Applies To: HSC Component(s): All Responsible Department: HSLIC TECHS

Title: Web Development Policy					**Policy**
Patient Age Group:	(X) N/A	( ) All Ages	( ) Newborns	( ) Pediatric	( ) Adult

POLICY STATEMENT

To promote the development of web sites, applications and other online services that provide our customers with quality information and resources, it is the policy of the Health Sciences Center (HSC) that employees acknowledge the procedures, guidelines and standards referenced in this document. Information within an HSC web site must be current, accurate and relevant in view of the site's intended audience and conform to UNM copyright guidelines. The presentation of information should consistently reflect the use of approved standards. Systems supporting HSC web sites will conform to security and contingency best practices defined in HSC information systems security and business continuity policies.

APPLICABILITY

This policy applies to the UNM and UNM Hospital workforce authorized to develop web sites for any part of the UNM Health Sciences Center.

POLICY AUTHORITY

This policy is an HSC policy. The KMIT Leadership is the authorizing group. This document was developed and reviewed by the KMIT Operations Council. The KMIT Operations Council should be contacted for revisions.

REFERENCES

- UNM Acceptable Computer Use Policy (2500)
- UNM Computer User Guidelines (2510)
- UNM Hospitals Information Security Policy
- UNM Hospitals Internet Security Policy
- UNM Hospitals Information Ethics Agreement
- HSC Web site Standards
- HSC Electronic Communications Policy
- UNM Data Classification Standard
- HSC Information Technology Security Policies

ROLES and RESPONSIBILITIES

1. **Web Administrator**: The individual that coordinates the development, application and enforcement of HSC web site policies, procedures and standards. He/she ensures an active, vibrant community of Site Managers, Web Authors and Content Owners.

2. **Site Manager**: An individual who manages the overall operation of one of the officially recognized consolidated web sites (e.g. hsc.unm.edu, hospitals.umn.edu). Responsibilities include posting content and maintaining applications, running reports, monitoring statistics, reporting security incidents, working with content owners to develop/maintain content

currency and relevance, and coordinating site development with the Web Administrator. A Site Manager's responsibilities must be a recognized by their supervisor as part of their ongoing duties and responsibilities. (Note: In some instance the roles described in 2. 3., and 4. are not necessarily filled by three separate individuals; there may be some overlap on duties.)

3. **Web Author**: An individual who is primarily focused on working with Content Owners to maintain the currency and relevance of and updates a web site accordingly. While a Web Author may be more involved in site development, it is an adjunct responsibility and not necessarily in their job description.

4. **Content Owner**: The individual responsible for the accuracy, relevance and timeliness of the information presented on a page. In the case of web based applications, the content owner is also responsible for any data accessed buy the application.

5. **Design:** The Health Sciences Center participates in discussions and decision making about web site design and templates. The HSC Web Advisory Committee and HSC Communication and Marketing both have input into the design process. Final web site design is produced by University Communication and Marketing.

6. **Web Development Teams**: The HSLIC and UNM Hospitals have teams of programmers, designers and managers who provide centralized web development and management services for Health Sciences Center schools and departments and UNM Hospitals.

7. **HSC Web Advisory Committee**: The committee is comprised of the Web Administrator, Web Designer, Site Managers and high-level institutional representatives as appropriate. The committee's primary focus is to regularly review and approve HSC website design and navigation changes.

8. **Security Officers**: The HSC Security Officer and UNM Hospitals Security Office have the authority to advise on actions required to protect the integrity of any information on an HSC website deemed vulnerable to inappropriate access

IMPLEMENTATION PROCEDURES

1. **Establishing a Public Web Site**

1.1 A web site is considered a public web site if its content and services are aimed at the general public and all information on the site meets the criteria of the P classification defined in the UNM Data Classification Standard. Public web sites do not require authentication.

1.2 New web authors must take the HSC Web Author Class before they will be given access to the web server to work on their site. See HSC Web Author Classes in the Resources/Training section below for more information.

1.3 Systems supporting departmental and project sites will be maintained by HSLIC or UNM Hospitals IT staff in accordance with HSC standards for security and service continuity.

1.5 Virtual hosts – i.e. unique domain names such as nursing.unm.edu – are supported at the HSC component level: HSLIC, School of Medicine, College of Nursing, College of Pharmacy, UNM Hospitals, UNM Cancer Research and Treatment Center, UNM Medical Group and Sandoval Regional Medical Center. Virtual hosts are also supported for the School of Medicine academic departments. Other HSC entities desiring a virtual host for their web sites need to present their request to KMIT Ops for review and a decision.

1.6 Content Owners, Web Authors and Site Managers will adhere to UNM copyright policy and other responsibilities described in the UNM Acceptable Computer Use Policy (2500).

2. **Establishing an Extranet**

2.1 Extranets contain information that meets the definition of the C and E classification in the UNM Data Classification Standard and therefore need to meet the security standards for C and E class data. Extranets are aimed primarily at external customers who are not employees of UNM or UNM Hospitals. Extranet customers only have access to their own information. Examples of extranet services include: 1) a process whereby potential students can apply online for admissions to a program at UNM, or, 2) a process that allows a patient to look up their own medical information from UNM Hospitals.

2.2 Persons requesting an Extranet will consult with the appropriate Web Site Administrator and the Security Officer to determine if: 1) account creation and management processes meet current HSC security practices, and, 2) other security measures meet with current HSC security practices.

2.3 Persons establishing an HSC extranet must follow the current standards for establishing a UNM Hospitals or HSC security plan.

3. **Intranet Sites**

3.1 An Intranet Site is required if the content and services of the site meet the criteria of the C or E classification defined in the UNM Data Classification Standard. Intranet sites are generally developed for use by employees. Intranet sites require some type of restricted access.

3.2 If it has been determined that an intranet site is needed, the web author and sponsoring department will work with the Web Administrator (or Site Manager) to determine the appropriate location for the site. Intranet sites should be hosted on servers intended for restricted access.

3.3 The Site Manager or Web Administrator will consult with the HSC Security Officer if an aspect of a an site falls outside the current normal restriction measures supported by the HSC.

3.4 Persons establishing an HSC intranet must follow the current standards for establishing a UNM Hospitals or HSC security plan.

4. **Required Design Elements**

4.1 All HSC websites will adhere to the following standards:

1) The web page templates used will be approved by University Communication and Marketing and HSC Communication and Marketing. The templates will include header, footer, page layouts, fonts, colors and all other aspects of the pages' design and layout.
2) All text, photographs and images on web pages will be used in compliance with copyright law.

3) In the case of a web site that is a joint effort between the UNM HSC and an outside entity and the site is hosted on an HSC server, the site will use an approved HSC navigation bar and standard HSC templates. Logos or other branding graphics from the outside entity or entities can be used on the site, in the main body of one of pages.

4) Any exceptions to these requirements will be discussed with the HSC CIO or the UNM Hospitals CIO, depending on organizational affiliation, and, if necessary, HSC Communications and Marketing.

5. **Updating Design Elements**

7.1 Individual Web Authors, Site Managers and other interested members of the HSC community may provide feedback to the HSC Web Administrator.

7.2 Comments and recommendations will be considered by the HSC Web Advisory Committee.

7.3 The HSC Web Advisory Committee will recommend changes to University Communication and Marketing and HSC Communication and Marketing.

6. **Updating HSC Splash Page**

6.1 The Web Administrator will review the HSC Splash Page at the beginning of each fiscal year or when organizational changes warrant.

6.2 If a redesign or update is deemed necessary, a project plan will be generated with an associated timeline.

6.3 The Web Administrator and Sr. Web Designer will present a proof of concept for the redesign to the KMIT Advisory Council for approval, and finally to the KMIT Leadership and the Executive Vice President for Health Sciences for authorization.

6.4 Minor redesigns can be commissioned or directly approved by the Executive Vice President's Office.

7. **Updating Approved Templates**

7.1 Changes to the approved web templates and top-level navigation will be made in conjunction with UNM Communication and Marketing and HSC Communication and Marketing. Input from HSC Site Administrators and Web Authors will be taken into consideration along with input from other web site developers from around UNM.

8. Establishing and Maintaining an FTP Site

8.1 FTP sites are subject to the same HSC and UNM Hospital security policies and procedures as public web sites, extranets and intranets.

8.2 Only HSLIC TECHS or UNM Hospitals and designated members of their workforce should establish and manage FTP sites.

8.3 Improperly managed FTP sites are a security risk. Anyone managing a FTP site must follow HSC and UNM Hospital security policies. Only authorized members of the HSC workforce are allowed to manage FTP sites and to transfer files to the FTP site. There will be no anonymous write access to FTP sites. FTP sites will provide audit trails that show who has written files to a FTP site.

8.4 Anonymous read-only access is appropriate only if the files accessible anonymously are appropriate for use by the general public. All files made available via anonymous FTP access must meet the criteria of the P classification defined in the UNM Data Classification Standard. It is the responsibility of FTP site managers to understand the UNM Data Classification Standard.

8.5 HSCNetID and password will be required for read access to any files that do not meet the P classification as defined in the UNM Data Classification Standard.

8.6 Data that meets the criteria for E classification must not be housed on a standard FTP server. HSLIC maintains an Enhanced File Transfer server which can be utilized to transfer data that must be encrypted under the UNM Data Classification Standard.

19. **Updating Web Development Policy**

9.1 The Web Administrator and KMIT Operations Council will review this Web Policy at least annually and whenever organizational changes warrant.

9.2 If an update is deemed necessary, the Web Administrator will draft an updated policy for review by the KMIT Operations Council.

9.3 The final draft will be presented to the KMIT Advisory Council for approval and then forwarded to the Leadership Council for final approval.

9.4 The UNM Health Sciences Center recognizes the need for the web policy to accommodate the changing needs of the different HSC components. If an HSC department or component believes a change in the web policy is needed, they may contact the HSC Web Site Administrator, who will present the desired change to KMIT Ops. KMIT Ops will make the final decision on whether a change to the policy is needed.

KEY DOCUMENTATION:

1. HSC Web site Standards which include:
   - Visual graphical standard
   - Navigation standard
   - Logo or branding standard
   - Security standard
   - Copyright standard (use of copyright logo)
   - Search engine standard
   - Templates standard
   - Content standard (currency, accuracy, appropriateness, relevance)

2. UNM Hospitals and HSLIC business continuity and information systems security plans (*Reference* detailed procedures that are recommended in order to carry out the intent of the policy.)

DEFINITIONS and DESIRED OUTCOMES

1. **Definitions**

1.1 **HSC web site**: The HSC web site is the set of web accessible documents and applications that are managed by staff dedicated to the development of the HSC's centralized web services. It includes any web site that supports a bi-directional link to http://hsc.unm.edu and contains official information about an HSC organizational unit.

1.2 **HSC splash page**: The entry point for the HSC web site – currently http://hsc.unm.edu.

1.3 **Public Site**: A site that is geared toward the general public. Public sites do not require authentication. These sites should provide information and services useful to our many

audiences: potential students, potential patients, and potential employees. Public sites must neither house sensitive nor provide online access to protected information. Public sites include any type of web resource that is based on the internet protocol suite. This includes HTML page, applications, blogs, wikis, discussion forums and portals.

1.4 Extranet: An extranet is a private network that uses Internet protocols and network connectivity to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses. Examples of extranet services currently in use at the HSC are the SOM Online Admissions Application, Combined BA/MD Admissions and BSGP Online Admissions (in development in 2009).

1.5 **Intranet**: A resources intended for HSC employees. Intranets can have their own navigation, access controls and development procedures, but must continue to comply with other policy statements within this document. Intranets often provide access to information and services meeting the criteria of the C or E classifications defined in the UNM Data Classification Standard. Intranets need to meet all security standards defined by the HSC Security Officer.

1.6 **Navigation**: A recurring set of links that allows visitors to move easily to specific areas of a site.

1.7 **Web application**: Client or server-side data processing programming that is run/executed from a web site. Almost all web applications have two main modules: the administrative module and the display module. All administrative modules must adhere to the security measures outlined in 1.7 above. The display module of some applications handles public information and is not subject to security concerns. Most display modules handle information that is not intend for the public and are therefore subject to security measure outlined in 1.7 above.

1.7 **Design standards**: Definitions of how to use design elements that are common to webs within the HSC and UNM web sites.

1.8 **Virtual host**: A web site registered in the Domain Name System (DNS) as a host that is logically distinct from the primary web site on a given system, e.g. myweb.unm.edu on the system that supports hsc.unm.edu .

1.9 **Public Site**: A site that is geared toward the general public. Public sites do not require authentication. These sites should provide information and services useful to our many audiences: potential students, potential patients, and potential employees. Public sites must neither house sensitive nor provide online access to protected information. Public sites include any type of web resource that is based on the internet protocol suite. This includes HTML page, applications, blogs, wikis, discussion forums and portals.

1.10 **Protected information**: Data that is intended only for specific internal use and should not be seen by the general public. This includes: ePHI, employee information

(other than name, title, duties, office phone and work email address) and payroll information. Protected information will be accessible only via secure sites. Protected information can have many forms: the content on a web page, data from a database or other documents accessible from the web server.

1.11 **FTP Site:** File Transfer Protocol (FTP) is a standard part internet protocol used for transferring files from one computer to another. Reading files via FTP can be anonymous (i.e. no authentication required) or non-anonymous (i.e. authentication required). FTP sites are generally used when there is a need for a way to provide customers with a way download files for their own use.

1.12 **EFT Site**: Enhanced File Transfer (EFT) is a proprietary, encrypted file transfer protocol used for transferring files from one computer to another securely. Reading files via EFT requires authentication and requires an encrypted connection to the server.

2. **Outcomes**

2.1 Consistently high service to online customers.

2.2 Consistent branding

2.3 Consistent navigation

2.4 Consistent high quality presentation

2.5 Improved currency and relevance of information

2.6 Clear procedure of how to post and link information

2.7 Clear accountability

2.8 Consistent implementation of security standards

SUMMARY OF CHANGES

- HSC adherence to UNM web templates standards and the role of University Communications and Marketing and HSC Communications and Marketing in defining the UNM web templates.
- Increased emphasis on how this policy promotes customer service.
- Discussion of web sites and services hosted outside of the UNM network.
- Discussion of extranets as a key part of online customer service.
- Inclusion of the UNM Data Classification Standard as a guide in making decisions about types of access required for different users.
- Virtual hosting is allowed for the entities defined in section 1.6

- Deletion of some whole sections that were too procedural in nature to be in a high-level policy.

KEY WORDS (For the Search Index. Separate words with a comma.)
Web, web sites, web applications, web security, HSC security standards, extranet, HIPPA, protected information.

RESOURCES/TRAINING

Resource/Dept	Internet/Link
Kevin Wiley, Manager Systems and Programming	kwiley@salud.unm.edu
HSC Web Author Site	http://hsc.unm.edu/webdev/webauthors/
HSC Web Author Classes	Learning Central

DOCUMENT APPROVAL & TRACKING

Item	Contact	Date	Approval
Owner	Kevin Wiley, Manager, Systems & Programming, Web Administrator, Health Sciences Library and Informatics Center		
Committee(s)	KMIT Operations Council, KMIT Advisory Council, IS Directors, KMIT Leadership Council		Y
Legal (Required)	Jeffrey Gilmore, Associate HSC Counsel		Y
Official Approver	Paul Roth, MD, Executive Vice President for Health Sciences		
Official Signature		[Day/Mo/Year]	
Effective Date		[Day/Mo/Year]	
Origination Date		08/2003	
Issue Date		02/2011	