COMPUTER HANDBOOK

Who should I call if I need help?

If you are having trouble with:

- network functionality, including e-mail issues, suspected virus issues, desktop/laptop issues, network issues (drives H:, S:, and T:), or any other issues not related to NIIMS - call 471-2443. Glen Riedel and Mark Peterson are responsible for this area.
- Nebraska Insurance Information Management System (NIIMS) issues – call 471-8332. If you receive a NIIMS error message please copy the error message by pressing the key combination <Alt + Print Screen and email to Cyndie White and Barb Sorensen for review. To create a copy of the error message, press the key combination <Alt + Print Screen>. In Lotus Notes, open a new memo and paste the information by pressing the key combination <Ctrl + V>. Include a brief explanation about what steps were completed before the error occurred**.** Barb Sorensen and Cyndie White are responsible for this area.

What do the different drive letters mean and what gets backed up?

You will mostly use the following drive letters:

C:/ This drive letter represents the hard drive physically located on your PC. You do not need to be logged into the network to access this drive. This should be used when security is not important and/or when a backup is not required. Anyone that turns on your computer will have access to this drive.

H:/ This drive letter represents a network directory that access is limited to only you. Because this is on the network, you must be logged into the network to access this drive. Also, this drive is backed up on a daily basis.

S:/ This drive letter represents a network directory that access is not limited. While all staff can access documents located on this drive, only other employee's within you division can make changes to documents and add documents under this drive. Because this is on the network, you must be logged into the network to access this drive. Also, this drive is backed up on a daily basis.

T:/ This drive letter represents a network directory that access is limited to your division only. Other employee's within your division can make changes to documents and add documents under this drive, but no employee outside your division can access this drive. Because this is on the network, you must be logged into the network to access this drive. Also, this drive is backed up on a daily basis.

What should I do if I suspect a virus or my computer is acting strange?

If practical, leave the computer as it was when you noticed the problem. Contact the Help Desk at 471-2443 immediately. Someone will visit you to diagnose the problem as soon as possible.

What is done to protect my computer from viruses?

The Department utilizes McAfee anti-virus software on network computers (including the e-mail server) and desktop/laptop computers. Approximately once a week, you will receive an update to the anti-virus program that you must accept and download. This usually happens when you first log on to the network. However, if a high-risk virus has been identified during the day, you will be asked to accept and download the update immediately.

The Department also updates Windows using the Windows Update utility. The I/S area determines what updates should be on each computer and then updates your computer remotely. Unless you use a laptop that is not normally connected to the network, under no circumstances should you attempt to use Windows Update from the Microsoft website unless directed to do so by the I/S area.

The Department also utilizes a firewall to limit access to the Department's network.

How do I change my passwords?

Network

You will be required to change your Network log-in password every 90 days. This password must be at least 6 characters in length. When you log-in to the network for the first time, no password is required, however you will be required to change the password at this time. To change the Network password before the 90 day expiration period:

Press Ctrl, Alt, Delete at the same time. Select the Change Password button and follow the instructions.

Lotus Notes

Your Notes password is not required to be changed. While in Notes, navigate to **File>Security>User Security**…Enter your current password. Select change password from the pop-up window and enter your current password again and follow the instructions.

NIIMS

Although NIIMS does not force you to change your password, your NIIMS password should be changed every 90 days per Policy 23. While in NIIMS, navigate to **Overviews>Administrative>Change Password** and follow the instructions.

POLICY NO. 20
Department of Insurance
Amended December 22, 1999
Amended June 1, 2006

SUBJECT: SECURITY AND SAFEGUARDING OF THE COMPUTER SYSTEM

Purpose. Because our computer system is an important tool in the way we do our jobs, certain policies and procedures are being implemented to assure:

1. Only authorized individuals can access the Department's system,

2. The data, hardware, and software of the Department are adequately protected from damage or theft,

3. The Department is in compliance with all software licensing agreements, and

4. Any hardware or software problems are corrected as soon as possible to minimize downtime.

These policies are supplement to any other policies set forth in statute or the NITC Standards and Guidelines.

Passwords/Security

All passwords must be at least six (6) characters in length and should contain at least one alphabetic and one numeric character.

The NIIMS and Network login password must be changed once every ninety (90) days. Disclosing passwords to a third party, including disclosing passwords to Administrators, is not allowed. **Passwords are not to be written down and left where a third party could discover them.** All passwords that have been disclosed to a third party or are suspected of being known by a third party must be immediately changed. Because the network and NIIMS assigns the employee's login name to an activity, this will provide assurance that responsibility for any activity is properly assigned to the appropriate employee.

The number of consecutive unsuccessful login attempts to enter a password is restricted to three. After three attempts, the login name will not be allowed access to the system until reset by the I/S Division. This will discourage access by unauthorized individuals.

The initial login procedure will include a notice stating (1) the system is to be used only by authorized users, and (2) by continuing to use the system, the user represents that he/she is an authorized user. The initial login procedure will also provide the user information on the last login time and date. Any user that suspects unauthorized access using his/her login name and password must report this immediately to the I/S Division. No more than three (3) simultaneous on-line network sessions are allowed unless authorized by the I/S Division. This allows an employee to be on up to three different machines and does not require the employee to login using someone else's ID and password.

No employee shall change or attempt to change the initial power-on password of any computer. This is the password that must be entered before DOS or Windows is launched. The I/S Division and each employee that uses the computer know these passwords. If this password is changed and later forgotten, there is no way to recover the password to allow the computer to operate.

Malicious Software

Any Department computer that is suspected of having a computer virus must be immediately reported to the I/S Division. Users must not attempt to remove any computer viruses found on the computer system. Only the I/S staff can remove viruses found on the system. Even though a virus scan is performed at each start-up, this program may miss new viruses. Reporting a virus immediately will limit the damage it may cause.

All disks leaving the Department shall include the following:

While the Department of Insurance has made every attempt to insure this disk is free from malicious software, you should also take necessary precautions.

In the event a third-party accuses the Department of passing a virus, the Department can show that it made every attempt to insure malicious software does not affect other systems.

Hardware and Software

Users shall not load, download or run **any** file or software on the Department's computers unless permission is first obtained from the I/S Division or the Director. The only exceptions to this statement are work-related text, spreadsheet, word processing and similar files that are not licensed and that are received in the normal course of Department business. Prohibited software includes, but is not limited to, games, diagnostic software, and security systems override software. This prohibition applies whether the software is loaded onto the PC's hard drive, run from a floppy or CD-ROM drive, or run from the Internet.

Only peripherals that are the property of the Department can be connected to PCs or laptops owned by the Department unless first approved by the I/S Division or the Director. Any hardware or software that is not authorized by the I/S Division or the Director will not be supported by the I/S Division and will be investigated for proper authorization. If it is determined that proper authorization has not been obtained, the unauthorized hardware and/or software will be removed.

Periodic monitoring of all computers will be done by the I/S Division to insure no unauthorized software has been loaded on the Department's computers.

All software or hardware problems shall be immediately reported to the appropriate I/S staff member.

Safeguarding Department Property/Appropriate Use

The Department of Insurance's computers, printers and communications systems are for business use. Policies regarding usage of e-mail and Internet access are similar to those that apply to telephones. These systems shall not be used for soliciting business, selling products or engaging in any commercial activities unless expressly authorized by the Director. No employee shall use the Department's systems to express his or her opinion on non-business matters. The State's telecommunications policy includes the following statement:

> Acceptable uses of the SDCN (State Data Communications Network) include:

> To communicate to children at home, teachers, doctors, day care centers, and baby sitters, to family members to inform them of unexpected schedule changes, and for other essential personal business. The use of the State's telecommunications systems for essential personal business shall be kept to a minimum and shall not interfere with the conduct of state business.

All messages sent and files created using the Department of Insurance's computer and communications systems, including electronic mail systems, Word, Excel, PowerPoint and Access documents, are the property of the Department. As such, the Director reserves the right to examine all data stored in or transmitted by these systems. Internet e-mail will be monitored and unusual usage patterns will be investigated.

No employee shall use an e-mail account assigned to another employee. This will provide some assurance that any e-mail sent using the employee's e-mail account was actually sent by that employee.

To limit the possibility of theft or damage to Department computers, Department computer shall remain in the possession of the employee as carry-on luggage and not checked in as airline luggage systems. Laptop computers must be transported in their protective carrying case at all times. An employee may be responsible for repair or replacement costs if a laptop computer was damaged during transportation and the protective carrying case was not used.

All computer program documentation and computer hardware and software belonging to the Department must remain with the Department when an employee, consultant, or contractor terminates employment with the Department.

In the event any Department hardware is lost or stolen, this fact must be reported immediately to the I/S Division. The Department will notify the Department of Administrative Services - Materiel Division as required by State Statute Chapter 81, Section 1118.02(2). The Materiel Division Administrator shall, with the advice of the Attorney General, take the proper steps to recover such state property or the reasonable value thereof from the responsible party if it is determined that the property was lost, stolen, or destroyed due to negligence or carelessness.

New and Terminated Employees

When any individual, whether permanent, temporary, or an intern, is **hired** by the Department, a Computer and Network Resources Checklist must be completed by both HR and the hiring division identifying what computer resources will be required. This form must be completed and forwarded to the I/S division within two days after the individual has accepted the position in order to give the I/S division time to allocate the resources.

When any individual, whether permanent, temporary, or an intern, **terminates** from the Department, an Employee Departure Checklist must be completed by both HR and the hiring division identifying what computer resources will be required. This form must be completed within two days after receiving notification that the employee will be terminating in order to give the I/S division time to unallocate the resources. After the I/S division has been provided this checklist, the employee’s supervisor will be given within one working day 1) access to employee’s email account, 2) a CD of the My Documents and/or Data folder on the employee’s hard drive and any data contained on the employee’s H drive. Supervisors will have 10 working days from the employee’s last day before the I/S division requests written authorization to delete the employee’s files from the network and computer.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Acceptable Use Policy
State Data Communications Network

Category	**Network Architecture**
Title	**Acceptable Use Policy** **State Data Communications Network**
Number	

Applicability

☑ **State Government Agencies**

□ All .... **Not Applicable**

☑ Excluding: Higher Education .... **Standard**

□ **State Funded Entities -** All entities receiving state funding for matters covered by this document .... **Not Applicable**

□ **Other:** _____________ .... **Not Applicable**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____________.
Guideline - Adherence is voluntary.

Status	☑ Adopted □ Draft □ Other:_________
Dates	Date: March 9, 2004 Date Adopted by NITC: March 9, 2004 Other: Previous version dated September 1997

Prepared by: Department of Administrative Services, Division of Communications
Authority: Neb. Rev. Stat. § 86-516(6) and § 81-1120.27
http://www.nitc.state.ne.us/standards/

1.0 Standard

1.1 Application and Intent

This policy shall apply to all users of the State Data Communications Network (SDCN). It is intended to provide minimum standards for acceptable use, including clarification of uses which are consistent or inconsistent with this policy. Any state agency, board, commission or affiliate organization may adopt policies or standards more stringent than those contained herein.

All use of the State Data Communications Network (such as, internet logs and email) is the property of the State of Nebraska and is subject to applicable State and Federal statutes, such as the public records laws of the State of Nebraska as applicable. End users should not have any expectations of privacy regarding personal business conducted on the State Data Communications Network unless protected by State or Federal statute.

1.2 Acceptable Uses

Use of the SDCN shall be consistent with the goals of:

- simplifying and disseminating information;
- encouraging collaborative projects and sharing of resources;
- aiding technology transfer within and outside the State of Nebraska;
- fostering innovation and competitiveness within Nebraska;
- building broader infrastructure in support of the performance of professional, work-related activities.

Acceptable uses of the SDCN include:

1. To provide and simplify communications with other state agencies, units of government, and citizens.
2. To communicate and exchange professional development information, including online discussion or debate of issues in a field of knowledge.
3. To exchange communications in conjunction with professional associations, advisory committees, standards activities, or other purposes related to the user's professional capacity.
4. To apply for or administer grants or contracts for work-related applications.
5. To carry out regular administrative communications in direct support of work-related functions.
6. To announce new products or services within the scope of work-related applications.
7. To access databases or files for purposes of work-related reference or research material.
8. To post work-related questions or to share work-related information.
9. To communicate to children at home, teachers, doctors, day care centers, and baby sitters, to family members to inform them of unexpected schedule changes, and for other essential personal business. The use of the State's telecommunications systems for essential personal business shall be kept to a minimum and shall not interfere with the conduct of state business.

1.3 Unacceptable Uses

Unacceptable uses of the SDCN, subject to remedial action (see Section 1.4), include, but are not limited to:

1. Violation of the privacy of other users and their data. For example, users shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users, or represent themselves as another user unless explicitly authorized to do so by that user.
2. Violation of the legal protection provided by copyright and licensing laws applied to programs and data. It is assumed that information and resources available via the SDCN are private to those individuals and organizations owning or holding rights to such information and resources, unless specifically stated otherwise by the owners or holders, or unless such information and resources clearly fall within the statutory definition of a public record. It is unacceptable for an individual to use the SDCN to gain access to information or resources not considered a public record without the granting of permission to do so by the owners or holders of rights to such information or resources.
3. Downloading of software in violation of license agreements.
4. Violation of the integrity of computing systems. For example, users shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
5. Use of the SDCN for fund-raising or public relations activities unrelated to an individual's employment by the State of Nebraska.
6. Use inconsistent with laws, regulations or accepted community standards. Transmission of material in violation of any local, state or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene or harassing material.
7. Malicious or disruptive use, including use of the SDCN or any attached network in a manner that precludes or significantly hampers its use by others. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and use of the SDCN to make unauthorized entry to any other machine accessible via the network.
8. Unsolicited advertising, except for announcement of new products or services as described in #6 under "Acceptable Uses."
9. Use of the SDCN for recreational games.
10. Use in conjunction with for-profit activities, unless such activities are stated as a specifically acceptable use.
11. Use for private or personal business ventures such as second sources of income, other family member business interests, etc.
12. Misrepresentation of one's self, an agency, or the State of Nebraska when using the SDCN.

1.4 Remedial Action

Any agency, board, commission or affiliate organization within which a violation of this policy occurs shall take immediate remedial action. To assist agencies in carrying out this responsibility, the Department of Administrative Services (DAS) shall notify the agency, board, commission or affiliate organization upon learning of a possible violation. DAS shall be notified of any remedial action taken in response to a violation of this policy.

Remedial action may include disciplinary proceedings against the individual or individuals responsible for the violation of this policy, including termination of employment. If, in the judgment of DAS, it is believed that criminal activity has taken place within the SDCN infrastructure, DAS will notify the proper authorities and will assist in any investigation and prosecution of any offense.

DAS accepts no responsibility for traffic which violates the acceptable use policy of any other networks connected, either directly or indirectly, to the SDCN. If the owner of any network connected to the SDCN notifies DAS of a violation of their acceptable use policy, DAS shall inform the agency, board, commission or affiliate organization within which such violation occurred. It shall be the responsibility of the agency, board, commission or affiliate organization to take appropriate remedial action and notify the owner of the connected network.

2.0 Definitions

2.1 State Data Communications Network (SDCN)

State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to State computers.

The purpose of the SDCN is to provide a vehicle that allows data communications to occur between agencies and across interstate and intrastate boundaries. Use of the SDCN is subject to the policies and standards contained in this document.

3.0 Applicability

This policy shall apply to all users of the State Data Communications Network (SDCN).

4.0 Responsibility

The Department of Administrative Services is responsible for administration of the SDCN and for ensuring compliance with applicable laws, regulations and policies. This responsibility is statutorily granted to DAS under the statutory authority of the Division of Communications in sections 81-1120.01 through 81-1120.28.

Each agency, board, commission or affiliate organization using the SDCN is responsible for the activity of its users and for ensuring that its users are familiar with this Acceptable Use Policy. Failure to comply with this policy may constitute grounds for disciplinary action (see Section 1.4).

This policy applies to all users of the SDCN, or any other networks accessed through a SDCN connection, including the Internet. Compliance with this policy and the acceptable use policies of any other networks accessed through a SDCN connection is also subject to enforcement by the owner of that network. For example, abuse occurring on a network outside the geographical boundaries of Nebraska will be considered a violation of this Acceptable Use Policy, and a violation of other applicable local, state or federal policies if access to that network was acquired via the SDCN.

It is normally the responsibility of those networks to enforce their own acceptable use policies. The Department of Administrative Services will make every effort to inform its clients of any restrictions on the use of networks to which it is directly connected as such information is made available by the network provider.

Should a violation of this Acceptable Use Policy occur, the individual who committed the violation shall be personally liable for his/her actions. Lack of knowledge of or familiarity with this policy shall not release an individual from such liability.