NORTH DAKOTA
UNIVERSITY SYSTEM
The Vital Link to a Brighter Future

NDUS Procedures

SUBJECT: MISCELLANEOUS **EFFECTIVE:** November 02, 2005

Procedure: 1901.2 Computer and Network Usage

INDEX

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:

1. meet the requirements of the state open records law and other statutory or regulatory requirements;

2. protect the integrity of the College or University and the rights and property of the State;

3. 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:

1. The user has voluntarily made them accessible to the public.
2. 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.
3. There is reasonable cause to believe that the user has violated, or is violating, Institution or NDUS policies or any applicable laws.
4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
5. Upon receipt of a legally served directive of appropriate law enforcement agencies.
6. 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.

600 E Boulevard Ave, Dept. 215, Bismarck ND 58505-0230 701.328.2960 ndus.office@ndus.nodak.edu