Rationale
An Internet Usage Policy is required to maintain a high level of IT Enterprise services and availability to customers and to the IT Enterprise. This policy is essential for Jackson Health System (JHS) to promote its primary goal of being a patient-focused organization by supporting a secure, reliable, robust, and interoperable computing environment.

Internet access is important to each individual at JHS. It is used as an efficient and effecting research and communication tool. Internet connectivity also is vulnerable to information security breaches if used incorrectly. This policy communicates the proper usage of the Internet privilege.

Scope
This policy applies to all personnel, including but not limited to Jackson Health System's staff, agency partners, vendors, and contractors who provide Jackson Health System's services while involved in activities related to providing those services.

Exemptions
Exemptions can be applied if the security protection mechanisms or processes exceed those communicated in this policy. For any other exemptions to this policy, contact the Chief Information Security Officer.

Definitions
The definitions for terminology in this document can be found in the Enterprise Glossary.

Policy Language

Web Surfing
Access to the Internet has become an important part of day to day business at Jackson Health System. Access to business related web sites is permissible for all authorized users. All other non business related Internet access will be controlled and monitored using an HTTP filter. Unless an exception has been authorized, access to sites that are not permissible include the following categories; Hate, Weapons, Games, Adult/Sexually explicit, Violence, Criminal Skills, and gambling. This category list is subject to change without notice, at the discretion of Jackson Health System's management.

Information Protection
Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, Jackson Health System's Protected Health Information must not be sent over the Internet unless it has first been encrypted by approved methods.

Credit card numbers, telephone calling card numbers, log-in passwords, and other parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form.

In keeping with the confidentiality agreements signed by all workers, Jackson Health System's software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Jackson Health System's ' party for any purposes other than business purposes expressly authorized by management. Exchanges of software and/or data between Jackson Health System and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected. Regular business practices--such as shipment of software in response to a customer purchase order--need not involve such a specific agreement since the terms are implied.

Expectation of Privacy
Personnel using Jackson Health System's information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers should not send information over the Internet if they consider it to be private.

At any time and without prior notice, Jackson Health System's management reserves the right to examine e-mail, personal file directories, and other information stored on Jackson Health System's computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Jackson Health System's information systems.

Public Representations

Safeguarding Our Corporate Image on the Internet
As a public entity, Jackson Health System works diligently to ensure that official communications to customers, providers and the general public are accurate and professional. What is produced and distributed directly impacts how the organization is perceived, whether it be a publication, a brochure or a letter. To this end, JHS has established certain guidelines and a strictly enforced approval process.

The same high standards must be applied to any Internet activity
Millions of people "surf" the Internet on a daily basis and Jackson Health System must take great pains to ensure that anything with a Jackson Health System address reflects well upon the organization.

All official Jackson Health System Internet communications must be approved by Authorized Personnel before being uploaded or distributed. This includes, but not limited to, web sites/home pages, "mass" e-mail messages to customers, providers, group leaders or other public, etc. This also includes any information provided to other web sites (i.e. provider listings, benefit information). The rule of thumb is that if you want to send something out for mass distribution via the Internet in your official capacity as a Jackson Health System employee, it must be approved first.

While JHS does not wish to infringe on private e-mail messages, remember that anything that is sent out from work will have a Jackson Health System's "address" and will reflect on JHS. No expectation of privacy can be assumed.

Internet Media Guidelines
The news media serves as an important information link between Jackson Health System and our members, as well as the general public. It is important for the organization to project a positive image in the media. In many cases, positive news media coverage has more impact on the opinions of the public than does advertising or publicity.

It is also important for the information disseminated by Jackson Health System to be accurate and consistent. To accomplish this, our Corporate Operating Guidelines contain a Media Relations Policy. This policy is now expanded to include Internet communications.

Contacting the news media via the Internet is strictly prohibited. Likewise, if you receive an Internet communication from a reporter, it should be referred immediately to the Corporate Communications Public Relations Department.

Access Control
All users wishing to establish a connection with Jackson Health System's computers via the Internet must authenticate themselves at an authentication server before gaining access to Jackson Health System's internal network. This authentication process must be done via a dynamic password system approved by the authorized personnel. Examples are hand-held smart cards or user-transparent challenge/response. This will prevent intruders from guessing passwords or from replaying a password captured via a

"sniffer attack" (wiretap). Designated "public" systems do not need these authentication processes because anonymous interactions are expected.

Workers may not establish Internet or other external network connections that could allow non-Jackson Health System's users to gain access to Jackson Health System's systems and information. These connections include the establishment of multi-computer file systems, Internet home pages, FTP servers, and the like.

Likewise, unless authorized personnel have approved in advance, users are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc.

Reporting Security Problems

If sensitive Jackson Health System information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Chief Privacy Officer or Chief Information Security Officer must be notified immediately. If any unauthorized use of Jackson Health System's information systems has taken place, or is suspected of taking place, the Chief Information Security Officer must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Office of the Chief Information Security Officer must be notified immediately. Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not "test the doors" (probe) security mechanisms at either Jackson Health System or other Internet sites unless they have first obtained permission from the office of the Chief Information Security Officer. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

Jackson Health System will assure Internet Usage mechanisms are in place and effective by assuring these processes are conducted:

- Perform regular quality assurance checks of applications & systems to assure the Internet Usage mechanisms are effective at least once per year.
- Produce reports, both regular and ad hoc, to fulfill associated processes and management's needs.

Jackson Health System's Internet Usage processes, procedures and standards:

- Gather pertinent data that will benefit the Health Systems collection of configuration and asset information.
- Support all the other service management processes (e.g., Change Management, Incident Management, and Problem Management).
- Are flexible enough to respond to the customer's business needs.
- Minimize effort to maintain data through automation, consolidation and sharing of data sources.
- Are readily accessible and available to Jackson Health System's customers and staff.
- Are written to be understandable to its audience.
- Are regularly updated based on customer feedback, new business needs and changing practices to ensure continual quality improvement and those changes communicated to Jackson Health System's customers and staff.

Human Resource Implications

In order to provide an exemplary standard of Internet Usage, Jackson Health System's management must:

- Offer initial and continuing training to Jackson Health System's staff in Internet Usage policy, processes, procedures and standards.
- Ensure documentation for Internet Usage policy, processes, and procedures documentation is accessible to all staff.
- Ensure all Jackson Health System's staff consistently follow the Internet Usage policy, processes, procedures, and standards.
- Assist staff to understand Internet Usage policy, processes, procedures, and standards, and enforce compliance with the policy, processes, procedures, and standards.

Related Policies, Processes, Procedures, Standards, or Best Practices

- Jackson Health System's Acceptable Use
- Jackson Health System's Asset & Classification
- Jackson Health System's Asset Protection
- Jackson Health System's Configuration/Asset Management
- Jackson Health System's Incident Management
- Jackson Health System's Information Security Staff
- Jackson Health System's Threat Assessment & Monitoring
- Jackson Health System's Vulnerability Assessment & Risk Management

Timeline

Effective Date: Effective upon implementation.

Review Date: Within one year from the effective date.

Authorization:

Marvin O'Quinn, President, Public Health Trust