Status **Active** PolicyStat ID **10449082**

Origination	04/2016	Owner	Michael Kinnell
Last Approved	06/2022	Policy Area	Information Technology
Effective	06/2022		
Last Revised	06/2022		
Next Review	06/2023		

Acceptable Use

POLICY

It is the policy of the Detroit Wayne Integrated Health Network (DWIHN) to maintain acceptable use of IT resources. The acceptable use policy is designed to protect the employees and the DWIHN from risks that IT resources used inappropriately would create. These risks include but are not limited to possible legal issues, virus, spyware, adware, malware, ransomware, and other infections of DWIHN systems, and possible compromise of servers, desk-top computers, laptops, corporate cell, voice, mobile devices, or the DWIHN's network. Management is committed to protecting DWIHN's partners, employees, and the organization from damaging or illegal actions through intentional or unintentional means. This policy applies to all Users.

This policy applies to all information, in whatever form, relating to DWIHN's activities and to all information handled by DWIHN relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by DWIHN or on its behalf.

PURPOSE

This acceptable use policy defines acceptable use of computer equipment, software, and data owned by the DWIHN. These rules protect the employees and DWIHN. Inappropriate use exposes DWIHN, the User, and Consumers to risks including virus attacks, compromise of systems and services, the potential leak of consumer's personal and healthcare related information, and legal issues. It also exposes the DWIHN to legal issues and compromises the systems and data.

APPLICATION

1. The following groups are required to implement and adhere to this policy: DWIHN Board, DWIHN Staff, Contractual Staff, Access Center, Network Providers, Crisis services vendor, Credentialing Verification Organization (CVO), consultants, temporary staff, and personnel

affiliated with third parties, and agents operating on behalf of DWIHN.

2. This policy impacts the following contracts/service lines: All Service Lines.
3. This policy applies to all equipment that is owned or leased by DWIHN.

KEY WORDS

1. **Systems:** All IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, phones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third-party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.
2. **Proprietary information:** Information that is not public knowledge (such as confidential information, certain financial data, test results etc.)

STANDARDS

System Use

1. DWIHN proprietary information stored on electronic and computing devices whether owned or leased by DWIHN, the employee or a third party, remains the sole property of DWIHN. All data stored on DWIHN's systems is the property of DWIHN. Employees ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
2. DWIHN's systems exist to support and enable the business and operations of DWIHN. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleague's productivity and nor should it result in any direct costs being borne by DWIHN other than for trivial amounts (e.g., an occasional short telephone call).
3. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of DWIHN proprietary information.
4. Employees may access, use or share DWIHN proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
5. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning the personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager. DWIHN IT Department reserves the right to regularly audit networks and systems to ensure compliance with this policy.
6. For security and network maintenance purposes, authorized individuals within DWIHN may monitor equipment, systems, and network traffic at any time, per the Audit Policy.
7. DWIHN reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. DWIHN can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the

content stored in the email and data files of any user and examination of the access history of any users.

8. Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent legitimate access by all properly-authorized parties.

Data Security

1. Users must take all necessary steps to prevent unauthorized access to confidential information including Protected Health Information (PHI).
2. Users are expected to exercise reasonable personal judgment when deciding which information is confidential.
3. Users must not send, upload, remove on portable media or otherwise transfer to a non-DWIHN system any information that is designated as confidential, or that they should reasonably regard as being confidential to DWIHN, except where explicitly authorized to do so in the performance of their regular duties.
4. All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
5. System-level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
6. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended. Users must keep passwords secure and not allow others to access their accounts.
7. Postings by employees from a DWIHN email address to newsgroups is prohibited. Any communication with newsgroups should take place through the Office of Communications, should an employee wish to comment on a news blog or social media site, they should do from a personal email account during non-work hours.
8. Users who are supplied with computer equipment by DWIHN are responsible for the safety and care of that equipment and the security of software and data stored on those devices as well as other DWIHN systems that they can access remotely using it.
9. Because information on portable devices, such as laptops, tablets, and phones are especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.
10. DWIHN staff are not to sub-loan equipment to any other individuals without adhering to the checkout procedure of the DWIHN Information Systems Helpdesk.
11. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
12. Because information on portable devices, such as laptops, tablets, and phones are especially

vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of DWIHN authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DWIHN-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

All employees should use their own judgment regarding what is unacceptable use of DWIHN's systems. The activities below are provided as examples of unacceptable use, however, it is not exhaustive. Should an employee need to compromise these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

1. All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
2. All activities detrimental to the success of DWIHN. These include sharing sensitive information outside the company, such as consumer information and customer lists, as well as defamation of the company.
3. All activities for personal benefit, that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).
4. All activities that are inappropriate for DWIHN to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
5. Circumventing the IT security systems and protocols which DWIHN has put in place.
6. 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 DWIHN.
7. 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 DWIHN or the end user does not have an active license is strictly prohibited.
8. Accessing data, a server or an account for any purpose other than conducting DWIHN business, even if you have authorized access, is prohibited.
9. Exporting software, technical information, encryption software or technology, in violation of

international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

10. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
11. Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
12. Using a DWIHN 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.
13. Making fraudulent offers of products, items, or services originating from any DWIHN account.
14. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
15. Effecting security breaches or disruptions of network communication. 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. 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.
16. Port scanning or security scanning is expressly prohibited unless prior notification is made to the IT Department.
17. 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.
18. Circumventing user authentication or security of any host, network or account.
19. Introducing honeypots, honeynets, or similar technology on the DWIHN network.
20. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
21. 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.
22. Providing information about, or lists of, DWIHN employees to parties outside DWIHN.
23. Unauthorized use of the password or the access credentials of any user.

Email and Communication Activities

When using DWIHN resources to access and use the Internet, users must realize they represent the DWIHN. Whenever employees state affiliation to the DWIHN, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the DWIHN". Questions may be addressed to the IT or the Communications Department.

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 DWIHN's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DWIHN or connected via DWIHN's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

1. Blogging by employees, whether using DWIHN's property and systems or personal computer systems, is also subject to the terms and restrictions outlined in this Policy. Limited and occasional use of DWIHN's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate DWIHN's policy, is not detrimental to DWIHN's best interests, and does not interfere with an employee's regular work duties. Blogging from DWIHN's systems is also subject to monitoring.
2. DWIHN's Confidentiality policy also applies to blogging. As such, Employees are prohibited from revealing any DWIHN confidential or proprietary information, trade secrets or any other material covered by DWIHN's Confidential Information policy when engaged in blogging. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of DWIHN and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by DWIHN's Non-Discrimination and Anti-Harassment policy.
3. Employees may also not attribute personal statements, opinions or beliefs to DWIHN when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of DWIHN. Employees assume any and all risk associated with blogging.
4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, DWIHN's trademarks, logos, and any other DWIHN intellectual property may also not be used in connection with any blogging activity.

QUALITY ASSURANCE/IMPROVEMENT

DWIHN shall review and monitor contractor adherence to this policy as one element in its network management program.

Compliance Measurement

1. The Information Technology Department team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

1. Any exception to the policy must be approved by the Information Technology team and the Compliance Officer team in advance.

Non-Compliance

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

COMPLIANCE WITH ALL APPLICABLE LAWS

In using DWIHN IT Systems, Authority staff, contractors and subcontractors are bound by all applicable local, state and federal laws, rules, regulations and policies, all federal waiver requirements, state and county contractual requirements, policies, and administrative directives, as amended.

LEGAL AUTHORITY

RELATED POLICIES

1. HIPAA Privacy Manual and Policies
2. HIPAA Security Manual and Policies
3. Password Policy
4. Audit Policy
5. Minimum Access Policy
6. Confidentiality Policy

CLINICAL POLICY

No

INTERNAL/EXTERNAL POLICY

External

EXHIBIT(S)

Approval Signatures

Step Description	Approver	Date
Final Approval Policy	Eric Doeh: President and CEO	06/2022
Stakeholder Feedback	Allison Smith: Project Manager, PMP	05/2022