as household contacts, friends, or coworkers, unless they also were also exposed to the same source of infection.

Treatment: In persons exposed to anthrax, infection can be prevented with antibiotic treatment. Early antibiotic treatment of anthrax is essential–delay lessens chances for survival. Anthrax usually is susceptible to penicillin, doxycycline, and fluoroquinolones.

Vaccination/Prophylaxis: An anthrax vaccine also can prevent infection. Vaccination against anthrax is not recommended for the general public to prevent disease and is not available.

This material has been developed by the Centers for Disease Control and Prevention. Reuse or reproduction of this material is authorized. Information updated September 2001. More information can be found on the CDC website at www.bt.cdc.gov.

GUIDELINES FOR ASSESSING SUSPICIOUS MAIL PARCELS OR OTHER SUBSTANCES

The following guidelines for assessing suspicious mail, parcels or other substances have been prepared by the N.D. Department of Health (NDDoH) and the Federal Bureau of Investigation (FBI)/Fargo Resident Agent in consultation with the N.D. Bureau of Criminal Investigation (BCI), the N.D. Highway Patrol (NDHP), and the N.D. Division of Emergency Management (DEM). These guidelines refer only to those threats that originate in North Dakota.

Notification of an Incident Related to Suspicious Mail, Parcels or Other Substances
Initial notification/consultation regarding a perceived threat from suspicious mail, parcels or other suspicious substances should be conducted in coordination with local law enforcement and the local/regional public health unit.

Prior to an assessment to determine if the item poses a threat, appropriate precautions, such as disabling the heating, ventilation and air conditioning (HVAC) system and initial evacuation of the immediate area or, if necessary, the entire building, should be instituted. The local/regional public health unit will provide consultation and assistance regarding initial precautions.

Attachment 1 contains detailed guidelines regarding suspicious packages. The following are recommendations for recipients of suspicious packages.

- Report the incident to an available supervisor or building security official.
- Do not shake or empty the contents of any suspicious envelope or package.
- Do not smell, taste, or touch the material.
- Do not try to clean up powders or liquids.
- Turn off local fans or ventilation units in the room, if possible.
- Leave the room and close the door, and/or section off the area, to prevent others from entering. (continued on next page)

- Instruct anyone who handled the item to wash their hands with soap and water.

- Remove contaminated clothing and place in a sealed plastic bag if materials spill onto clothing. Shower with soap and water as soon as possible. Do not use bleach or harsh disinfectant on your skin.

- Obtain, if possible, a list of all people who handled the letter/package or were in the room or area when the letter/package was recognized or opened.

Important Telephone Numbers
North Dakota Homeland Security Fusion Center……866-885-8295
(during business hours) 800-472-2121 (after hours)
Federal Bureau of Investigation.....701-232-7241
North Dakota Department of Health (NDDoH)..... .....800-472-2121 (via State Radio). *Request the NDDoH Case Manager be paged.*
North Dakota Division of Emergency Management/.....800-472-2121
State Radio

ATTACHMENT 1
GUIDELINES TO EVALUATE THE THREAT OF AN OBJECT

- Is there an explicit threat (substance need not be present)? Yes No

- Is the object suspicious for a bomb or other hazardous material, e.g., ticking, protruding wires or foil or unexplained material leaking from package? Yes No

- Does the material have a suspicious odor? Yes No

- Does the letter or package have other suspicious characteristics such as:

  - Excessive postage? Yes No
  - Handwritten or poorly typed addresses? Yes No
  - Incorrect titles? Yes No
  - Title, but no name? Yes No
  - Misspellings of common words? Yes No
  - No return address/unknown return address? Yes No
  - Excessive weight? Yes No
  - Lopsided or uneven envelope? Yes No
  - Excessive security materials (e.g., heavily taped)? Yes No
  - Visual distractions? Yes No
  - Marked with restrictive endorsements (e.g., "Personal" or "Confidential")? Yes No
  - Does the letter or package have material present, whether opened or unopened (e.g., powder spilling) Yes No
  - Has material been confirmed by another independent party? Yes No
  - Is there a logical explanation for the letter/package or material? Yes No
  - Is the letter/package "suspicious" because:

    It is unfamiliar? Yes No

    It has no return address? Yes No

    Return address is unknown to recipient or follow-up indicates return address is nonexistent or otherwise "suspicious"? Yes No

DACOTA COLLEGE AT BOTTINEAU
Hostile Work Environment Policy

Dakota College at Bottineau is committed to providing a climate which fosters respect for all campus employees. As part of that commitment, DCB prohibits any action or activity that that creates fear, intimidates, ostracizes, psychologically or physically threatens, embarrasses, ridicules, or in some other way unreasonably interferes with an employee's work performance or creates a hostile or offensive work environment. Hostile Work Environment harassment **will not be tolerated.** Disciplinary action including but not limited to letter of reprimand, leave without pay, or dismissal can be taken against any employee who engages in such harassment.

Anyone who perceives they have been subjected to harassment is encouraged to report the situation to your supervisor or to someone in supervisory line immediately. See reporting procedures for Harassment.

DAKOTA COLLEGE AT BOTTINEAU
Computer Acceptable Use Policies

Faculty, staff and students who use Dakota College at Bottineau computer facilities assume the responsibility for using these resources in an appropriate manner. Misuse of computer facilities and copyright infringements are considered a violation of State Board Policy 1901.2 and is subject to disciplinary action.

All users of DCB computer facilities are required to comply with the following:

- Files, logins, usernames, passwords, and computer output belonging to an individual or to the institution are considered to be personal property. Users cannot examine, change, or use another person's files, or institutional files for which they do not have explicit authorization. Users can not use another person's login and password.
- No obscene or offensive material can be entered into a campus owned-computer, viewed on the computer, saved on the campus file server, or sent through e-mail or the Internet.
- Users cannot deliberately attempt to degrade system performance or capability. Loopholes in the computer systems, knowledge, or special passwords shall not be used to damage a system or file, or to change or remove information in a system or file without authorization.
- University computer systems cannot be used for commercial purposes without written authorization.
- Unauthorized copies of copyrighted material cannot be created, distributed, or knowingly utilized.
- Reconfiguring the hardware arrangement by unplugging various cables and moving hardware from one workstation to another will not be allowed.
- Software downloads to student lab and public area machines is prohibited. Illegal downloading of music and movies is prohibited and may result in the loss of your computer login.

NORTH DAKOTA UNIVERSITY SYSTEM
Computer and Network Usage

Revised: November 02, 2005

INDEX

6.2 Responding to security and abuse incidents
6.3 First and minor incident
6.4 Subsequent and/or major violations
6.5 Range of disciplinary sanctions
6.6 Appeals

1. DEFINITIONS

Authorized use: Use of computing and networking resources shall be limited to those resources and purposes for which access is granted. Use for political purposes is prohibited (see Section 39-01-04 of the ND Century Code). Use for private gain or other personal use not related to job duties or academic pursuits is prohibited, unless such use is expressly authorized under governing institution or system procedures, or, when not expressly authorized, such use is incidental to job duties or limited in time and scope, and such use does not: (1) interfere with NDUS operation of information technologies or electronic mail services; (2) burden the NDUS with incremental costs; or (3) interfere with the user's obligations to the institution or NDUS.

Authorized user(s): Computing and networking resources are provided to support the academic research, instructional, outreach and administrative objectives of the NDUS and its institutions. These resources are extended to accomplish tasks related to the individual's status with NDUS or its institutions. Authorized users are (1) current faculty, staff and students of the North Dakota University System; (2) individuals connecting to a public information service (see section 5.3); and (3) other individuals or organizations specifically authorized by the NDUS or an NDUS institution. For the purposes of this policy, no attempt is made to differentiate among users by the user's group. These policies treat all users similarly, whether student, faculty, staff or other authorized user, in terms of expectations of the user's conduct.

Campus IT Department: Official central information technology department as designated by the institution's president or chief executive officer.

Campus Information Technology Security Officer: Individual, designated by the Institution, responsible for IT security policy education and enforcement, and coordination of incident investigation and reporting.

Campus Judicial Officers: The designated Campus Judicial Officers for students, or appropriate supervising authority for faculty and staff, as defined by the Institution.

NDUS Chief Information Officer Council representative (CIO): The senior staff member responsible for information technology.

Computing and networking resources: Computing resources and network systems including, but not limited to, computer time, data processing, and storage functions; computers, computer systems, servers, networks, and their input/output and connecting devices; and any related programs, software and documentation. Further, it is understood that any device that connects to a campus network, whether wired or wireless, is expected to comply with all NDUS and institutional policies and procedures.

Electronic information: Any electronic text, graphic, audio, video, digital record, digital signature or message stored on or transported via electronic media. This includes electronic mail messages and web pages.

HECN: The North Dakota Higher Education Computer Network, which has been given the responsibility of maintaining the computer and network systems for the North Dakota University System.

Institution: One of the eleven colleges or universities within the North Dakota University System.

Open record: Electronic information used in support of college, university or NDUS business, regardless of where the electronic information originated or resides may be subject to open records laws of North Dakota (see Section 44-04-18 of the ND Century Code).

Scrubbed: The act of ensuring that no data is retrievable from a storage device according to current "best practice."

Sensitive data: Any data, the unauthorized disclosure of which may place the Institution or NDUS at risk.

Server: Any device that provides computing service to multiple computers or individuals.

Student record: As defined by the Family Educational Rights and Privacy Act of 1974 (FERPA), a student educational record includes records containing information directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.

Unit: Department, office or other entity within an institution.

Update: A new release (or version) or a piece of software that is generally understood to be an error correction release and does not contain new functionality.

Upgrade: A new release (or version) of a piece of software that contains new functionality.

User: See Authorized User(s)

2. INDIVIDUAL PRIVILEGES

The following individual privileges are conditioned upon acceptance of the accompanying responsibilities within the guidelines of the Computer and Network Usage Policy.

2.1 Privacy

In general, all electronic information shall be free from access by any but the authorized users of that information. Exceptions to this basic principle shall be kept to a minimum and made only when essential to:

- meet the requirements of the state open records law and other statutory or regulatory requirements;
- protect the integrity of the College or University and the rights and property of the State;
- allow system administrators to perform routine maintenance and respond to emergency situations such as combating "viruses" and the like (see 4.3, 4.4).

2.2. Encryption and password protection

When using encryption utilities or password protection schemes on institutional information or computing equipment, a unit-level recovery process must be used. No data protection schemes may be used to deprive a unit or institution from access to data or computing equipment to which they are entitled.

2.3. Freedom from harassment and undesired information

All members of the campus community have the right not to be harassed by computer or network usage of others (see 3.1.3.).

2.4. Appeals of sanctions
Individuals may appeal any sanctions according to the process defined for their Institution.

3. INDIVIDUAL RESPONSIBILITIES
Each member of the campus community enjoys certain privileges and is responsible for the member's actions. The interplay of these privileges and responsibilities engenders the trust and intellectual freedom that form the heart of this community.

3.1. Respect for rights of others and legal and policy restrictions
Users are responsible to all other members of the campus community in many ways. These include the responsibility to:

- respect and value the right of privacy;
- recognize and respect the diversity of the population and opinion in the community, and;
- comply with NDUS and Institution policy and all laws and contracts regarding the use of information that is the property of others.

3.1.1 Privacy of information
All electronic information which resides on NDUS and institution computers, and any data on any device that connects, wired or wireless, to the campus network may be determined to be subject to the open records laws of North Dakota.

Individuals are prohibited from looking at, copying, altering, or destroying another individual's electronic information without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so unless the information has been placed in a public area such as a web site.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. The NDUS Data Classification and Information Technology Security Standard further defines and explains NDUS and institution data classifications, standards, and security responsibilities.

Except to the extent that a user lacks control over messages sent to the user, electronic information is deemed to be in the possession of a user when that user has effective control over the location of its storage.

3.1.2 Intellectual property
Users are responsible for recognizing and honoring the intellectual property rights of others. Users are prohibited from using, inspecting, copying, storing, and redistributing copyrighted material and computer programs in violation of copyright laws. Software subject to licensing must be properly licensed and all users must strictly adhere to all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.).

When reproducing or distributing information, users are responsible for the observation of copyright rights and other intellectual property rights of others and all state and federal laws, Institutional and NDUS policies. Generally materials owned by others cannot be used without the owner's permission. Written consent from the copyright owner is normally necessary to reproduce or distribute copyrighted material. There are some exceptions such as fair use in teaching and in research.

Documentation of consent to use copyrighted materials must be kept on record and made available to institution officials upon request. The NDUS assumes no obligation to monitor users for infringing activities, but will, when such activities are called to the appropriate official's attention, investigate to determine if there is likely infringement and make appropriate responses.

Users should also be careful of the unauthorized use of trademarks. Certain uses of such marks online on websites or in domain names can constitute trademark infringement. Unauthorized use of an institution's name in these situations can also constitute trademark infringement.

3.1.3 Harassment
Users may not use NDUS or NDUS Institution computers or networks to harass any other person.

Prohibited activities include, but are not limited to: (1) intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right or institutional sanction to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (4) intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; or (5) Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

3.2. Responsible use of resources
Users are responsible for knowing to which resources they have been granted access, and refraining from all acts that waste or prevent others from using these resources, or from using them in ways proscribed by the NDUS or NDUS institutions or state or federal laws.

3.3. Information integrity
Electronic information is easily manipulated. It is the user's responsibility to verify the integrity and completeness of information compiled or used. No one should depend on information or communications to be correct if the information or communication is contrary to expectations. It is important to verify that information with the source.

3.4. Use of personally managed systems
Any device connecting directly to a NDUS or institution network, whether via wire or wireless or modem device must be administered and maintained in a manner consistent with the policies of the NDUS and institution and all applicable laws, including access and security issues. Anti-virus software should be installed and any software installed (especially operating system and anti-virus software) should be kept up-to-date with regard to security patches.

Personal firewalls should be deployed when their installation will not interfere with the function of the device or the administration of the network; and such firewalls should be configured to allow minimal traffic.

At a minimum, password facilities should be utilized to ensure that only authorized individuals can access the system.

Passwords should be a minimum of eight characters and a combination of upper and lower case letters, numbers and special characters, as the system allows. They should not be words found in a dictionary. Nor should they be something that is easily discerned from knowledge of the owner. Passwords should not be written anywhere and not sent via email or shared with others. System administrators will ensure that passwords are not readable in plain text on the systems.

The administrative account/login and password should be changed to values specified by the campus IT department; and any system default "guest" account/login should be assigned a password and disabled.
All unnecessary software and services should be disabled.

Any device configured as a server must be registered with the campus IT department.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. The NDUS Server Information Technology Security Standard further defines NDUS and institution server standards and security responsibilities.

It is the responsibility of the owner/administrator of a personally managed system to maintain logs appropriate to the type of server and to make those logs available to NDUS or institution personnel as needed.

The HECN manages the name space and IP subnets for the NDUS. Policies pertaining to these services can be found at http://www.ndus.nodak.edu/uploads/document-library/835/1901.2-DNS.PDF

3.4.1 Video transmission devices
All audio and/or video transmission devices (web cams, etc.) must be utilized in a manner consistent with these policies and all applicable laws.

3.5. Access to computing and networking resources
The NDUS makes every effort to provide secure, reliable computing and networking resources. However, such measures are not foolproof and the security of a user's electronic information is the responsibility of the user.

Administrative desktop computers should be behind locked doors when the office is unoccupied and access to these devices should be based on minimal need.

Under no circumstances may an external network be interconnected to act as a gateway to the campus network without coordination and explicit approval from the campus IT department.

3.5.1 Sharing of access
Access to computing and networking resources, computer accounts, passwords, and other types of authorization are assigned to individual users and must not
be shared with others. Users are responsible for any use or misuse of their authentication information and authorized services.

Institution Departments or Administrative Offices; or Institution-wide Help Desk or information functions; or officially recognized Faculty, Staff or Student Organizations may be granted permission for multi-user accounts with common authentication, for approved purposes. Requests for these types

of accounts must come from the individual assuming responsibility for the activity of the account and be approved by the NDUS Chief Information Officer Council representative. Only the person responsible for the activity of the account is authorized to share access and authentication information and only persons individually entitled to access NDUS systems may be given access to these accounts.

3.5.2 Permitting unauthorized access
Authorized users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users (see section 1).

3.5.3 Use of privileged access
Access to information should be provided within the context of an authorized user's official capacity with the NDUS or NDUS institutions. Authorized users have a responsibility to ensure the appropriate level of protection over that information.

3.5.4 Termination of access
When an authorized user changes status (e.g., terminates employment, graduates, retires, changes positions or responsibilities within the Institution, etc.), the user must coordinate with the unit responsible for initiating that change in status to ensure that access authorization to all institution resources is appropriate. A user may not use computing and networking resources, accounts, access codes, privileges, or information for which the user is not authorized.

3.5.5. Backups
While the NDUS will make every effort to provide reliable computing facilities, ultimately it is the individual user's responsibility to maintain backups of their own critical data. Such backups should be stored in a secure off-site location.

3.5.6 Device registration
Any desktop computer and any network addressable device that connects to a campus network should be approved by and registered with the campus IT department.

3.6. Attempts to circumvent security
Users are prohibited from attempting to circumvent or subvert any system's security measures. Any security incidents should be reported to the system administrators and the Campus IT Security Officer.

3.6.1 Decoding access control information
Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

3.6.2. Denial of service
Deliberate attempts to degrade the performance of any computer system or network or to deprive authorized personnel of resources or access to any computer system or network are prohibited.

3.6.3 Harmful activities
Harmful activities are prohibited. Examples include, but are not limited to, IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data.

3.6.4. Unauthorized activities

Authorized users may not:

- damage computer systems;
- obtain extra resources not authorized to them;
- deprive another user of authorized resources, or
- gain unauthorized access to systems by using knowledge of:
    - a special password;
    - loopholes in computer security systems;
    - another user's password, or
    - access abilities used during a previous position.

3.6.5. Unauthorized monitoring

Authorized users may not use computing resources for unauthorized monitoring or scanning of electronic communications without prior approval of the campus CIO or the campus or NDUS IT Security Officer.

3.7. Academic dishonesty

Use of NDUS computing facilities to commit acts of academic dishonesty will be handled through existing campus procedures which address allegations of academic dishonesty.

3.8. Personal business

Computing and networking resources may not be used in connection with compensated outside work or for private business purposes unrelated to the NDUS or institutions, except in accordance with the NDUS Consulting Policy.

4. NDUS AND NDUS INSTITUTION PRIVILEGES

4.1. Control of access to information

NDUS and NDUS institutions may control access to their information and the devices on which it is stored, manipulated, and transmitted, in accordance with the policies of the Institution and NDUS and federal and state laws. Access to information and devices is granted to authorized NDUS personnel as necessary for the performance of their duties and such access should be based on minimal need to perform those duties.

4.2. Imposition of sanctions

The Institution may impose sanctions on anyone who violates the Computer and Network Usage Policy.

4.3. System administration access

A system administrator (i.e., the person responsible for the technical operation of a particular machine) may access electronic information as required for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all rights to privacy of information are to be preserved to the greatest extent possible.

4.4. Monitoring of usage, inspection of electronic information

The Electronic Communications Privacy Act allows system administrators or other authorized campus and NDUS employees to access a person's electronic information in the normal course of employment, when necessary, to protect the integrity of computing and networking resources or the rights or property of the Institution or NDUS. Additionally, other laws, including the U.S.A. P.A.T.R.I.O.T.

ACT of 2001, may expand the rights and responsibilities of campus administrators. Electronic information may be subject to search by law enforcement agencies under court order.

The NDUS and Institution may also specifically monitor the activity, systems and accounts of individual users of the Institutions' computing and networking resources without notice. This includes individual login sessions, electronic information and communications. This monitoring may occur in the following instances:

- The user has voluntarily made them accessible to the public.
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Institution or to protect the Institution or NDUS from liability.
- There is reasonable cause to believe that the user has violated, or is violating, Institution or NDUS policies or any applicable laws.
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- Upon receipt of a legally served directive of appropriate law enforcement agencies.
- Upon receipt of a specific complaint of suspected or alleged violation of policy or law regarding a specific system or activity.

Any such monitoring must be accomplished in such manner that all privileges and right to privacy are preserved to the greatest extent possible and with the prior permission of the Campus ITSO or CIO, if reasonable.

For further information, please see 2.1 for information on privacy.

4.5 Suspension of individual privileges

NDUS and Institutions operating computers and networks may suspend computer and network privileges of a user:

- to protect the integrity, security or functionality of the Institution or NDUS and/or their resources or to protect the Institution or NDUS from liability;
- to protect the safety or well-being of members of the community, or
- upon receipt of a legally served directive of appropriate law enforcement agencies or others.

Access will be promptly restored when the protections are assured, unless access is suspended as a result of formal disciplinary action imposed by Campus Judicial Officers, HECN or other legal officers.

4.6 Retention of access

User accounts are assigned to a specific individual at a specific institution within the NDUS. When a specific affiliation is terminated, the NDUS or Institution may elect to terminate the user's account, transfer the account, continue the account for a limited period of time, or, in the case of e-mail, temporarily redirect incoming communications.

4.7 Network maintenance

The HECN and the campus networking personnel have the responsibility of maintaining the networks for the benefit of all authorized users. This implies that, in emergency situations, they may, if there is no other way to resolve a problem, request that a device (whether wired or wireless) be disconnected from the network or powered down, or, if necessary, take such action themselves.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. NDUS network standards are further defined in the NDUS Network Information Technology Security Standard.

5. NDUS AND NDUS INSTITUTION RESPONSIBILITIES

The Institution shall ensure that physical or network access to all critical infrastructures shall be monitored; and such access granted and maintained based solely on need.

Individual campuses are expected to develop policies and procedures to address those environments unique to their campus. Such policies or procedures may not be contrary to the express terms or the intent of NDUS policies and procedures.

5.1. Risk management

Periodic risk assessment of information systems infrastructure and data shall be completed by NDUS and Institutions. Any discovered vulnerabilities should be presented to the appropriate campus and NDUS officials.

The networking services and computer operations personnel are responsible for providing adequate disaster recovery plans and procedures for critical systems under their responsibility in the event of a natural or man made disaster.

5.1.1. Physical concerns

Desktop computers and computer peripherals should be protected from theft and vandalism and any institutionally owned devices should be readily identifiable as institutionally owned. Public access computers should be in a monitored area.

Installations with computer and networking resources will implement reasonable security measures to protect the resources against natural disasters, environmental threats, accidents and deliberate attempts to damage the systems.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. See NDUS Physical Information Technology Security Standards for additional information.

5.1.2. Configuration concerns

The Institution's campus IT department shall, for those desktops they manage, change the Administrative login and password, make inaccessible any system defined accounts and turn off any unnecessary software or services. Any access to a server, other than a public server, should be authenticated and logged. Access to all servers should be based on minimal need.

Software with security vulnerabilities will be patched in a timely manner.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. Refer to the NDUS Server Information Technology Security Standard for more information.

5.2. Security procedures

The NDUS and Institutions have the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional computing and networking resources, and to impose appropriate sanctions when security or privacy is abridged.

Each Institution shall designate an Information Technology Security Officer to coordinate the security efforts on their campus. This individual shall be considered an "other school official" determined to have legitimate educational interests for purposes of sharing information under federal law. This person shall coordinate efforts and share information, with other campus officials, as necessary. The Information Technology Security Officer will keep appropriate records of any incidents/investigations on the Officer's campus and, if requested, share those records with the appropriate NDUS personnel.

The NDUS shall designate an Information Technology Security Officer, who will assist the campus Information Technology Security Officers in their duties and who shall be considered an "other school official" determined to have legitimate educational interests for each campus under federal law.

5.3. Public information services
Institutions may configure computing systems to provide information services to the public at large. (Current examples include, but are not limited to "ftp" and "www") However, in so doing, any such systems must comply with all NDUS and institution policies and applicable laws. Particular attention must be paid to the following sections of this policy: 1(Authorized use), 3.1.2 (Intellectual Property) and 3.2 (Responsible use of resources). Use of public services must not cause computer or network loading that impairs other services or impedes access.

5.4 Communications and record keeping
It is the responsibility of each institution that provides computing facilities to: inform users of all applicable NDUS computing policies and procedures; to address, through existing campus judicial procedures any resulting complaints to maintain appropriate records and to inform the NDUS CIO designate of the progress and resolution of any incident responses; and provide an environment consistent with these policies and procedures.

5.5 Backup and retention of data
Normal backup procedures are employed for disaster recovery on NDUS and institution systems. Therefore, if a user removes electronic information, it may still be retrievable by the system administrators. These backups may or may not be retained for an extended period of time. Backed-up electronic information may be available for the investigation of an incident by system administrators or law enforcement personnel. Administrators of the systems may be required to attempt to recover files in legal proceedings.

For data critical to the function of the Institution, a second set of backups should be maintained off-site in a secured protected area.

5.6 Schedule of service
Most scheduled maintenance of NDUS computing and networking resources will be done at pre-announced times. There are times when some computing and networking resources will be unavailable due to unforeseeable circumstances. Problems may arise with electronic information transmission and storage. Such occurrences may cause a disruption to service or loss of data. The NDUS assumes no liability for loss of service or data. However, all efforts must be made to ensure the availability of services at other than scheduled maintenance times.

5.7 Privacy of records
Campus access to student computer records will be governed by existing campus records policies. Generally, student records, including computer records, fall under the Family Educational Rights and Privacy Act of 1974 (FERPA). The computer records of a student are educational records and cannot

be released without written consent from the student except as elsewhere defined by institutional policy or state or federal law. The institution's response to subpoenas for student records will be carried out as defined by the institution and state or federal law.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. Standards for institutional data and its classifications can be found in the NDUS Data Information Technology Security Standard.

5.8 Domain name services
The HECN administers the nodak.edu domain and IP subnets for NDUS. Procedures for adding hosts and related policies can be found in the "Policy for Name Service and Usage"

5.9 Virus protection software
The HECN shall make available virus-protection software for NDUS users and keep available the most current updates.

5.10 Legal software
The Institution shall periodically audit institutionally owned devices for proper software licenses.

5.11 Data privacy
Any electronic data asset of the NDUS or the Institution shall be classified as Public, Private or Confidential according to the NDUS Data Information Technology Security Standard.

The owner of data is that person, department or office that is responsible for the integrity of the data. It is the responsibility of the owner of the data to classify the data.

It is the responsibility of anyone using or viewing the data to protect the data at the level determined by the owner of the data or as mandated by law.

Appropriate efforts must be taken to ensure data integrity, confidentiality and availability.

6. PROCEDURES AND SANCTIONS
The NDUS makes every reasonable effort to protect the rights of the individual users of its computing and networking resources while balancing those rights against the needs of the entire user community. The NDUS and Institution will make every effort to resolve any system or network problems in the least intrusive manner possible.

6.1. Investigative contact
If anyone is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, ISP security officials, etc.) that is conducting an investigation of an alleged violation involving NDUS or Institution computing and networking resources, they must inform the Institution's Information Technology Security Officer and the NDUS Information Technology Security Officer.

6.2. Responding to security and abuse incidents
All authorized users are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response. In the NDUS, the HECN has been delegated the authority to enforce information security policies and is charged with:

Implementing system architecture mandates, system protection features, and procedural information security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.

Initiating appropriate and swift action, using any reasonable means, in cases of suspected or alleged information security incidents to ensure necessary protection of NDUS or an Institution's resources, which may include disconnection of resources, appropriate measures to secure evidence to support the investigation of incidents, or any reasonable action deemed appropriate to the situation.

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of NDUS or Institution computing and networking resources. All users and units that have reported to them (other than as in 6.1 above) a security or abuse problem with any NDUS or Institution computing or networking resources, including violations of this policy are to:

Take immediate steps as necessary to ensure the safety and well being of information resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 4.5, 4.6 and 4.7).

Make appropriate reports on any discovered unauthorized access attempts or other improper usage of institution or NDUS computing and networking resources.

Ensure that the following people are notified: (1) The administrator of the computer, if known. (2) If appropriate, the campus Information Technology Security Officer or the campus IT Department.

6.3. First and minor incident

Minor infractions of these policies are generally resolved informally by the unit administering the accounts or network in conjunction with the Campus Information Technology Security Officer. Minor infractions are those in which the impact on the computer or network resource is minimal and limited to the local network. Resolution of the infraction will include referral to the Code of Student Life, staff or faculty handbooks, or other resources for self-education about appropriate use. In the case of students, a copy of the resolution will be sent to the Campus Judicial Officer.

6.4. Subsequent and/or major violations

Repeated minor infractions or more serious misconduct may result in immediate loss of computer access privileges or the temporary or permanent modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computing facilities, attempts to steal passwords or data, unauthorized use, distribution or copying of licensed software, or other copyrighted materials, use of another's account, harassment or threatening behavior, or crashing the system. Policy violators will be referred by the campus Information Technology Security Officer to the Campus Judicial Officer for further action.

6.5. Range of disciplinary sanctions

Users who violate this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the institution, and legal action. Use that is judged excessive, wasteful, or unauthorized may result in denial of access to computing and networking resources and may subject the user to appropriate disciplinary and/or legal procedures. Any offense which violates local, state, or federal laws may result in the immediate loss of all computing and networking resource privileges and will be referred to appropriate college or university offices

and/or law enforcement authorities.

6.6. Appeals
Notice of violations and appeals of decisions will follow campus procedures.

REFERENCE: SBHE Policy 1901.2

HISTORY: Chancellor's Cabinet Meeting, June 2001
Chancellor's Cabinet Meeting, January 2003
Chancellor's Cabinet Meeting, April 16, 2003
Chancellor's Cabinet Meeting, November 2, 2005.

DAKOTA COLLEGE AT BOTTINEAU
Armed Assailant Emergency Response Procedures

Emergency Telephone Numbers
From campus phones (except student housing): 9 -911 must be dialed to access emergency services.
From cell phones, off-campus phones and student housing phones: dial 911

Procedures

1. If you are in a building:
    - Don't panic.
    - Do not sound the fire alarm. A fire alarm would signal the occupants in the rooms to evacuate the building and could place them in potential harm as they attempted to exit.
    - Lock yourself in the room and push furniture or anything you can against the door. Lock the windows and close blinds or curtains -- then stay away from the windows. Turn all lights and audio equipment off.
    - If communication is available, **call 911 (9-911 from campus extension).**
    - After calling 911**, call 228-5432 (432) from campus extension)** to activate campus response.
    - Try to stay calm and be as quiet as possible.
    - Remain where you are until you're certain of your safety.

2. If you are caught in an open area such as a hallway or lounge-type area:
    - Don't stay in the open hall.
    - You can try to hide, but make sure it is a well-hidden space.
    - If communication is available, **call 911 (9-911 from campus extension).**
    - After calling 911**, call 228-5432 (432) from campus extension)** to activate campus response.
    - If you decide to run out of the building, keep any objects you can between you and the hostile person(s) while in the building. Once outside, don't run in a straight line. Use trees, vehicles or any other object to block your view as you run. When away from the immediate area of danger, summon help any way you can and warn others.
    - If you are unable to run or hide, you may choose to play dead.
    - If you are caught by the assailant and are not going to fight back, follow their directions and don't look the assailant in the eyes.
    - The last option you have is to fight back. This is dangerous, but depending on your situation, this could be only option.

3. When police arrive:
    - Anyone with a weapon will be considered a suspect.
    - Obey all commands. This may involve your being handcuffed or made to put your hands in the air. This is done for safety reasons and once circumstances are evaluated by the police, they will give you further directions to follow.
    - Assist emergency personnel. The police may need assistance from personnel that have working knowledge of the buildings, exits, escape routes, and mechanical systems.
    - Re-enter a building only when authorized to do so by emergency personnel or Senior Administration

DAKOTA COLLEGE AT BOTTINEAU
Incident Reporting Procedures

Reporting Instructions

Prompt reporting of incidents involving injury or property damage adds tremendous value to our Risk Management process by helping to identify risks, limiting liability, and offering timely handling of claims. All accidents involving staff, faculty, students, or visitors that occur on our campus must be reported within 24 to 48 hours to the State Risk Management Division. To report an accident, complete a **Risk Management Fund Incident Report (SFN 50508)**. You can obtain this form the Business Office or on the web at www.state.nd.us/risk/forms. Forward the completed incident report to the Director of Financial Affairs. The director will file the report with the Risk Management Division. If you are aware of an accident but are unable to complete the form, contact the Director of Financial Affairs for assistance.

Near Miss Reporting

Near misses are incidents that do not result in employee injury or property damage but had the potential for either. Reporting of near misses will aid in correcting a potentially hazardous situation before an injury occurs. Report all near miss incidents by completing a **Near Miss Report**. This report is available from the Business Office or on-line at www.misu-b.nodak.edu/acabusforms.html. After completing this form, it must be forwarded to the Director of Financial Affairs who will investigate the near miss incident and take corrective action to help prevent recurrence.

Injury Reporting – Workers Compensation

Employees must report all work related injuries to their supervisor immediately. When medical assistance is required, the supervisor or assigned person is encouraged to accompany the injured worker to the medical facility rendering service. In all cases, the worker or person accompanying the worker shall notify the medical facility that this is a work related injury and that the injured is a Dakota College at Bottineau employee.

The supervisor shall report work related injuries to the Business Office within 24 hours of the incident or at the beginning of the next regularly scheduled work day (whichever is appropriate). The supervisor must also forward a completed **Risk Management Fund Incident Report** (SFN 50508) to the Director of Financial Affairs within 48 hours of the injury. This form is available from the Business Office or on the web at www.state.nd.us/risk/forms. The injured worker must complete a **First Report of Injury Form** within 24 hours of the incident. This form is only available on-line at https://secure.apps.state.nd.us/wsi/ofroi/ofroiWeb/Welcome.do , and is the only method of submitting a claim to Workforce Safety & Insurance (WSI). The Business Office can assist the employee with the completion of the First Report of Injury form.

DAKOTA COLLEGE AT BOTTINEAU
Near Miss Report

This report is to be filled out by any employee involved in or witnessing a near miss. A near miss is an incident that did not result in any personal injury, property damage or production interruption. It is a very important indicator of potentially harmful future accidents.

Completed by Employee

Department: _____ Building: _____

Date of incident: _____ Time: _____

Location: (Describe where incident occurred) _____

_____

_

Description of incident/potential hazard: _____

_____

_____

_____

_____

_____ _____ _____

Print employee's name Employee's signature Date

Completed by Supervisor

Corrective action(s) taken to prevent recurrence: _____

_____

_____

_____

_____

_____ _____ _____

Print supervisor's name Supervisor's signature Date

Send original to the Director of Financial Affairs

DAKOTA COLLEGE AT BOTTINEAU
Key Control Policy and Procedures

Policy:

Dakota College at Bottineau will maintain a system for the management of keys for the protection of students, staff, faculty, facilities and property. It is the intent of campus administrators to responsibly balance security and protection with building access and personal convenience. This policy establishes a framework by which keys will be issued, monitored and maintained.

Definitions:

- **Key** -- Any device (e.g. card, key pad, metal key, etc.) which is used to gain access to a room, building or restricted area.
- **Key Holder** -- Faculty, staff, and students who are issued keys to college buildings and facilities.
- **Master Key** -- A key which allows access to all buildings and all rooms located within each building.

General Provisions:

- All keys are issued by, and remain the property of DCB.
- The key holder is responsible for using reasonable safeguards to prevent theft, loss or unauthorized use of keys, and for physically securing access points upon entering or leaving a room or facility after operational hours. Unauthorized use includes allowing others to use the keys to gain access to campus facilities. Failure to exercise reasonable safeguards may result in the loss of key privileges.
- Keys will only be issued to employees of Dakota College at Bottineau and only for those areas that are necessary for performance of assigned duties. Students and non-employees will not be issued keys to buildings or rooms. If it is necessary that a student or non-employee have keys, an employee will act as the key holder (with all the responsibilities thereof).
- The Director of Business Affairs is responsible for safeguarding and controlling access to key blanks, core keys, key boxes and master keys.
- The Physical Plant Supervisor (or his/her designee) is the only one authorized to duplicate keys. Any attempt to duplicate keys by any other person is a violation of this policy.
- The Campus Dean and Division Directors have the authority to confiscate keys in possession of a person not authorized to have them.
- The Physical Plant Supervisor is the only one authorized to change, add, or alter any locking device. This includes the installation of hasps or padlocks. All locks will be supplied and installed by the Maintenance Supervisor.
- The Physical Plant Office is responsible for maintaining the key management system which includes the key numbering system, key management database and assignment of rooms for sub- master designations.

- An annual inventory of keys maintained by each key holder can be conducted by the Director of Business Affairs to review the accuracy of system records and to determine if changes in procedures are required.

Requesting Keys:

- A key request is initiated by completing a Key Request Form available in the Business Office or at the DCB website (under Faculty/Staff, downloadable forms, Business Affairs).
- The key request form will be approved by the appropriate Division Director and the Director of Business Affairs before keys are issued. Upon receipt of an approved key request, the Physical Plant Supervisor will prepare the key(s) and delivery them to the Business Office for distribution to the key holder.
- The key holder must personally pick-up and sign a receipt for the keys.
- The Physical Plant Office will maintain a file of all completed key request forms.
- Issuance of a master key requires the approval of the Campus Dean and the Director of Business Affairs.
- Records of all keys issued will be maintained by the Physical Plant Office.

Returning Keys:

- When keys are no longer required for performance of job duties (e.g. reassignment, promotion, change in location, etc.), the key holder shall surrender the keys to the Director of Business Affairs or the Physical Plant Supervisor. The key holder will receive a key receipt as evidence of surrender. Under no circumstances are keys to be transferred to any other individual or kept by the division.
- The key holder must surrender their keys to their supervisor prior to separation of employment. The supervisor will request an inventory report, from the Plant Supervisor, of the keys held by the key holder (see separation checklist). The supervisor with cross check the keys received from the key holder to the report. Discrepancies are reported to the Director of Business Affairs for evaluation and resolution.
- A key-return receipt will be issued when keys are returned.

Lost/Stolen/Non-Returned Keys:

- The key holder can be assessed $10.00 per key which are lost, stolen or not returned.
- If a key is lost or stolen, it is the responsibility of the key holder to immediately notify the Director of Business Affairs. Failure to do so may result in the loss of key privileges.
- If an individual has two or more separate incidents of key violations, the Campus Dean may revoke his/her key privileges.
- If the Campus Dean determines that a security breech exists due to negligence by the key holder, the key holder can be assessed the actual costs incurred to re-key the building (or the affected portion).

DAKOTA COLLEGE AT BOTTINEAU
KEY REQUEST FORM

Keys will be issued in accordance with the key control policy.

# of Keys	Building	Room#	Name of Key Holder
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Justification for Key Request: _____

_____

_____

_____

Authorizations and Approvals

Request by:_____ Date:_____

Assistant Dean : _____ Date: _____

Director of Business Affairs: _____ Date: _____

Executive Dean: _____ Date: _____

DAKOTA COLLEGE AT BOTTINEAU
Employee Separation Checklist

THIS FORM MUST BE RETURNED BEFORE THE EMPLOYEE'S LAST WORKDAY

Supervisor: Please use this form when an employee is leaving DCB. Once all actions are completed, please forward this form to the Business Office.

_____ _____

Employee's Name Last Date of Employment

Address all items applicable with your employee:

____ Submit appropriate documentation to the Business Office concerning the employee's separation, i.e.: resignation letter, notice of reduction-in-force, dismissal notice;

____ Contact the Business Office at #440 for appointment to complete separation or retirement forms;

____ Complete an exit interview form available in the Business Office;

____ Contact Student Services and Business Office to remove access to ConnectND

____ Contact the Information Technology Department to terminate e-mail account, login account and voicemail account

____ Contact Plant Services at #461 to obtain list of keys issued to employee

____ Obtain building and office keys – report missing keys to the Director of Financial Affairs

____ Contact the Dean's Office to remove employee's name from building, office, and telephone directories;

____ Obtain campus equipment (vehicle keys, pagers, cellular phone, laptop computer, etc.);

____ Obtain employee's ID Card, activities pass and parking pass;

____ Contact Library at #454 for confirmation that all library materials have been returned;

_____

_____

All actions completed: _____

Supervisor's Signature

DAKOTA COLLEGE AT BOTTINEAU
REPORTING AND INVESTIGATING THEFT AND FRAUD
Revised August 2010

Campus employees are responsible for safeguarding Campus resources and ensuring they are used only for authorized purposes, in accordance with Campus rules, policies, and applicable law. All employees are responsible for reporting suspected theft, fraud, or unlawful or improper use of public funds or property.

A. As used in this policy, "theft, fraud or unlawful or improper use of public funds or property" includes:

1. stealing, larceny or embezzlement;
2. making or altering documents or files with the intent to defraud;
3. purposely inaccurate accounting or financial reporting at any level;
4. fraudulent conversion or misappropriation of public resources, including funds, supplies or other property;
5. improper handling or reporting of financial transactions;
6. authorizing or receiving compensation for goods not received, services not performed or hours not worked, including payment or receipt of a bribe, kickback or other unlawful or unauthorized payment.

B. Procedures for reporting suspected or detected fraudulent activity

1. An employee with knowledge or suspicion of theft, fraud or unlawful or improper use of public funds or property involving DCB or affiliated entities, shall report that information to their immediate supervisor, the Director of Financial Affairs, or the Campus Dean. An employee with knowledge or suspicion of theft, fraud or unlawful use of public funds involving their immediate supervisor, shall report that information to the Director of Financial Affairs or the Campus Dean.
2. Unreasonable failure to report such information as required may result in discipline, up to and including dismissal.
3. The employee or supervisor who suspects fraudulent activity should not attempt to conduct an investigation.
4. It is a violation of Campus policy to retaliate against an employee who, in good faith, reports dishonest or fraudulent activity.
5. An employee may also anonymously report fraudulent behavior by calling the toll-free hotline number 866-912-5378 or by completing an on-line form at: www.eidebailly.com/hotline

C. Procedures for investigating suspected or detected fraudulent activity

1. The DCB employee designated with responsibility for receiving and acting upon reports under this policy is the Director of Financial Affairs (DFA) or his/her designee. A supervisor or other person who receives a report of suspected theft or fraud shall report that information to the DFA or his/her designee, unless the DFA is implicated, in which case the information shall be reported to the Campus Dean. If both the DFA and the Campus Dean are implicated, the report shall be made to the North Dakota Campus System

General Counsel. The DFA shall inform the Campus Dean, unless the Campus Dean is implicated, in which case the DFA shall inform the General Counsel.

2. The DFA or his/her designee shall take reasonable and appropriate action in response to receipt of a report, which may include an internal investigation, commission of an audit, referral to law enforcement officials, recommended policy or procedure amendments, a report summarizing findings or other steps. The DFA may consult with the NDUS General Counsel and information shall be kept confidential.
3. The DFA or his/her designee, with assistance from other Campus officials as appropriate, has the primary responsibility for the investigation. If the investigation reveals that fraudulent activities have occurred, the DFA or his/her designee will issue a report to the Campus Dean.
4. Decisions to prosecute or involve appropriate law enforcement and/or regulatory agencies for independent investigation will be made by the DFA or his/her designee in consultation with the Campus Dean and may include the NDUS General Counsel.
5. Employee discipline, up to and including dismissal will follow Campus processes and procedures that verify the occurrence of theft, fraud, or unlawful/improper use of Campus resources.

DAKOTA COLLEGE AT BOTTINEAU
Emergency Notification System Policy

Dakota College at Bottineau employs an Emergency Notification System (ENS) to quickly contact or send messages to students, employees, and designated people in event of an emergency. An "emergency" means a situation that poses an immediate threat to the health or safety of someone in the campus or system community or significantly disrupts campus or system programs and activities. In order for the ENS to be an effective communication tool, emergency contact information is necessary for all participants. The following policy delineates who will participate in the ENS, what contact information is needed and how the information is obtained, maintained and protected:

1. NDUS policy 1902 mandates that all university system employees, including student employees, shall participate in the emergency notification system. Participation means employees shall submit emergency notification information and review and update (if necessary) that information at least annually. Employees will receive reminders semiannually to update their records. Emergency notification information includes campus email, campus phone, home phone, home cell phone, and work cell phone. Employees of the North Dakota Forest Service, Sodexho and other non-DCB personnel residing on the campus will also be required to provide emergency notification information.

2. Students other than student employees shall participate in the emergency notification system unless they "opt-out". Students will have the ability to "opt-out", add and update emergency notification information in the Connect ND portal. The portal will allow students to enter campus phone, cell phone, email, texting information, and home phone. The student will receive periodic reminders to review/update their notification information and to provide additional opportunities to participate. Since students can be enrolled on multiple campuses, they may choose to receive emergency notifications from those campuses.

3. Employee emergency notification telephone numbers or other emergency notification information is exempt from the state's open records laws as provided in NDUS Policy 1912 and may be released only as provided in that policy. Student emergency notification information, or contact information such as phone numbers or email addresses submitted for purposes of participation in an emergency notification system, shall be excluded from directory information and is therefore confidential as provided under the Family Educational Rights and Privacy Act (FERPA). However, if a student phone number or email or other address submitted for the purpose of participation in an emergency notification system is also contained in other institution records used for other purposes, the information contained in the other institution records is directory information and not confidential, unless a student has exercised the student's right to refuse to permit disclosure of directory information.

4. The emergency notification system is only intended for use for emergencies as defined in NDUS policy 1902. A test of the emergency notification system will be conducted at least once each semester.

5. Students are allowed to have cell phones "on" (vibrate mode) during class to receive emergency notifications unless instructed otherwise by faculty. If a faculty member instructs students to turn their cell phones off, the faculty member must be able to receive emergency notifications by registered personal cell phone or classroom phone.

6. Emergency notification information will originate from Connect ND databases, and be refreshed a minimum of once per semester. This procedure removes former employees and students from the system.

7. The authority to activate the emergency notification system is limited to the following positions (including their designees): Campus Dean, Director of Financial Affairs, Associate Dean for Student Affairs, Associate Dean for Academic Affairs, Director of Athletics and Director of Housing and Student Life and Plant Services Supervisor.

8. Students, employees, and visitors should report all emergency situations to the local emergency service providers by calling 911 (9-911 from a campus extension). In order to activate a campus response to the situation, the Sheriff's Office will contact one of the positions listing in item 7 of this policy.

9. All media inquires must be referred to the Campus Dean or his/her designee. The Campus Dean is responsible for communications with the media and public for all emergency events (see page 3 of the Risk Management Handbook).

10. Notifications to provide additional details and instructions or to announce a return to normal operations is the responsibility of the Campus Dean or his/her designee.

DAKOTA COLLEGE AT BOTTINEAU
Shelter In-Place/Lock-Down Procedures

Some emergencies, such as a hostage situation, armed assailant, or hazardous material leak, may prevent an evacuation of personnel from a building. These situations may warrant campus administration or emergency services personnel from issuing either a "shelter-in-place" or a "lock-down" notice to help you prepare your environment for temporary safety and security until you can safely evacuate. These procedures are intended to supplement those identified under Armed Assailant Emergency Response Procedures and Hazardous Material Procedures found in this handbook.

A. Shelter In-Place

There may be situations when it is not safe to leave a campus building because of either an accidental or intentional discharge of chemical, radiological or biological agents. When such an event occurs, you may be instructed to "shelter in-place" by campus administration, law enforcement or other emergency response personnel. When you receive a shelter in-place notice, it is recommended for your personal safety that you do the following:

1. Remain inside the building you are in. If outside, go to the nearest building and instruct other people to come inside as well.
2. Close all windows and doors.
3. Turn off all ventilation systems (heaters/air conditioning).
4. If possible, relocate to an interior room with few doors and windows.
5. Seal all doors, windows and air vents with plastic sheeting and duct tape if available. If you don't have these items, use damp paper, clothing or rags to fill the gaps around doors and to cover vents.
6. You will receive instructions and official news through the Emergency Notification System. But it is recommended that you monitor local TV and radio broadcasts as well.
7. If you have internet access, you can access the U.S Department of Homeland Security at www.dhs.gov/dhspublic/index.jsp and get additional information on what to do during a shelter in place event.
8. Do not leave the room until instructed to do so by emergency response personnel or if you receive an "all clear" notice through the Emergency Notification System.

B. Lock Down

A lock down involves staying inside a secure location and NOT evacuating until instructed to do so by campus administration or emergency response personnel. A lock down may be initiated by campus administration when it is determined that it is the best course of action, given the circumstances and information available, for preventing injury or loss of life. The Emergency Notification System will be used to communicate a "Lock Down" notice. The following steps must be taken if a lock down is declared:

1. Faculty and staff will immediately secure students and themselves in the classroom of office. If the door swings out, and it cannot be locked, barricade the door using desks and other large items. If possible, cover any windows or openings that have a direct line of sight into the hallway.

2. If you are in a hallway or other public area, try to get to a room that can be locked or barricaded.
3. Do not sound the fire alarm. A fire alarm would signal the occupants to evacuate the building and potentially put them in harm's way as they attempt to exit.
4. Lock the windows and close blinds or curtains then stay away from the windows.
5. Turn off lights and all audio and video equipment.
6. Try to remain as calm as possible.
7. Stay out of open areas, and be as quiet as possible.
8. Do not leave the room until instructed to do so by emergency response personnel or if you receive an "all clear" notice through the Emergency Notification System.

DAKOTA COLLEGE AT BOTTINEAU

EMPLOYEE CRIMINAL HISTORY BACKGROUND INVESTIGATIONS

Effective 11/05/2012

I. Introduction

Dakota College at Bottineau (DCB) intends to maintain a safe and productive learning, working and living environment. To assist in this endeavor, prospective DCB employees and current employees seeking a transfer or promotion to positions named in this policy must consent to a background investigation. Offers of employment, transfer or promotion are contingent upon the finalist passing the necessary background investigation. In accordance with SBHE policy and procedure 602.3, the type of background investigation varies by position.

II. Type of Background Checks

A. A nationwide FBI criminal history background check (Defined as a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, federal employment, naturalization, or military service) is required **before the beginning of employment** for the following benefitted or non-benefitted positions:
   1. Police officer; and
   2. Security guard.

B. The following positions, whether benefited or non-benefited require a criminal history records check performed by a private vendor **before beginning employment**:

   a. Resident hall and apartment manager or director and assistants;
   b. Information technology staff;
   c. Employees responsible for or with unsupervised access to cash, credit, debit or other financial transactions or numbers, or confidential or other protected information, including medical records, social security numbers, tax, retirement, or vendor or contractor proprietary or other confidential information;
   d. Custodians and other employees with master keys or other means of unsupervised access to residence halls or secure buildings or facilities;
   e. Child care employees and other employees who have unsupervised contact with children;
   f. Part-time instructional staff including online instructors;
   g. Employees responsible for or with access to controlled substances and other drugs, explosives or potentially dangerous chemicals and other substances; and
   h. Counselors and coaches.

C. All other benefited and non-benefitted faculty and staff positions (excluding students unless the position is listed in section A or B) not mentioned in sections A and B require a criminal history records check **before beginning employment**.

III. Procedures

A. All job announcements for positions governed by this policy must state that: "Employment will require passing a criminal history background investigation".

B. All initial contracts and letters of appointments will be issued after the background check has been completed and passed.

C. The selection committee is responsible for reminding applicants, selected for an interview, that a background investigation is a requirement of employment. It is suggested that this reminder be given at the time the applicant is contacted for scheduling an interview.

D. The finalist must provide all necessary information needed to perform a criminal history background investigation. The information is provided with the understanding that Dakota College at Bottineau reserves the right to withdraw the offer of employment if the results of the background check meet the standards described in section H below.

E. All documentation related to a FBI background investigation is confidential and cannot be disseminated. These FBI records must be kept separately and securely from other records, and accessible to only those with a need to know. These records can be destroyed by shredding 30 days after the position is filled. If the records are retained, they will remain confidential and be destroyed by shredding in accordance with DCB's record retention policy.

F. All documentation related to a BCI or private vendor checks are subject to North Dakota open records law and will be maintained in accordance with DCB's record retention policy.

G. Conducting Background Checks
   1. The Director of Business Affairs (or designee) will provide the finalist the forms required to complete the investigation.
   2. The FBI check requires fingerprints with the request. The Director of Business Affairs (or designee) will provide instructions to the applicant for obtaining fingerprints. DCB is responsible for paying the law enforcement agency for fees associated with fingerprinting.

H. Background Check Result Handling and Consideration
   1. After all requested background investigation reports are received, the Director of Business Affairs will notify the supervisor of the results. The supervisor will notify the finalist/employee of the results. If the record is clear, the employment offer can be finalized with a contract or letter of employment.
   2. If the record is not clear, the Director of Business Affairs will coordinate a review of the information. This review will include the supervisor, divisional director and Campus Dean. NDUS legal counsel will be consulted as necessary. The supervisor will notify the finalist/employee of the employment decision based on this review.
   3. Dakota College at Bottineau seeks to provide a consistent method of consideration of the background check results; however, each check is dynamic and many factors may influence the final decision. All results will be considered on a case-by-case basis. It is expected that, over time, the decisions will build a consistent decision logic that will be incorporated into this document. Generally, employment will be denied due to the following results:

      a. Applicant listed on a sexual offender registry of any state
      b. Applicant convicted of drug-related charges within the last three years

c. Applicant convicted of a felony

I. Denial of Employment
   1. If employment is denied based on either a private vendor or FBI investigation report, the finalist/employee has no right of appeal. However, the individual has the right to see and challenge any of the information on the criminal history record and rap sheet. The challenge must be made directly to either the private vendor or the FBI by the individual.
   2. Anyone denied employment on the basis of a background check made through a private vendor is afforded certain rights under the Fair Credit Reporting Act (FCRA). The Director of Business Affairs will coordinate the appropriate notifications to the finalist/employee.
   3. At the discretion of the Campus Dean, the employment decision may be suspended for one week if the results of a challenge would influence that decision.

DAKOTA COLLEGE AT BOTTINEAU
Code of Conduct
June 2010

This Code of Conduct is adopted in accordance with SBHE Policy 308.1* and applies to all Dakota College at Bottineau (DCB) employees. The State Board of Higher Education (SBHE) and entire North Dakota University System (NDUS) are committed to upholding the highest ethical and professional standards. All DCB employees must, at all times, comply with all applicable laws and regulations. Activities that achieve results unlawfully or by unethical behavior - including, but not limited to, payments for illegal acts, indirect contributions, rebates, and bribery - are not tolerated and must be reported. All conduct must meet or exceed minimum standards established by law. Employees who have information concerning a possible violation of this Code or are uncertain about application or interpretation of any legal requirement should report the matter to their supervisor or, if the matter involves a supervisor, to the Campus Dean, Director of Financial Affairs or NDUS legal counsel. Employees to whom such reports are made should consult legal counsel as necessary or appropriate.

A. General Employee Conduct

DCB supports an environment that is free of discrimination or harassment.

1. All employees are expected to conduct themselves in a businesslike manner. Unlawful consumption of alcoholic beverages or use of illegal drugs, being at work while under the influence of alcohol or drugs, disruptive behavior, unlawful gambling, unauthorized use of public property or resources and other unauthorized activities that disrupt the efficient and economical administration of the DCB or the NDUS, are prohibited.
2. Violation of applicable laws or policies governing possession and use of alcoholic beverages or drugs, including the Drug Free Workplace Act, SBHE Policy 615* or applicable campus policy, is cause for dismissal or other discipline.
3. Likewise, sexual or other harassment (including actions contributing to a hostile work environment) in violation of federal or state law, SBHE Policy 603.1* or applicable DCB policy, is cause for dismissal or other discipline.

B. Conflicts of Interest

All employees are expected to perform their duties conscientiously, honestly, and in accordance with the best interests of DCB and the NDUS.

1. Employees must comply with applicable federal and state laws, including policies in Section 611 of the SBHE Policy Manual.
2. Employees may not unlawfully use their position or the knowledge gained as a result of their position for private or personal advantage.
3. All employees are responsible for their own actions. Any individual who has concerns or questions regarding a perceived or potential conflict or regarding application or interpretation of federal or state law or SBHE policy is encouraged to communicate with their supervisor or NDUS legal counsel.

C. Outside Activities and Employment

All employees share responsibility for good public relations, especially at the community level. Their readiness to help with charitable, educational, and civic activities brings credit to DCB and the NDUS and is encouraged.

1. However, all employees must comply with applicable federal and state laws, policies in Section 611 of the SBHE Manual* and related DCB polices.
2. At all times, employees must avoid outside activities that create an excessive demand upon their time and attention, thus depriving the campus of their best efforts in fulfilling their job duties or that create a conflict of interest, or an obligation, interest, or distraction, that interferes with the independent exercise of judgment in the best interest of the campus.

D. Relationships With Clients and Suppliers; Conflicts of Interest

1. All employees must comply with applicable federal and state laws and SBHE Policy 611.4* and are responsible for being familiar with applicable laws and policies governing conflicts of interest.
2. Employees should avoid investing in or acquiring a financial interest for their own accounts in any business organization that has a contractual relationship with DCB or any NDUS institution, or that provides goods or services to the NDUS, if such investment or interest could influence or create the impression of influencing their decisions in the performance of their duties.

E. Gifts, Entertainment and Favors; Kickbacks and Secret Commissions

Employees may accept only *de minimus* contributions, such as purchase of a meal at reasonable value as part of a conference or other event with no conditions attached to such purchase (as permitted under applicable federal and state laws).

1. Employees may not accept entertainment, gifts, or personal favors that could influence, or appear to influence, decisions in favor of any person or organization with whom or with which campus or NDUS has, or is likely to have, business dealings.
2. Employees may not accept any other preferential treatment under circumstances that because of their position with DCB, the preferential treatment may influence or be perceived as influencing their official conduct.
3. Employees may not receive payment or compensation of any kind from any source for DCB duties and responsibilities, except as authorized under NDUS pay policies. Specifically, the acceptance of "kickbacks" or commissions in any form from vendors, suppliers or others is prohibited and any violation of this prohibition shall be cause for dismissal and result in referral for prosecution under the law.

F. DCB Funds and Other Assets

1. Employees who have access to campus funds and other assets in any form must follow the prescribed procedures for recording, handling, and protecting money and

other assets as detailed in applicable procedure manuals or other explanatory materials.

2. Any person who has information concerning possible fraud or dishonesty shall immediately report such information to their supervisor, Campus Dean, Director of Financial Affairs or to NDUS legal counsel.
3. Employees who are responsible for spending or approving expenditure of DCB funds or incurring any reimbursable expenses must comply with all applicable laws and policies and use good judgment on behalf of DCB to ensure that good value is received for every expenditure.
4. DCB funds and all other assets are for DCB purposes only and not for personal use or benefit. DCB or other public equipment, supplies and other property or assets may not be used for private or personal use, except as authorized under SBHE Policy 611.5 or other applicable law or policy.

G. DCB Records and Communications

Accurate and reliable records of many kinds are necessary to meet DCB legal and financial obligations and to manage the campus affairs.

1. DCB books and records must reflect in an accurate and timely manner all business transactions.
2. The employees responsible for accounting and recordkeeping must fully disclose and record all assets and liabilities and exercise diligence in enforcing these requirements.
3. Employees must not make or engage in any false record or communication of any kind, whether internal or external, including, but not limited to, false expense, attendance, enrollment, financial, or similar reports and statements, or false advertising, deceptive marketing practices, or other misleading representations.

H. Dealing with Outside People and Organizations

Employees must take care to separate their personal roles from their DCB positions when communicating on matters not involving DCB and NDUS business.

1. Employees may not use DCB identification, stationery, supplies, and equipment for personal or political matters.
2. When communicating publicly on matters that involve campus business, employees may not represent that they speak for DCB, unless that is one of their duties or they are otherwise authorized to do so.
3. When dealing with anyone outside the campus, including public officials, officers and employees must take care not to compromise the integrity or damage the reputation of DCB and the NDUS.

I. Prompt communications

In all matters involving communication with DCB students, customers, suppliers, government authorities, the public and others, officers and employees must endeavor to make complete, accurate, and timely communications and respond promptly and courteously to all proper requests for information and complaints.

J. Privacy, Confidentiality and Open Records

Employees must at all times comply with applicable laws, regulations and SBHE policies concerning privacy, confidential records, access to open records and records retention.

K. Reporting Suspected Violations; Procedures for Investigating Reports

1. Employees shall report suspected violations of this Code to their supervisor, Campus Dean, Director of Financial Affairs or NDUS legal counsel.
2. In addition, DCB will maintain a fraud hotline and suspected violations may be reported by use of that hotline.
3. Any employee who makes a report in good faith shall be protected against retaliation of any kind; any employee who retaliates or attempts retaliation in response to a good faith report shall be subject to dismissal or other discipline.
4. Failure to report known or suspected violations is in itself a violation and may lead to dismissal or other disciplinary action.
5. Alleged violations of this Code shall be investigated by the Director of Financial Affairs and/or NDUS legal counsel, or other person designated by the Campus Dean.
6. All employees shall cooperate in investigations of alleged violations.
7. A violation of this Code is cause for dismissal or other appropriate disciplinary action, in addition to any criminal or other civil sanctions that apply.

L. Employee Review and Certification

1. Review of this Code of Conduct shall be part of each new employee's orientation or training. Employees shall sign a statement certifying that they have read and agree to comply with the Code.
2. Benefitted employees shall annually certify in writing that they have read and are in compliance with the Code.

DAKOTA COLLEGE AT BOTTINEAU

I acknowledge that I have carefully read and reviewed all the information contained in the:

Code of Conduct
&
Theft & Fraud Reporting Policy

By signing this document, I understand that my failure to comply with the laws, rules, policies and procedures referred to within these documents may result in disciplinary action up to and including termination of College employment and possible criminal prosecution, depending on the nature of the violation.

_____

Name
(print legibly: last name, first name, middle initial)

_____

Signature

_____

Today's Date

_____

Department

To be properly credited for participating in the fraud training program, please complete and return the signature page to your supervisor.

Original signed forms are required, faxed copies cannot be accepted

DAKOTA COLLEGE AT BOTTINEAU
VIDEO SURVEILLANCE POLICY
August 2010

A. Purpose

The purpose of this policy is to regulate the use of surveillance equipment which has been installed for security or investigation purposes. This standard practice applies to all personnel of Dakota College at Bottineau (DCB) who are authorized to use the surveillance equipment.

A committee made up of the Associate Dean of Student Affairs, Director of Financial Affairs, Plant Services Supervisor and Director of Information Technology will designate the placement and storage methods of any surveillance equipment.

B. General principles

1. The purpose of surveillance equipment is to:
    a. Provide a visual deterrent to crime and policy violations
    b. Assist law enforcement with criminal investigations
    c. Assist Campus Administrators in protecting campus assets
2. Any use of security technologies for other purposes is prohibited by this policy.
3. The use of surveillance equipment will be conducted in a professional, ethical, and legal manner. Personnel involved will be appropriately trained and supervised in the responsible use of the technology. Abuse and destruction of surveillance equipment will result in disciplinary action consistent with the rules and regulation governing students and employees of DCB.
4. Information obtained through surveillance equipment will be used exclusively for security, risk management investigation purposes, and enforcement of DCB and North Dakota University System policies and procedures.
5. The use of any surveillance equipment will be conducted in a manner consistent with all existing College policies and legal requirements.
6. The use of surveillance equipment for security purposes at DCB is limited to uses that do not violate the reasonable expectations of privacy as defined by law. Surveillance equipment installed for security purposes will not be placed in such a manner that confidential or sensitive information is visible.
7. Any data retained for investigations or proceedings will be burned to a DVD and retained for three years. DCB will retain other video feeds for a minimum of fourteen (14) days.
8. For every building containing video surveillance equipment, DCB will post signage at each exterior entry warning that surveillance cameras are located within the premises.

C. Viewing of Recorded Media

1. Only the Campus Dean, Associate Dean of Student Affairs, Director of Financial Affairs, Plant Services Supervisor, Director of Housing and Director of Information Technology may review the results of the use of surveillance equipment. Other individuals who may have a legitimate need to review the recorded material may be permitted to do so with the approval of the Director of Financial Affairs.
2. A log will be maintained by those personnel identified in C.1 to record the time and date the video surveillance information is reviewed. The log must contain the time, date, persons present, and justification for the review. A copy of all logs will be maintained by the Director of Financial Affairs.

D. Examples of surveillance equipment use in public areas

1. Protection of buildings and property – Building entrances and exits, parking lots, exercise rooms, etc.
2. Monitoring building access – Records access to building entrances.
3. Criminal investigation – Robbery, destruction of property, assault, etc.
4. Accident investigation – Personal injury, vehicle accident, medical problems, etc.
5. Policy violation – Use of alcohol, hostile work environment, harassment, fraud, etc.