Policy/Procedure Title: **Acceptable Use Policy**	Hardcopy Manual Location:
Issued (Date): March 3, 2012	
Department (Name of Department): Information Technology	
Department Director: Jeff Cooper / Betty Hite	
Department Vice President: Mike Canfield	

1.0 Purpose

The purpose of this policy is to outline the principles governing the proper and efficient use of the computer equipment and network resources provided by Augusta Health. These rules are in place to protect Augusta Health and its employees from the risks associated with inappropriate use of an organization's information systems. These risks include, but are not limited to, virus attacks, compromise of network systems, illegal activity, privacy violations, and service interruptions. While the appropriate use of software is briefly discussed in this policy, Augusta Health network users should refer to the Augusta Health Software Use Policy for complete details.

2.0 Scope

This policy applies to all workforce members of Augusta Health who have access to a workstation or Augusta Health network service.

3.0 Definitions

3.1. **Workstation:** Includes desktop personal computers, laptops, mobile devices, or any device that is network-enabled.

3.1.1. Network access may include direct wired connection through configured wall- plate connections, VPN (virtual private network) or other remote access, or wireless access through managed wireless access points

3.1.2. Locations include any part of an Augusta Health managed facility or the near vicinity, as well as residential locations for approved remote access.

3.2. **Network:** Enables access to business and clinical applications, Internet, Email, FTP, and Intranet.

3.2.1. **Business and Clinical Application:** All business and clinical related productivity software available and approved for use per the Augusta Health Software Use Policy.

3.2.2. **Internet Services:** Includes all activity related to the Internet such as, but not limited to: browsing, file transfer, streaming audio & video, and remote access.

3.2.3. **Email:** The Microsoft Exchange Email system (Outlook) licensed and operated by Augusta Health for the use of internal and external business and clinical communications.

3.2.4. **FTP:** The internal resource used for the transfer and temporary storage of large digital documents by Augusta Health network users.

3.2.5. **Intranet:** Includes the Augusta Health Web Portal (also known as Pulse)

which provides a shared, web-enabled workspace for internal Augusta Health business and personal use.

3.2.6. **Cloud Storage:** Augusta Health will provide access to Sharefile private cloud storage to facilitate file and document sharing with approved external Business Associates.

4.0 Policy

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments may have additional guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such additional guidelines, and if there is any uncertainty, employees should consult their manager.

4.1. Workstations

4.1.1. All desktop workstations and other devices for use on Augusta Health's corporate network must be pre-approved by organizational management; no personally acquired peripheral devices may be connected to an Augusta Health workstation or the organizational network unless approved by the Director of Technology Services.

4.1.2. No electronic Protected Health Information may be permanently stored on single- user workstations and other devices. All ePHI must be backed up to secure servers at least at the end of the workday or shift and removed from the workstation.

4.1.3. Workstations may be used only for appropriate organizational purposes as determined by organizational management.

4.1.4. Workstations must be used within the protected organizational network to afford the highest protection from external access attempts and malicious software.

4.1.5. Portable devices that contain ePHI must encrypt data at rest.

4.1.6. Remote access to the organizational servers with ePHI must be approved and authorized by appropriate management, and access must be through approved network pathways and technology.

4.1.7. Only software that has been acquired per the Augusta Health Software Use Policy may be installed on workstations.

4.2. Network Services

Data that is created, sent, posted for public view, obtained, or requested via the Internet, an e- mail system, or any system must not contain material that could be considered discriminatory, offensive, obscene, threatening, harassing, or intimidating.

Intentionally interfering with the normal operation of the network including, but not limited to, the spread of computer viruses or the intentional continuous exchange of large volume information that hinders others in their use of the network, is a violation of policy.

4.3. Business and Clinical Applications

All business and clinical applications are to be used in accordance with their

associated license agreements and in compliance with U.S. Copyright law. Employees should refer to the Augusta Health Software Use Policy or their immediate supervisor if they have questions regarding the appropriate use of software acquired by Augusta Health.

All data or information created, accessed, or stored by business and clinical applications are considered to be the property of Augusta Health and subject to review at any time by Augusta Health management.

4.4. Internet Services

Internet access is provided to all users of Augusta Health's network system for the performance of business related activities as well as limited personal use. All access to the Internet is monitored and filtered for content. The following Internet activities have specific restrictions:

- 4.4.1. Access to Internet Webmail services such as Gmail, Outlook.com, Yahoo, ISP provided Webmail, etc. is prohibited.
- 4.4.2. Access to internet file sharing or delivery such as DropBox is prohibited
- 4.4.3. Peer-to-peer activity for the purpose of sharing video, audio or software is prohibited.
- 4.4.4. Online gambling is prohibited.
- 4.4.5. Online dating, singles, or personals are prohibited.
- 4.4.6. Viewing and/or downloading of pornographic content is prohibited.
- 4.4.7. FTP – Restricted to authorized business purposes.
- 4.4.8. Personal Cloud Storage (i.e. Google Docs, OneDrive), is prohibited.
- 4.4.9. Streaming audio/video – Limited primarily to business use, but personal use is permitted when the impact on network capacity is minimal. IT will block the access of streaming content to users whose usage has a negative impact on network performance.
- 4.4.10. Remote Access – Restricted to business use only for employees working from a remote office or their home. Authorization is required prior to connecting to the Augusta Health network from a remote location by a Director or Vice President.
- 4.4.11. Any Internet activity not identified above which is in violation of Federal, State, or local laws and/or ordinances is prohibited.

Business needs that violate these restrictions will be handled on a case by case basis and exceptions may be granted by Organizational management if no suitable options exist.

4.5. E-mail

All email sent from, received by, and subsequently stored on Augusta Health's email system is considered the exclusive property of Augusta Health.

4.5.1. Personal Use

Using a reasonable amount of Augusta Health resources for personal emails is acceptable, but the sending or forwarding of chain letters, SPAM, or messages that solicit orders or trade not related to Augusta Health are prohibited. Virus or other malware warnings and mass mailings from Augusta Health shall be approved by Augusta Health's Chief Information Officer before sending.

4.5.2. **ePHI**

Augusta Health will permit internal email of unencrypted ePHI under limited circumstances where the appropriate safeguards as described below are applied. Augusta Health will utilize encryption in an effort to ensure the confidentiality and integrity of email containing ePHI that is being transmitted to destinations outside of the Augusta Health electronic mail system.

Communicating ePHI via E-mail

4.5.2.1. Email communications containing PHI about Augusta Health patients are automatically encrypted by Augusta Health's ZixCorp encryption gateway before delivery to destinations outside the Augusta Health email system.

4.5.2.2. Users have the ability to force encryption of any email by placing the word *Secure* in the subject line.

4.5.2.3. ePHI that is specially protected (i.e., HIV/AIDS information, substance abuse treatment information, and mental health information) must not be communicated via email.

4.5.2.4. If a document that contains ePHI is included as an attachment to the message, the User should verify before transmitting the email message that it is the correct document.

4.5.2.5. Any User who is unsure as to whether an email message or attachment contains ePHI should contact his/her supervisor or the HIPAA Privacy Officer before initiating the email communication.

4.5.2.6. See the "Secure Transmission of ePHI" policy for additional information

4.5.3. **Prohibited Use.**

The Augusta Health email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Augusta Health employee should report the matter to their supervisor immediately.

4.5.4. The email addresses **<employee>@augustamed.com, @augustahealth.com, @augustacarepartners.com** are owned by Augusta Health and are provided to its employees for their business related and limited personal use. As such, the use of an Augusta Health email address to register for a non-business related service (i.e., eBay, Match.com, Yahoo, HotMail) is strictly prohibited.

4.5.5. Forwarding of Augusta Health email to personal email accounts is prohibited unless authorized by Organizational management.

4.5.6. **Monitoring**

Augusta Health employees shall have no expectation of privacy in anything they send, receive, or store on the company's email system. Augusta Health may monitor messages without prior notice and reserves the right to override individual passwords and access the email system at any time for

valid business purposes such as system maintenance, repair, and security or regulatory investigations. Augusta Health is not obliged to monitor email messages.

4.5.7. **Retention of E-mail**

4.5.7.1. Augusta Health regularly archives email for the purposes of record recovery and regulatory compliance and is retained for a maximum of 6 months.

4.5.7.2. Questions about retention activities should be directed to the Chief Information Officer.

4.6. **FTP**

The FTP service provided by Augusta Health is strictly for business related use. It is to be used as an intermediate transport service for data that is too large to convey via email to Augusta Health's vendors, support providers, and business associates. Personal use is strictly prohibited.

4.7. **Intranet**

MySites - are content areas that each employee can personalize in a format similar to the Internet's MySpace.com. "MySite" provides a central location for Augusta Health employees to view and manage all of their links, calendar, colleagues, and other personal information as well as a way for other users to learn about an employee and their areas of expertise, current projects, and colleague relationships.

The content posted on "My Sites" will be monitored and held to the same guidelines specified in Section 4.2 (Network Services) of this policy. Though the "My Site" will allow employees to maintain their own personal document store, they should refrain from doing so.

5.0 Security and Confidentiality

5.1. Sharing of Augusta Health computer/communications systems user accounts and passwords is not permitted. Each user is personally responsible for any access made through their account.

5.2. Use of systems and/or networks in attempts to gain unauthorized access to systems is prohibited.

5.3. Information about Augusta Health systems access (including firewall systems, operating systems and means of access) is restricted to authorized Augusta Health employees.

5.4. All Augusta Health policies and procedures concerning use of patient/employee information also apply to use of the internet/e-mail. Accessing or revealing by any means, patient, employee, or other information, which a network user is not authorized to access and share is prohibited.

5.5. Unauthorized scanning or probing of any of Augusta Health's internal systems and networks, and/or the use or electronic storage of any unauthorized network "tools" that can be utilized for scanning, probing, or unauthorized access attempts to any system or network is prohibited.

6.0 Enforcement

6.1. All Augusta Health users must be made aware of and educated on policies related to the acceptable use of corporate workstations and network services.

6.2. Violation of Policy - see Section III (Conduct) of the Augusta Health Employee

Handbook.

7.0 Definitions

7.1. **Business Application** – Software related to finances, security, product development, user productivity, etc. (i.e., Microsoft Office, Adobe Acrobat, Trend Anti- Virus, MySites)

7.2. **Clinical Application** – Software and systems related to the admission, diagnosis, care of Augusta Health's patients. (i.e., Meditech, PACS, McKesson)

7.3. **Data at Rest** – A term that is sometimes used to refer to all data in computer storage while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated. Data at rest can be archival or reference files that are changed rarely or never; data at rest can also be data that is subject to regular but not constant change. An example would be ePHI files stored on the hard drive of an employee's notebook computer.

7.4. **E-mail** – A means or system for transmitting written messages electronically (as between terminals linked by telephone lines, cable networks, or wireless relays)

7.5. **Email Address** – The identifier used by email systems to distinguish individual recipients. For the Augusta Health email system uses <user>@augustahealth.com, where user is typically identified by the initial of the first name followed by the last name, i.e., jsmith@augustahealth.com.

7.6. **Electronic Protected Health Information (ePHI) –** All electronic data that identifies an individual and their private health information. This information is protected under federal law via the Health Insurance Portability and Accountability Act (HIPAA).

7.7. **FTP** – File Transport Protocol: A software protocol for exchanging information (files) over a network.

7.8. **Malware** – Malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

7.9. **Organizational Network** – The local and remote workstations, servers, routers, switches, and other data network components that comprise Augusta Health's information systems.

7.10. **Remote Access** – Connecting to Augusta Health's organizational network via the Internet or a point-to-point service (i.e., cable modem, DSL, or cellular data) from a remote location. Internet connections can be made utilizing services such as Citrix client or through a VPN

7.11. **SPAM** - Unauthorized and/or unsolicited electronic mass mailings

7.12. **User Account** – The network login identifier each Augusta Health network user is provided. This is typically different than an employee's email account and consists of the employee's department ID and a period followed by their initials, i.e. NUR.JKM.

8.0 Regulatory Compliance

8.1. HIPAA Rule § 164.310(b) Workstation Use
8.2. HIPAA Rule § 164.310(c) Workstation Security
8.3. HIPAA Rule §164.312(e) Transmitted ePHI

Revision History
Draft 1.0: 14 July 2007
Approved: 14 July 2007

Acceptable Use Policy

Employee, Vendor, Student, Volunteer Acknowledgement

Your signature acknowledges that you have received and read this policy and understand the rules and principles within.

Signature:_____ Date:_____

Print Name (First, MI, Last):_____