Information Services

Policy Title: Acceptable Use of Wyoming Medical Center Systems

Policy Number: 9360-IS-POL-0045
Effective Date: 01/2015
Replaces: Information Systems Utilization
Review Date: 1/2018

Purpose:
This policy applies to all Wyoming Medical Center employees, contractors, consultants, vendors, agents, and those affiliated with third parties that access Wyoming Medical Center networks and/or computers. It also applies to all equipment that is owned or leased by Wyoming Medical Center. Wyoming Medical Center is committed to protecting its resources from illegal or damaging actions by individuals, either through intentional or unintentional methods. Inappropriate use of company systems exposes Wyoming Medical Center to risks including compromise of network systems and services and/or unauthorized data disclosure. It is the responsibility of every technology user to conduct their activities according to the practices established by this policy and Wyoming Medical Center’s Code of Conduct.

Policy:
All systems, including, but not limited to, computer equipment, software, operating, storage media, electronic mail, internet/intranet browsing, and FTP (hereafter to as the “system”), are the property of Wyoming Medical Center. These systems are to be used for business purposes in serving the interests of the company, our clients, and our customers in the course of normal operations.

A. General Use and Ownership

1. Users should be aware that the data they create on the systems remains the property of Wyoming Medical Center. Users should have no expectation of privacy regarding any information stored on or transmitted over any network or device belonging to Wyoming Medical Center.
2. Wyoming Medical Center reserves the right to examine all information stored in or transmitted by the system. At the direction of Senior Management, Corporate Security, Law Enforcement, or the Office of General Counsel, authorized individuals within Wyoming Medical Center may monitor equipment, systems, communication, information, and network traffic at any time. If necessary, Wyoming Medical Center will disclose information obtained through such auditing to appropriate third parties, including law enforcement authorities.
3. Wyoming Medical Center also reserves the right to audit or review systems on a periodic basis to ensure compliance with this and all other policies.
4. Wyoming Medical Center may prohibit access to and/or may take disciplinary action if it is determined that use of any Wyoming Medical Center resource is inappropriate.
5. Employee use of the system should be in compliance with the Wyoming Medical Center Code of Conduct at all times.
B. Appropriate Use

Wyoming Medical Center’s computer systems and networks are provided for business use only. Occasional, reasonable personal use is allowed but employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or manager. In no event should employees have any expectation of privacy surrounding such personal use. NOTE: Any use perceived to be illegal, harassing, offensive, in violation of other Wyoming Medical Center policies, or any other uses that would reflect adversely on Wyoming Medical Center can be the basis for disciplinary action up to and including termination of employment and/or legal action.

1. Computer Software Installation

It is prohibited for staff members of our healthcare team, patients or vendors to install unsupported software of any nature on computers owned by Wyoming Medical Center without express authorization from the Information Services Department. ALL software must be cleared for use and installed by or in conjunction with the Information Services Department.

2. Illegal Software Distribution

It is strictly prohibited for staff members of our healthcare team to load unlicensed copies of computer software onto ANY computer system owned by Wyoming Medical Center. It is strictly prohibited for staff members of our healthcare team to make copies of Wyoming Medical Center licensed software for personal use. All of the above mentioned activities are illegal and can result in immediate termination.

3. Downloading Software

Downloading of software from external sources such as the Internet or commercial online services without express authorization from the Information Services Department is a violation of this policy. This activity can subject the hospital’s computer systems to unwanted viruses, damaging executable programs, or illegal software. Downloading software is defined as the transfer of ANY computer file(s) from an external computer (not owned by Wyoming Medical Center) to a computer owned by Wyoming Medical Center.
4. Computer System Modification

Modifications to the software configuration, hardware setup, or wiring of any computer system, owned by Wyoming Medical Center not only hampers the delivery of patient care, but can result in wasted resources in terms of cost and effort restoring the computer system to its original state. It is a violation of this policy to tamper with the configuration of any computer system, owned by Wyoming Medical Center without express authorization from the Information Services Department.

5. Internet/Network Access

Use of the Internet is a privilege granted by Wyoming Medical Center to those employees who agree to accept the terms and conditions of this policy. Wyoming Medical Center may withdraw that privilege at any time. The following terms and conditions must be followed by those using Wyoming Medical Center’s connection to the Internet. Wyoming Medical Center has the capability to monitor Internet use.

A) Internet access is granted to all employees, however, Wyoming Medical Center will filter content it feels is inappropriate or not needed for business purposes. Individual employees may be provided unfiltered access upon approval of the head of Information Services or his or her designee when there is a bonafide business need.

B) An employee’s account is their responsibility. Inappropriate use of the Internet can compromise Wyoming Medical Center’s computer systems. Failure to comply with the terms and conditions governing Internet use will result in removal of your access privileges and possible disciplinary action in accordance with Wyoming Medical Center’s Policies and Procedures.

C) Wyoming Medical Center’s Internet access is intended to be a gateway to valuable information to be used toward furthering the hospital’s goals. The Internet will permit you to use computer, databases and automated systems in universities, organizations and government. Internet should be utilized only for hospital purposes.

D) Internet access is a shared resource and as such has it limitations. Employees are expected to keep network resource use at a minimum.

E) Any use which violates laws and/or regulations of the State of Wyoming or the United States is strictly forbidden. Use of this system to deliver threats to others, including sexual harassment, is forbidden. The State of Wyoming and U.S. Government have specific laws dealing with computer crime. These laws include: crimes against intellectual property, crimes against computer equipment and supplies, crimes regarding interruption or impairment of government operations or public
services and crimes against other computer users. Severe penalties exist for violating these laws.

F) Access to the system is a privilege which may be revoked by Wyoming Medical Center at any time for unlawful or abusive conduct. Such conduct would include, but is not limited to, the unlawful use of the system, the use of obscene, abusive language in either a public or, upon registration of a complaint, a private message. Wyoming Medical Center is the sole arbiter in their discretion of what constitutes obscene, abusive, threatening, or objectionable language.

G) An individual may experience material on the Internet that you or others may find offensive. Wyoming Medical Center is responsible only for the content of its internal network. Internal is defined as those systems located on the Wyoming Medical Center side of its Internet connection.

H) This system is provided by Wyoming Medical Center for educational and research purposes only. Other inappropriate use of access include; games or playing games against opponents across the internet, personal commercial activities, any form of sexual explicit media, and downloading distributing pirated software or data. Violations may be subject to disciplinary action up to termination.

I) The Information Services Department reserves the right to inspect any and all data the user has on the system.

J) Individuals will not engage in any conduct or activities on the Internet which could expose Wyoming Medical Center to liability for damages of any kind.

6. Transmission Of Data To And From External Sources
The following rules apply to transmission of data to and from external databases and other sources.
A) All care should be taken to ensure that secure point to point leased phone lines are used when transmitting patient identifiable or other confidential information or data to insurance providers or other healthcare partners.
B) All submissions of data to national data banks shall be in aggregate form, not to include patient identifiable information or other confidential information.
C) Never transfer unencrypted patient identifiable information through Email via the Internet.
D) The following forms of transmission media is accepted at Wyoming Medical Center:
   1) FTP
   2) SFTP
   3) HTTP
   4) HTTPS
5) TELNET
6) SSH
7) Others as required, and approved by the Information Services Manager

C. PROHIBITED USE
The activities listed below are, in general, prohibited; however, employees may be exempted from these restrictions during the course of their 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 Wyoming Medical Center authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Wyoming Medical Center owned resources. The following lists are by no means exhaustive, but attempt to provide a framework of activities that fall into the category of unacceptable use.

1) 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 Wyoming Medical Center.

2) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, and copyrighted music. The installation of any copyrighted software for which Wyoming Medical Center or the end user does not have an active license is strictly prohibited.

3) Unauthorized recording of Wyoming Medical Center data through electronic recording devices such as camera phones, digital cameras, video recorders, etc.

4) Employees must never download software from the Internet. Only authorized Employees are allowed to download and install software that is required for daily business operations. Examples can include, but are not limited to, software patches, security alerts, hardware drivers, etc.

5) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is strictly prohibited.

6) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

7) 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.

8) Using a Wyoming Medical Center computing asset to engage in procuring or transmitting material that is in violation of antidiscrimination, antiharassment, or hostile workplace laws or policies in the user’s local jurisdiction.

9) Making fraudulent offers of products, items, or services originating
10) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

11) 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, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

12) Port scanning or security scanning is expressly prohibited unless prior notification to Information Services is submitted and approval obtained.

13) 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.

14) Circumventing user authentication or security of any host, network, or account. Workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise the system’s security unless specifically authorized in writing by Information Services Security.

15) Employees must not test or attempt to compromise the system’s security measures. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file encryption, bootleg software copying, or similar unauthorized attempts to compromise security measures are considered serious violations of this Policy.

16) 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.

17) Providing information about, or lists of, Wyoming Medical Center employees to parties outside Wyoming Medical Center.

18) Unapproved and/or unlicensed software cannot be loaded on Wyoming Medical Center computers without express permission of the Information Systems Department.

19) Personal equipment cannot be brought internally to Wyoming Medical Center facilities and connected to the Wyoming Medical Center corporate network without express permission of the Information Systems Department. Personal equipment may be used remotely when access is gained through an approved remote access method.
D. Enforcement
Any violation of Wyoming Medical Center’s policies and/or any governmental laws or regulations is cause for disciplinary action up to and including termination of employment, and may result in civil and/or criminal action being taken against the employee. All policies and guidelines referenced in this policy apply to Wyoming Medical Center and all its subsidiaries and affiliates.

E. Exceptions
Where valid business reasons exist, exceptions to the Information Services Security Policy(s) will be considered. Written documentation must be provided to Information Services Systems and Security stating the reason(s) and risks associated with the requested exception(s). Once the documentation is received, Information Services management will make a determination as to whether sufficient mitigating controls are in place. If the exception is approved, the appropriate documentation will be retained by Human Resources and the Information Services Department. Exceptions are to be determined on a case by case basis.

Definitions:

Materials & Equipment: N/A

Procedure / Guidelines: N/A

Reference(s) / Related Policies: N/A

Related Documents: None

Key Reviewer/Owner: Information Services

Stakeholders: Wyoming Medical Center