UNM HEALTH SCIENCES CENTER

How IT Security Tools Protect You and the Institution

Why do we need information security at the HSC? Information security supports and enables the HSC's missions, in keeping with the institution's values regarding risk to our data and systems. Security awareness and good security practices along with technical tools can help to ensure public trust and confidence in the security of our information systems. The HSC's IT security program is defined by policies, security strategies and a work plan that includes the tools listed below.

What actions are we taking for your benefit?

Spam filtering of incoming email: All in-bound mail at UNM is filtered by reputation and content type to reduce the number of spam and malicious messages users receive, many of which contain malware and links to other internet exploits. As an example, in April 2011 spam accounted for 85% of all in-bound e-mail traffic to UNM.

Centralized anti-virus and operating system patches: Over 4,500 HSC computer systems are protected by centrally-managed operating system patch management and distribution as well as continually-updated enterprise anti-virus solutions.

Blocking risky web sites: Web based attacks are responsible for the vast majority of system compromises at the HSC. Web security software installed at the HSC network perimeter blocks an average of 12 million web sessions per month, both risky sites and legitimate sites that unknowingly host bad data, screening by reputation and content type.

NEW! Opt-in encrypted email *secure*: HSC GroupWise users benefit from a comprehensive array of security features and policies to ensure the safety and confidentiality of their email. GroupWise keeps all internal communication fully encrypted and will soon have the capability to optionally protect email sent via the open Internet to colleagues, patients and business partners outside of the HSC.

COMING SOON! Full disk encryption: According to Gartner, one laptop is stolen every 53 seconds, and lost and stolen laptops and mobile devices continue to be the most frequent cause of a data breach in the US[1]. UNMH and the UNM Medical Group already require laptop encryption. Beginning this fall, HSC computer users may have the hard drives of their Windows® laptops or other high-risk devices encrypted using a centrally managed system so data is not accessible in the event the device is lost or stolen.

COMING SOON! Routine monitoring to build public trust and confidence: In order to ensure the appropriate use of the HSC network (a shared resource designed to meet the HSC's business obligations), traffic is monitored by automated means to a degree necessary to ensure the security of HSC information assets. Soon this will be enhanced to include email transmissions to recipients outside the HSC. Improper use may result in an automated action designed to protect health information (PHI) that is not secured, as required by federal law. Automated actions may include but are not limited to: returning a message to the sender, encrypting a message before transmission to the destination, or blocking network access.

ENDORSED BY THE HEALTH SCIENCES LIBRARY AND INFORMATICS CENTER, THE UNM CANCER CENTER, THE UNM MEDICAL GROUP, AND THE UNMH IT DEPARTMENT

The UNM Health Sciences Center must maintain and protect its institutional information assets, comply with applicable federal (HIPAA, FERPA, etc.) and state legislation, and maintain good security practices as a matter of public trust and confidence. – *Policy HSC-210 Security of HSC Electronic Information*

[1] http://www.dell.com/content/topics/global.aspx/services/prosupport/get_connected?c=us&l=en&s=gen