NEVADA DEPARTMENT OF AGRICULTURE
COMPUTER USE
POLICY #AG-2-ADM-6

PURPOSE:

This policy establishes procedures for the appropriate use of the Nevada Department of Agriculture (NDA) technology, including but not limited to equipment, hardware, software, network (including wireless networks), computers, e-mail, internet, intranet, and proprietary data as it pertains to NDA.

POLICY:

Information technology resources within NDA are to be used in a manner that supports the mission of the agency. This policy provides guidelines regarding employee privileges, requirements, limitations, and liabilities of using and maintaining NDA technology.

SCOPE:

This policy applies to all NDA employees, contractors, and all other persons who may use computer resources owned or managed by NDA, and/or is connected by any means to the state SilverNet Network (SilverNet is the State's Wide Area Network (WAN), used by agencies for connection between agency PCs and LANs, host computers and state application programs, and outside access to the Internet).

REFERENCES:

NRS 205.473 to 205.513: Unlawful Acts Regarding Computers and Information Systems, NRS 242.300, NRS 281.195, and NRS 281A.400, NRS 239B.040. The State of Nevada Information Security Program Policy 4.100000 Rev B, and NDA Prohibitions and Penalties.

PROCEDURES:

1. **System Access**
    a. All users must safeguard the confidentiality, integrity and availability of NDA systems, including password login, access codes, network access information and log-on IDs from improper access, alteration, destruction or disclosure.
    b. Users shall only access or use NDA systems when authorized. Users must abide by NDA's and Enterprise IT Services (EITS) policies regarding the protection of data and information stored on these systems.
    c. When personally owned systems are used for NDA business, NDA retains the right to any NDA records or materials developed for NDA use. Also, any materials must be appropriately safeguarded according to

applicable standards, including, but not limited to, virus protection, protected access, and backups.

d. When a user ceases to be an employee, contractor, or other authorized user of NDA systems, the user must not use NDA's facilities, accounts, access codes, privileges, or information for which he/she is no longer authorized. This includes the return of all NDA IT resources including hardware, software, data, and peripherals.

2. **Use of State Systems**
   a. Users must not use NDA systems to engage in activities that are unlawful or violate federal or state laws, NDA, State or EITS security polices or in ways that would:
      i. Be disruptive, cause offense to others, or harm morale.
      ii. Be considered harassing or discriminatory, or create a hostile work environment.
      iii. Result in State or NDA liability, embarrassment, or loss of reputation.
   b. Users must maintain the integrity of information and data stored on NDA's systems by:
      i. Only introducing data that serves a legitimate business purpose.
      ii. Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.
      iii. Protecting data and information stored on or communicated across NDA systems, and accessing appropriate data or information only when authorized.
      iv. Protecting data and information communicated over internal or public networks to avoid compromising or disclosing nonpublic information or communications.
   c. While NDA systems are primarily intended for NDA-business purposes, limited (incidental and occasional) personal use is permitted by users so long as it does not:
      i. Interfere with work responsibilities or business operations.
      ii. Involve interests in personal outside business or other non-authorized organizations or activities (which may include, but not limited to, selling personal property, soliciting for or promoting commercial ventures, or soliciting for or promoting charitable, religious, or political activities or causes).
      iii. Result in personal financial gain for the user or an associate.
      iv. Violate any of the federal or state laws or NDA, State or EITS security policies.
      v. Lead to inappropriate cost to the NDA.
      vi. Excessively uses of system resources.
   d. Written prior approval from the Deputy Director (PCN 0002) and the employee's Administrator is required for any exceptions to any part of section 2c. A request for an exception shall be for a limited scope and a limited time and cannot interfere with employee's work responsibilities and NDA's business operations. Any employees wishing make a request for an exception must make it in writing in a memo. The memo must include the purpose for requesting the exception, identify the length of time (beginning and ending date for the exception), total time expected to use for requested exception, assurances that the exception will not

interfere with the employee's work or other NDA employees' work nor will the employee be accessing prohibited materials , identify benefits to the agency for granting this exception, identify all benefits, including financial benefits to the employee, and detail the NDA resources to be used for request and identify all web sites and list their URL's that will be used for the requested exception. This memo once completed must be submitted to the and submit the request to the Business Process Analyst (PCN 0017), who will make a technical and policy review of the request and make a written recommendation for approval or disapproval to the Deputy Director and the employees' Administrator. Within 15 business days of receiving the written recommendation from the Business Process Analyst, the Administrator and Deputy Director must approve or disapprove in written the employees request for exception to 2c and provide a copy of the approval or disapproval to the Business Process Analyst for recordkeeping purposes.

e. User's must check all electronic media, such as software, CDs, flash drives, and files for viruses when acquired through public networks (e.g., internet sites) or from outside parties before using them on any of NDA's systems. This can be done using virus detection programs prior to installation or use. If users suspects or detects a virus, the applicable system(s) or equipment shall not be used on any NDA system until the virus is removed. If a user suspect or detects a virus while using electronic media, such as software, CDs, flash drives, and files for viruses when acquired through public networks (e.g., internet sites) or from outside parties on the NDA system, the matter must be immediately reported to either the Business Process Analyst (PCN 0017) or the IT Technician 4 (PCN 0030).

In compliance with NRS 281.195, Section 5, any inappropriate use of the computer or technology must be reported. As such, IT staff will report prohibited activity to supervisors (and to Administrators and Deputy Director as necessary). Furthermore, IT staff is authorized to remove any unauthorized software or hardware.

3. **Software**
   a. Only NDA approved and properly licensed software will be used or installed on NDA computers, and will be used according to the applicable software license agreements. Installing personal or unauthorized software without the approval NDA IT staff is prohibited.
   b. It is the responsibility of the NDA's IT staff to maintain and support all technology (hardware and software). No other employee is permitted to open, modify, or otherwise alter the operating nature of agency technology. In no case shall any third-party software be installed on the computer or network by the user. Software that is required must be licensed, and must be requested from and installed by IT Staff. Updates to licensed software are *not* considered new software.

4. **Security**
   a. The security standards for password and authentication were developed by the State of Nevada Enterprise IT Services. In accordance with the

State of Nevada Security Policy, and Procedure 118, User Identification and Authentication (Passwords), all passwords must meet the minimum requirements:

   i. Passwords must be a minimum of eight (8) characters long.
   ii. Passwords must contain a combination of upper and lower case letters.
   iii. Passwords must include **at least** one number (0-9).
   iv. Passwords must include **at least** one special character (e.g., #, $ %, etc.).

b. Passwords must be changed at least every 90 days, but not more than once per day unless a comprise is reported or suspected.
c. Passwords cannot be re-used or rotated within three previous password changes.
d. Passwords must not be shared with anyone, EITS staff will never ask you for your password.
e. Users must ensure that any non-public information, data or software that is stored, copied, or otherwise used on State systems is treated according to the State and NDA's standards regarding non-public information, applicable agreements, and intellectual property restrictions.
f. If users take "mobile" storage devices/media off State premises they need to take proper measures to ensure sensitive data is protected in the event that the devices/media are lost, stolen, or hacked. Mobile storage devices/media may include, but is not limited to: laptops, thumb drives (USB flash drives), and CDs. If "personal information" or highly sensitive data (e.g., SSNs, etc.) on these devices then it must be encrypted. In addition, users must obtain approval from the NDA's management staff before taking sensitive data off state premises.
g. All workstations must be logged off or locked when a user is logged in and leaves the immediate physical area of the workstation. If there is no activity for fifteen minutes the screen will automatically lock and the user will have to enter their password to log in.

5. **Email**
    a. The State email system is to be used to support NDA business by facilitating communication and transmission of documents and files.
    b. Personal use of email on the state's system is a privilege, not a right. As such, the privilege may be revoked at any time.
    c. All messages distributed via NDA's email system, even personal emails, are the property of NDA. Employees must have no expectation of privacy in anything that you create, store, send or receive on NDA's email system.
    d. Management has the right to view employees' usage patterns and take action to assure that agency Internet and email resources are devoted to maintaining the highest level of productivity.
    e. Inappropriate use of email includes, but is not limited to, sending and forwarding:
        i. Messages, including jokes or language, that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive or otherwise inappropriate (for example, messages about age, race, gender, disability, sexual orientation, national origin or similar matters).
        ii. Pornographic or sexually explicit materials.
        iii. Chain letters.
        iv. Information related to religious materials, activities or causes.
        v. Charitable solicitations unless sanctioned by the State or Director.
        vi. Auction-related information unless sanctioned by the State or Director.
        vii. Software or copyrighted materials without a legitimate business or instructional purpose.
        viii. Large personal files containing graphics or audio files.
        ix. Materials related to personal or commercial ventures or solicitations for personal gain.
        x. Information related to political materials, activities, or causes unless sanctioned or permitted by the State or Director.
        xi. Unauthorized or inappropriate mass distribution of communication.
        xii. Any other materials that would be improper under this policy or other State or EITS policy.

In addition to avoiding the prohibited acts above, email etiquette should be used. While e-mail communications are less formal than other forms of written correspondence, the employee should always strive for a professional message by reviewing the content for clarity, grammar, punctuation, format, and tone.

6. **Internet Use and Network Access**
    a. Use of the Internet is primarily intended for business purposes. Casual use of the Internet is permissible, during breaks or other non-working hours as long as it does not interfere with the conduct of any duties, nor conflict with any policy, or NDA Prohibitions or Penalties.
    b. Inappropriate use of the Internet includes, but is not limited to, accessing, sending, forwarding information about, or downloading from:
        i. Sexually explicit, harassing, or pornographic sites.
        ii. Sites that promote violence and acts of discrimination towards another group.

iii. Peer-to-peer sharing of music, video or software files.
iv. Use of streaming media (e.g., radio, music, etc.).
v. Phishing, fraud, or hacking, viewing sites that encourage those activities.
vi. Any attempt to circumvent, harm, disable, or otherwise interfere with the agency network or network resources.
vii. Using entertainment software such as games or non-work related materials or on-line gambling.
viii. Instant messaging, chat rooms through downloaded programs or social networking sites.
ix. Offensive or insensitive materials, such as sexually or racially oriented topics.

c. The use of instant messaging software on state-owned computers is strictly prohibited. This type of uncontrolled communication method is considered a high security risk to state IT resources. All access to such systems from state networks will be blocked or disabled if possible (EITS Policy on Peer-to-Peer File Sharing and Instant Messaging – Control No. 130).
d. Employees must have no expectation of privacy of browse history or internet use. Even when browsing history or cookies are deleted, they are not removed permanently and remain on the network server. Public servants are under specific scrutiny, and integrity should be exercised in every way.
e. In order to maintain optimal network speed and bandwidth, as well as to monitor the network for defense against virus and other malware intrusion, NDA's IT staff remotely monitors and regularly audits browsing history, as does the State of Nevada EITS.

7. **Online Security Awareness Class Required Annually**
   a. All employees are required to annually take the Nevada Information Security Awareness (NISA) online training at https://nvelearn.nv.gov. Annually, through the Deputy Director's office, supervisors will be required to report all NISA online training completed by their employees by December 31st.

POLICY COMMUNICATION:

This policy will be made available to all employees within the Department of Agriculture and to the public.

DIRECTOR'S POLICY AUTHORIZATION:

Jim R. Barbee, Director

Date 1/15/15

APPROVED BY THE BOARD OF AGRICULTURE ON 12/3/14

Effective Date