NWF Health Network
Policy & Procedure

Series: 900: Data Collection, Records and Reporting

Policy Name: Use of Information System Resources

Policy Number: 912

Origination Date: 03/09/2009 **Revised:** Board Meeting of 06/27/2024

Policy

It is the policy of NWF Health Network (NWFHN), to establish a standard for the acceptable use of computer resources for its employees and Case Management Organizations (CMOs).

Procedure

A. General Requirements

1. This policy applies to all employees, contractors, consultants, temporary staff, and other workers at NWFHN and CMOs and pertains to all information resources that are owned or leased by NWFHN.
2. NWFHN reserves the right to audit networks and systems on a periodic basis to ensure compliance.
3. Users accessing the Internet are representing NWFHN.
    a. All communications should be for professional reasons.
    b. Users are responsible for seeing that the Internet is used in an effective, ethical and lawful manner.
    c. Databases may be accessed for information as needed.
    d. E-mail may be used for business contacts.
4. The installation of any personally owned electronic devices (i.e., PDAs, external storage media) is prohibited.

B. Security and Proprietary Information.

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies.
    a. Examples of confidential information include, but are not limited to: company private or identifying client information.
    b. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Users need to keep passwords secure and not share accounts.
    a. Authorized users are responsible for the security of their passwords and accounts.
    b. System level and user level passwords should be changed quarterly.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at fifteen (15) minutes or less, or by logging off (control + alt + delete) when the host will be unattended.
4. All portable computers will be encrypted and equipped with tracking software.
5. Postings by employees from NWFHN email address to newsgroups is not permitted, unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the NWFHN Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

C. Unacceptable Use.

1. Under no circumstances is an employee of NWFHN authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NWFHN-owned resources.
    a. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.
    b. Attempting to gain access or accessing another user's system files or messages.
    c. Solicitation of non-NWFHN business, or any use of the Internet for personal gain
    d. Internet use that results in disrupting the operation of the NWFHN network or the network(s) of other users (e.g., streaming video and/or audio).
    e. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NWFHN.
    f. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NWFHN does not have an active license is strictly prohibited.
    g. Unauthorized downloading of any software. All software downloads require prior approval of the Director of Information Services or his designee.
    h. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
    i. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
    j. Using a NWFHN computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
    k. Making fraudulent offers of products, items, or services originating from any NWFHN account.
    l. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
    m. Effecting security breaches or disruptions of network communication.

i. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

ii. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

n. Port scanning or security scanning is expressly prohibited unless prior notification to NWFHN is made.

o. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

p. Circumventing user authentication or security of any host, network or account.

q. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

r. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

s. "Surfing" pornographic, gaming, warez, or any other web sites of a questionable nature is expressly prohibited.

D. Email and Communications Activities. The following activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within NWFHN's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NWFHN or connected via NWFHN's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. Email signature blocks that contain any information that is not strictly related to the conduct of official agency business
9. The use of email stationery.

E. Employee Responsibility for Mobile Devices Owned by NWFHN

1. Mobile Devices owned by NWFHN in order to conduct business must be used appropriately, responsibly and ethically. The following must be observed:

a. Company-owned Mobile Devices are the property of NWFHN and must be treated, used, and safeguarded as such. If an employee damages or loses a company-issued Mobile Device, the employee must notify their manager immediately.

b. If an employee damages a company-issued mobile device, their supervisor is responsible for notifying NWFHN immediately in order for the device to be deactivated.

c. No employee is to use company-owned devices for the purpose of illegal transactions, harassment, or obscene behavior, in accordance with other existing employee policies.

d. Employees are prohibited from using a company-issued Mobile Devices while operating a motor vehicle unless utilizing a hands-free device. Further, if state or local laws are more restrictive, the employee must follow the appropriate law.

e. Mobile devices must not be loaned to or used by others.

F. Lost, Stolen, Hacked, or Damaged Equipment

1. Employees are expected to protect mobile devices used for work-related purposes from loss, damage, or theft. In an effort to secure sensitive company data, employees are required to have remote wipe software (MDM) installed on their mobile devices by the IT department prior to using the devices for work purposes.

   a. This software allows all NWFHN data to be erased remotely in the event the mobile device is lost or stolen. The remote wipe process will remove all NWFHN programs and data from the phone and if requested for personal devices can reset the device to factory defaults. NWFHN will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or remote wiping. Employees must notify management immediately in the event their mobile device is lost or stolen. If the mobile device is damaged, the employee must notify management immediately.

2. The employee will be responsible for the cost of repair or replacement. If an employee reports more than one lost, broken or stolen device in a 12-month period, the employee may be subject to appropriate disciplinary action regarding the misuse of a company asset. This action may include a deduction from the employees' pay for replacement of the hardware.

3. When equipment or a device (laptop, desktop, smart phone, iPad, other) is lost or stolen, immediately call the Police to report the incident at any time of day or night. In addition, if any NWFHN equipment or devices are damaged by a shelter/foster child or parent thereof, a police report will be filed for insurance purposes.

4. If a NWFHN owned device or personal device containing NWFHN data or used to access NWFHN data is lost or stolen while out of office, first file a police report with the appropriate local authorities. Then, also report the occurrence to NWFHN.

5. Authorities will gather initial details of the loss or theft from you including whether or not the device was on, logged into the NWFHN network when stolen, if it contained files with sensitive NWFHN data, and if those files were encrypted and password-protected or not. The police will ask for contact information from you for follow-up. Please make immediate contact with the IT department once a report is filed.

6. The IT department will, among other things, reset your password and block all access to network resources, including e-mail, until such a time that you can change your password.

7. IT will contact you to determine the nature and scope of any compromised NWFHN sensitive data.
8. If there was a potential compromise of sensitive information or exposure of network resources, the IT Department may confer with appropriate NWFHN officials and/or legal counsel, coordinate notification to affected individuals, and report the incident as required.

G. Traveling in a Personal or Rental Car

1. Extreme temperatures can damage a laptop. You should not leave a laptop in an unattended vehicle.
2. If you must leave your laptop in an unattended vehicle for a short period of time, always lock your laptop in the trunk of the car. A visible laptop is a target. This should also apply to your daily commute, as you never know when you may decide to make a "quick stop" for milk or coffee.
3. On rare occasions when a vehicle may not have a trunk or lockable compartment, the laptop must still be locked in the vehicle and stored out of sight.

H. Enforcement. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.