INTERNET SECURITY

SCOPE:

All West Virginia University Health System (WVUHS) Entities*

CITATION

§ 164.312 — Technical Security Mechanisms
§ 164.312 — Information Access and Control

POLICY

This policy applies to all users, employees, contractors, consultants, temporaries, and volunteers, who use the Internet with West Virginia University Health System (WVUHS) computing or networking resources. All Internet users are expected to be familiar with and fully comply with this policy. Questions about the policy should be directed to the WVUHS Chief Information Security Officer. Violations of this policy can lead to revocation of system privileges or additional disciplinary action in accordance with the WVUHS Corrective Action Policy V. 230S.

Access to the Internet will be provided to only those users whose management has requested such access. These requests are handled via the WVUHS Information Technology Identity Management and Role Base Access Request Process.

The wide array of new resources, services, and inter-connectivity available through the Internet all introduce new business opportunities, and new security and privacy risks. In response to the risks, this policy describes the WVUHS official policy regarding Internet security.

PROCEDURE

Information Integrity

Software Downloading: As the Computer Use Policy VIII.211S states, users shall not install Internet downloaded software on their WVUHS-supplied computers without prior approval from a WVUHS Information Technology CIO, AVP, Director or Manager.

Automatic updating of software on WVUHS computers through background push Internet technology is prohibited unless the involved vendor's system has been tested and approved by the WVUHS Chief Technology Officer or designee.

* West Virginia University Health System adopts this policy and procedure for WVU Hospitals, Inc.; Summersville Regional Medical Center; WVUHS Home Care, LLC; WVUHS Medical Group; Reynolds Memorial Hospital; Berkeley Medical Center; Jefferson Medical Center; Potomac Valley Hospital of W.Va., Inc.; United Summit Center; United Hospital Center, Inc.; Wheeling Hospital, Inc.; Barnesville Hospital Association; Harrison Community Hospital, Inc.; United Physician's Care, Inc.; St. Joseph's Hospital of Buckhannon, Inc.; Camden-Clark Memorial Hospital Corporation; Camden-Clark Physician Corporation; Braxton County Memorial Hospital, Inc.; Jackson General Hospital; Wetzel County Hospital; Uniontown Hospital; Allied Health Services, Inc.; West Virginia United Insurance Services, Inc.; Accountable Care Organization of West Virginia, LLC(ACO); AHS, LLC; Gateway Home Health Care, LLC; Peak Health Holdings, LLC; Garrett Regional Medical Center; Princeton Community Hospital Association, Inc.; Grant Memorial Hospital, Inc.; and Thomas Health System, Inc.

User Anonymity—Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any WVUHS electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

Electronic Mail Attachments—Users must not open electronic mail attachments unless they were expected from a trusted sender. Users must comply with the E-mail, Instant Messaging, Collaboration Usage Policy VIII.230S.

Web Page Changes—Users shall not establish new Internet pages dealing with WVUHS business, or make modifications to existing web pages dealing with WVUHS business, unless they have obtained the approval of the VP Marketing and Communications. This encompasses all forms of social media, creating unapproved chat groups, interest groups or other pages meant to represent any facet of the business for WVUHS. Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page. The VP Marketing, and Communications or designate must ensure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected with adequate security measures. Users should also reference Social Networking Policy VIII.206S.

Copyrights—While at work, or when WVUHS computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Participation in pirate software bulletin boards and similar activities represent a conflict of interest with WVUHS work, and are therefore prohibited. The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author or owner. Users must assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" and specifics about the source of the information.

Information Confidentiality

Information Exchange—WVUHS software, documentation, protected health information (PHI), business asset data, and all other types of internal information must not be sold or otherwise transferred to any non-WVUHS party for any purposes other than business purposes expressly authorized by management. Exchanges of PHI between WVUHS and any third party must not proceed unless a written Business Associate agreement has been signed. Such an agreement must specify the terms of the exchange, and the ways that the PHI is to be handled and protected.

Disclosing/Posting Materials—Users shall not disclose/post WVUHS PHI or business asset data on any publicly-accessible Internet system, including but not limited to, CHAT-GPT, Signal, WhatsApp and Conversational AI (this is not an exhaustive list), unless the posting of these materials has been approved by the WVUHS Enterprise Information Management Privacy Director, WVUHS Chief Information Security Officer, and VP Marketing, and Communications. WVUHS internal information must not be placed in any computer unless the persons who have access to that computer have a legitimate business need to know the involved information.

Personal Online Internet Storage – Users must not store, copy or transmit WVUHS protected health information (PHI), business asset data, secret, proprietary, or private information to a personal online storage application or any other electronic system that is not explicitly approved for storage of such information by the WVUHS Chief Technology Officer. This includes, but is not limited to, cloud based applications such as iCloud, Dropbox, MyDrive, Google Docs, etc. In order for WVUHS to protect patient information,

specific agreements must be in place with such third party vendors as to ensure the confidentiality, integrity and availability of this highly sensitive information.

Inadvertent Disclosure—Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Blogs, chat rooms, and related public postings on the Internet. Before posting any material, users must consider whether the posting could put WVUHS at a significant competitive disadvantage or whether the material could cause public relations problems. Users should keep in mind that several separate pieces of information could be pieced together by a competitor to form a picture revealing confidential information and then could be used against WVUHS. Users must never disclose/post on the Internet the specific computer or network products employed by WVUHS.

Message Interception—Protected health information (PHI), business asset data, secret, proprietary, or private information must not be sent over the Internet unless it has been encrypted by approved methods. This also includes telephone calling card numbers, payroll information, passwords, and other security parameters. Credit card information must never be stored in databases, shared folders or emailed to ensure WVUHS complies with the Payment Card Industry (PCI) standards. Reference the WVUHS E-Mail, Instant Messaging, Collaboration Usage Policy VIII.230S.

Internet Access Control

Inbound Connections—All inbound connections should comply with the Remote Access Policy VIII.225S.

Establishing Internet/Network Connections—Unless the prior approval of the WVUHS Chief Information Security Officer or WVUHS Chief Technology Officer has been obtained, users must not establish Internet or other external network connections that could permit non-WVUHS users to gain access to WVUHS systems and information. These connections include, but are not limited to, the establishment of separate Internet Service Provider connections, Telecommunication lines, multi-computer file systems, Internet pages, Internet commerce systems, and FTP servers.

With the exception of telecommuters and mobile computer users, users must not employ Internet Service Provider (ISP) accounts and dial-up lines to access the Internet with WVUHS computers while connected to the WVUHS network. All Internet activity must pass through WVUHS firewalls and filters so that access controls and related security mechanisms can be applied.

Personal Use—Users who have been granted Internet access, shall also comply with the Computer Use Policy VIII.211S and Security Standards for Mobile and Other Portable Devices Policy VIII.215S.

Offensive Web Sites—WVUHS is not responsible for the content that users may encounter when they use the Internet. When and if users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session. Users using WVUHS computers who discover they have connected with a web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site and contact the WVUHS IT Help Desk to request that the site be blocked.

Forbidden and Blocked Sites—The ability to connect with a specific web site does not in itself imply that users of WVUHS systems are permitted to visit that site. WVUHS may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include images and music files; more specifically, users may not access streaming video files, i.e., video clips of news, sports, movie trailers, etc., music stations, stock tickers, games or any activity that results in a continual

flow of information via the Internet to the user's PC. WVUHS employees are permitted to view work-related webcasts.

Privacy Expectations

No Default Protection—Users using WVUHS information systems or the Internet must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, users shall not send PHI or other business asset information over the Internet.

Management Review—At any time and without prior notice, WVUHS management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through WVUHS computers.

Auditing —WVUHS logs the web sites visited, time spent on the Internet, and related information. Department directors or managers may request reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities. Management determining inappropriate activities should initiate disciplinary action in accordance with WVUHS Corrective Action Policy V.230S.

Reporting Security Problems

Notification Process—If sensitive WVUHS information is lost, disclosed to unauthorized parties, or suspected of either, users must report the security incident following the Information Technology Security Procedures and Response Policy – VIII.201S. If there is a suspected breach of Protected Health Information (PHI) then users must report the breach as outlined in Breach of Patient Confidentiality Policy of the WVUHS hospital(s) involved. If any unauthorized use of WVUHS information systems has or is suspected of taking place, the WVUHS Chief Information Security Officer must be notified immediately. All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages must be immediately reported to the WVUHS IT Help Desk. The specifics of security problems must not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports—Users in receipt of information about system vulnerabilities must forward it to the WVUHS Chief Information Security Officer, who then will determine what if any action is appropriate. Users must not personally redistribute system vulnerability information to other users.

Author: WVUHS Chief Information Security Officer