

# DHHS Information Technology (IT) Acceptable Use Policy

---

**Issue Date:** October 1, 2013

**Effective Date:** October 1, 2013

**Revised Date:**

**Number:** DHHS-2013-002

## 1.0 Purpose and Objectives

The purpose of this policy is to:

- Define acceptable use of Nebraska Department of Health and Human Services (DHHS) and State IT resources
- Promote effective and efficient use of information technology resources.

DHHS and State IT Resources can be effective tools for DHHS staff provided they are used appropriately and adequately protected. It is the responsibility of every IT resource user to know DHHS policies.

## 2.0 Scope and Applicability

The scope of this policy applies to DHHS personnel, contractors, consultants, temporary employees, volunteers, vendors, and business partners (hereinafter referred to as "Staff") with access to DHHS IT resources.

This policy applies to all DHHS and State IT resources (as defined in section 3.1 of this policy) owned, leased, or managed by DHHS.

### 2.1 Policy Enforcement

Should a violation of this policy occur, it is the responsibility of management for the area in violation to mitigate or remediate the violation in a timely manner. Violation of this policy, as it includes compliance with federal and state regulations, may result in criminal and monetary penalties for DHHS and Staff found violating these standards. Any Staff who committed the violation will be personally responsible for their own actions and any reasonably foreseeable consequences of those actions. Lack of knowledge or familiarity with this standard shall not release an individual from their responsibilities.

Any Staff working directly for DHHS found to have violated this policy may be disciplined in accordance with the applicable workplace policies and labor contracts administered by DHHS Human Resources. Such discipline may include termination of employment.

Any Staff working directly for a business partner under contract with DHHS to provide services to or on behalf of DHHS who is found to have violated this policy may be disciplined in accordance with state and federal laws and penalty provisions as defined in the service contract. Such discipline may include termination of the service contract.

### **3.0 Policy**

DHHS and State IT resources are the property of DHHS and the State of Nebraska and are provided for the specific and express purpose of performing state business. Acceptable use of DHHS IT resources and the State Communication System (SCS)/DHHS network is limited to activity directly related to performing state business as outlined in DHHS acceptable use standards defined in section 3.1 of this policy.

Uses of IT resources for any purpose other than to carry out state business will be considered a violation of this policy. DHHS owns all information compiled, stored, and used by Staff and reserves the right to monitor all IT resources to verify compliance of this policy.

### **3.1 Acceptable Use of IT Resources**

#### **3.1.1 Acceptable Use of IT Devices**

IT Devices used by Staff to perform DHHS business activities must be owned, leased, managed or approved by DHHS and meet specifications and requirements published by IS&T and approved by IS&T for agency use.

- 3.1.1.1 – IT devices are defined as desktop computers, servers, laptop computers, PDA's (personal digital assistant), MP3's players, tablet computers, mainframe computers, printers, routers, switches, hubs, portable storage devices, digital cameras, cell phones, smart phone, multi-functional devices, and any other electronic device that creates, stores, processes, or exchanges DHHS information created, stored, contracted, or managed by DHHS. Hereinafter referred to as "IT devices".
- 3.1.1.2 - Staff are responsible for the reasonable care and protection of IT devices and for meeting all policies and standards governing their use.
- 3.1.1.3 – Use of IT devices provided by DHHS is limited to authorized actions and transactions necessary for the performance of State business or sponsored activities.
- 3.1.1.4 – Authorized Home Office access to DHHS network, applications, email, and/or DHHS information is restricted to the use of desktop computers, laptops, remote access software, and procedures provided by or approved by IS&T.
- 3.1.1.5 – Staff authorized to work periodically from remote locations using personal desktop computers or laptops are restricted to access DHHS IT devices using a unique assigned DHHS secure remote access account. Confidential and protected data owned by DHHS may only be

accessed or processed using a DHHS-provided remote access account. Confidential or Highly Restricted data owned by DHHS, or accessed from a DHHS IT Device, will not be stored on any IT Devices not owned, managed, or approved by IS&T. Staff must insure personal IT Devices are maintained and kept current and meet minimum security safeguard and security software requirements as defined in the *DHHS-2013-001-A Securing Hardware and Software Standard*.

- 3.1.1.6 - Wireless access devices (including but not limited to laptop computers, smartphones, tablet computers, and other mobile devices) used by Staff for business activities must:
- be owned, leased, or approved by DHHS
  - meet specifications and requirements published by the IS&T
  - be approved for use by the IS&T

### **3.1.2 Acceptable Use of DHHS Network (LAN, WAN, Internet/Intranet/Extranet)**

DHHS network is defined as the Local Area Network (LAN), and Wide Area Network (WAN), owned by, contracted by, or managed by DHHS, and DHHS Cellular, Broadband Internet/Intranet/Extranet access, supported by, contracted by, or managed by DHHS.

- 3.1.2.1 – Acceptable use of the DHHS network must be limited to actions and transactions necessary for the performance of State business or sponsored activities.
- 3.1.2.2 - No Individual may implement wireless technology to process any DHHS transactions without the review and approval of the IS&T.
- 3.1.2.3 - Only IS&T authorized staff may install a wireless access device to the DHHS network connection jack, port, PC, or other devices connected to the DHHS network.
- 3.1.2.4 – DHHS network access may not be used to perform any illegal activity such as trying to gain unauthorized access to restricted sites (hacking), harassment of any kind, creation of unauthorized Intranet sites or pages, sharing of copyrighted material, or the production of any material that may be deemed offensive.
- 3.1.2.5 – Use of the DHHS network to deliberately spread software viruses of any kind is strictly forbidden and may result in disciplinary action up to and including termination of employment.
- 3.1.2.6 – Staff are responsible for the reasonable protection and use of the DHHS network access assigned to them and must follow all security rules and standards defined and published in the *DHHS-2013-001-A DHHS Securing Hardware and Software Standard*.

- 3.1.2.7 – The DHHS network may not be used for any unauthorized file sharing, downloading any unauthorized music, video, or software. Staff may be held personally liable for any fines or judgments that may result from their actions.
  
- 3.1.2.8 - The DHHS network operates on the State of Nebraska State Communication System managed by the OCIO. DHHS supports and enforces state policy NITC 7-101 *State Of Nebraska Acceptable Use Policy* for use of the State Communications System (SCS). The following are acceptable uses as published for policy NTIC 7-101.
  - 3.1.2.8.1 - For the conduct of state business.
  
  - 3.1.2.8.2 - For state government sponsored activities.
  
  - 3.1.2.8.3 - For use by state Staff and officials for emails, text messaging, local calls, and long-distance calls to children at home, teachers, doctors, daycare centers, baby-sitters, family members, or others to inform them of unexpected schedule changes, and for other essential personal business. Any such use for essential personal business shall be kept to a minimum and shall not interfere with the conduct of state business. A state Staff or official shall be responsible for payment or reimbursement of charges, if any, that directly result from any such communication. [Neb. Rev. Stat. § 81-1120.27(1)] Essential personal business shall not include use of the State Communications System for personal financial gain or campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question. These uses are prohibited. [Neb. Rev. Stat. § 49-14,101.01(2) and § 49-14,101.02(2)]
  
  - 3.1.2.8.4 - And, for such other uses as allowed by law.

### **3.1.3 Acceptable Use of Electronic Communication (Email, Instant Messaging, Data Exchange, Remote Access, E-FAX)**

Electronic communication includes email, instant messages, electronic data exchange, and any other electronic method of exchanging information created, stored, contracted, or managed by DHHS.

- 3.1.3.1 All electronic communication is the property of DHHS and not the personal property of any individual. DHHS rules and regulations govern

privacy and confidentiality of information contained in electronic communication.

- 3.1.3.2 Acceptable use of the electronic communication access provided by DHHS must be limited to actions and transactions necessary for the performance of State business or sponsored activities. DHHS supports and enforces the State of Nebraska NITC 7-101 *Acceptable Use Policy* standards and guidelines. All other use is prohibited.
- 3.1.3.3 Transmitting or emailing confidential or protected DHHS information to be used in an unauthorized remote location is prohibited.
- 3.1.3.4 Emailing confidential or protected DHHS information to an authorized external partner must be encrypted using DHHS-provided or authorized encryption tools.
- 3.1.3.5 Deliberate spreading of software viruses of any kind is prohibited and may result in disciplinary action up to and including termination of employment.
- 3.1.3.6 Deliberate spreading of unsolicited email or electronic messages (i.e., SPAM) is strictly prohibited and may result in disciplinary action up to and including termination of employment.
- 3.1.3.7 Staff are responsible for the reasonable protection and use of the electronic communication access granted to them and must follow all security rules and standards published by IS&T.
- 3.1.3.8 No electronic communication technology may be used by Staff that is not provided by or approved by IS&T.
- 3.1.3.9 No remote access to the DHHS network, LAN, WAN, or any software application is permitted without the review and approval of IS&T.
- 3.1.3.10 Staff are not allowed to create a Personal Folders File (.pst) from the DHHS Email System. PST files are not reliable, vulnerable to data loss, can become corrupted, are not backed up, and hinder eDiscovery.
- 3.1.3.11. As email messages are property of the state Staff are not allowed to forward email messages, containing State or DHHS information from their state email account to a personal email account.

#### **3.1.4 Acceptable Use of DHHS Electronic Information (Data)**

Electronic information is defined as any digital information (data), picture, or graphics owned, created, stored, retrieved, processed, contracted, maintained, or managed by DHHS.

- 3.1.4.1 Electronic information used by Staff in the course of doing business is the property of DHHS and is subject to all policies, procedures, privacy rules and regulations, and acceptable use guidelines that may be implemented by DHHS. It is the responsibility of the user to know and abide by rules governing access and use of this information.
- 3.1.4.2 Use of electronic information is restricted to State business or supported activities and is subject to all policies, procedures, privacy rules and regulations, and acceptable use guidelines implemented by the DHHS agency, division, or program area that owns or holds the license of the electronic information.
- 3.1.4.3 Confidential and Highly Restricted electronic information may not be copied, processed, or stored on personal IT devices.
- 3.1.4.4 No electronic information may be copied or distributed in violation of any policies, procedures, privacy rules and regulations, and acceptable use guidelines implemented by the DHHS agency, division, or program area that owns or holds the license of the electronic information.
- 3.1.4.5 Accessing or attempting unauthorized access to PHI (protected health information), FTI (Federal Tax Information) or other DHHS protected private and confidential information for other than a required business “need to know” is prohibited.
- 3.1.4.6 Confidential and Highly Restricted electronic information may not be copied or stored on a mobile or portable IT devices unless fully encrypted using procedures provided by or approved by IS&T.

### **3.1.5 Acceptable use of Electronic Signatures**

Nebraska Administrative Code (NAC) Title 437 Digital Signatures Act sets the standard for the creation of and use of electronic signatures as enacted by Nebraska Revised Statute §86-611.

- 3.1.5.1 Use of an electronic signature must comply with all standards set down by NAC Title 437 and meet the electronic signature configuration requirements defined in NAC Title 437 Chapter 7.

### **3.1.6 Acceptable Use of Social Media**

- 3.1.6.1 Use of DHHS IT assets to access or interact with social media is limited to the actions and activity defined in the DHHS Social Media Policy managed by the DHHS Communications and Legislative Services unit.

- 3.1.6.2 Posting, texting, or otherwise distributing confidential or protected information including; but not limited to, client, patient, or employee data, video, pictures, email, or text messages on any social media is prohibited.

**3.1.7 Acceptable Use of DHHS Data Applications**

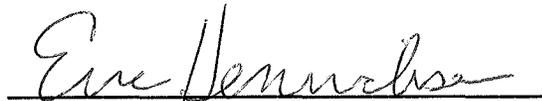
Data applications are defined as software applications created, owned, licensed, or managed by DHHS and used to create, store, retrieve, process, and maintain information owned, supported, contracted, or managed by DHHS.

- 3.1.7.1 Use of a software application is restricted to state business only and is subject to all policies, procedures, security/privacy rules, regulations, and acceptable use guidelines implemented by the DHHS division or program area that owns or holds the license of the software application.

**4.0 Revision History**

Legal Review – 09-30-2013  
Policy Approved – 09-30-2013

**Signature:**



Date: 9/30/2013

**Eric Henrichsen**  
**Information System & Technology Administrator**  
**Nebraska Department of Health & Human Services**