WEB
Policies and Standards

Authored by
DHTS Web Services,
Marketing and Creative Services
Executive Summary

Purpose
This document serves to centralize policies, standards and best practices that affect the web sites and web-based applications of Duke Medicine in terms of development, design, security, hosting and content management.

Intended Audiences
This document is intended for application and web site owners, content editors, users and web service providers. It covers both internal- and external-facing applications and sites, and applies to both internal and external providers of web services.

Web Security Policies
All web sites and web-based applications must adhere to federal security and privacy laws, as well as Duke Medicine’s Information Security Standards regarding protected health information and sensitive electronic information, encryption, authentication, and authorization.

Web Site Standards
Standards apply to web registration, domain names, branding, and hosting. For developers, guidelines are also provided for content display, meta data, RSS syndication, navigation, ADA compliance, and server configuration.

Web Site Content Policies
Web-published content must adhere to federal laws governing copyright, intellectual property, libel and privacy, as well as Duke University and Duke Medicine rules and regulations pertaining to text, photos, images, video, Flash and multimedia content.

Web Application Policies
To prevent malicious attacks via web applications, scripts must be validated on the server side and user input data sanitized before passing it to a database system. Best practices for application functionality and for server administration help minimize vulnerabilities, as does technical standardization of processes and tools.

Vendor Policies
External web service providers must be approved to do business with Duke Medicine by the Web Steering Committee and sign a Business Associate Agreement that outlines the terms of the relationship. Special requirements affect any Duke employee functioning as a fee-based vendor outside of her regular job.

Web Governance
The Web Steering Committee approves development and launch of new sites to ensure adherence to the policies and standards herein.
# Table of Contents

1. **Introduction** .......................................................................................................................... 4
   1.1 Scope ......................................................................................................................................... 4
   1.2 Benefits ...................................................................................................................................... 4
   1.2.1 User Experience .................................................................................................................. 4
   1.2.2 Information .......................................................................................................................... 4
2. **Web Security** ........................................................................................................................ 5
   2.1 General Guidelines ................................................................................................................ 5
   2.2 Information Security ............................................................................................................... 5
   2.2.1 Protected Health Information ......................................................................................... 6
   2.2.2 Social Security Numbers ................................................................................................. 6
   2.2.3 Confidential Information ................................................................................................. 6
   2.2.4 Privacy .................................................................................................................................. 6
   2.3 Access ....................................................................................................................................... 6
   2.3.1 Authentication/Login ........................................................................................................ 6
   2.3.2 Authorization ..................................................................................................................... 7
3. **Web Sites** ............................................................................................................................. 7
   3.1 Web site registration .............................................................................................................. 7
   3.2 Domain Naming ..................................................................................................................... 7
   3.3 Branding .................................................................................................................................... 7
   3.4 Development .......................................................................................................................... 8
   3.4.1 General Guidelines ........................................................................................................... 8
   3.4.2 Display ................................................................................................................................ 8
   3.4.3 Generating Unique Titles ................................................................................................. 9
   3.4.4 DOCTYPE Declaration ................................................................................................... 9
   3.4.5 Metadata ............................................................................................................................ 10
   3.4.6 Cascading Style Sheets ................................................................................................... 11
   3.4.7 Syndication (RSS) ............................................................................................................ 11
   3.4.8 Headers and Footers ......................................................................................................... 11
   3.4.9 Labeling Systems (Headings) .......................................................................................... 12
   3.4.10 Navigation and Links ....................................................................................................... 12
   3.4.11 Body and Text Formatting ............................................................................................. 14
   3.4.12 Accessibility Guidelines ............................................................................................... 14
   3.4.13 Tables and Lists .............................................................................................................. 14
   3.4.14 Navigation Link Boxes & Highlight Boxes ................................................................... 15
   3.4.15 Frames ............................................................................................................................. 15
   3.5 Server Configurations ............................................................................................................ 15
   3.6 Hosting .................................................................................................................................... 16
4. **Web Content** ......................................................................................................................... 17
   4.1 General Rules .......................................................................................................................... 17
   4.2 Content Authoring and Maintenance .................................................................................. 17
   4.3 Multi-media Content ............................................................................................................. 17
   4.3.1 Images ................................................................................................................................ 17
   4.3.2 Videos and Flash ............................................................................................................... 18
   4.4 Content Usage or Abuse ....................................................................................................... 18
   4.4.1 Files of larger size .............................................................................................................. 19
   4.4.2 Power Point Presentations ............................................................................................. 19
   4.5 Search ...................................................................................................................................... 19
   4.6 Copyrights ................................................................................................................................ 19
   4.7 Terms & Conditions .............................................................................................................. 20
   4.8 Advertising and Commercial Activity ................................................................................ 20
   4.9 Gifts and Donations ............................................................................................................... 20
   4.10 Intranet Content .................................................................................................................... 20
5. **Application Functionality on Web Sites** ............................................................................. 20
   5.1 Validations ............................................................................................................................... 20
   5.2 Development Best Practices ................................................................................................. 21
6. **Technical Standards** ............................................................................................................ 22
7. **Vendors** .................................................................................................................................. 22
   7.1 External Vendors ..................................................................................................................... 22
   7.1.1 Vendor Engagement Process .......................................................................................... 22
   7.1.2 External Hosting of Duke Web Sites .............................................................................. 22
   7.2 Internal Vendors ..................................................................................................................... 23
8. **Governance** ........................................................................................................................... 23
   8.1 Approval for Development .................................................................................................... 23
   8.1.1 Approval for Launch ........................................................................................................ 24
Introduction
The Web Policies encompass all internal and public facing websites and applications that serve content and functionality to Duke Medicine constituents or solicit appointments on behalf of Duke.

1.1 Scope
For the purposes of these policies, Duke Medicine includes:

- Duke University Health System and all its entities and programs
- Duke University School of Medicine, Departments, Divisions and Programs
- Duke affiliated Research Centers and Institutes
- Duke University School of Nursing
- Private Diagnostic Clinic, PLLC

These policies and standards apply to **external- and internal- facing web sites and applications** that are utilizing the Duke University Health System logo, and/or are hosted by Duke servers, and/or offer content or functionality to patients, students, faculty, researchers, and are owned by students, faculty, clinical and administrative staff who are part of Duke Medicine enterprise.

**Audiences** for Web policies and standards are: (1) **Website/Application Owners**, including their content editors and users, and (2) **Web Service Providers** (web site developers, web infrastructure providers). Web Service Providers are Web Service Groups inside Duke Medicine and approved External Web Service Provider Vendors. (Approved by Web Steering Committee - see Governance at Section 8).

Web policies and standards cover web security, web sites (initiation and implementation), web content, web applications (development), communications using web, technical standards for implementing web sites and applications, web infrastructure management, vendor management and web governance.

1.2 Benefits
The policies are to serve as a minimum guideline when developing web sites and web applications to Duke Medicine constituents. Standards decrease barrier to entry, implementation and usage of Duke’s web experience. Benefits of proper policies and standards focus on two key areas: User experience and Information.

1.2.1 User Experience
Purpose of policies and standards around user experience is to bring a clear, consistent, and user friendly face to Duke Medicine’s web presence. By striving towards the goal of a unified web identity, several key benefits can be gained, such as:

- Consistent user experience across Duke Web sites
- A unified vision of what each website should look like means users can tell, at a glance, that they are on a Duke Web property. They also instantly know how to navigate and use the site.
- A unified identity means that multiple websites are easier to maintain and components can easily be used across websites. This decreases cost and development time.
- A unified data organization scheme means that data can be accessed in a standard way, across multiple sites. This aids communication and interoperability.

1.2.2 Information
Purpose of policies and standards around Information is to provide consistent, accurate, current and secured information to users of Duke Medicine web sites. This will provide several benefits such as:

- Accurate, current and consistent information across Duke Medicine web sites
- A unified data organization scheme with data that can be accessed in a standard way, across multiple sites. This aids communication and interoperability.
- Information that is secured and complies with organizational policies (ISO, HIPAA etc.)
- Reducing risks to the organization, Duke constituents and stakeholders
Web Policies and Standards

2 Web Security

2.1 General Guidelines

All Duke Medicine websites and applications must adhere to the following security standards and policies:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  http://www.hhs.gov/ocr/privacy/index.html
- Payment Card Industry (PCI) Data Security Standard
  https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf

All Duke Medicine websites must adhere to the Duke Medicine Information Security Standards. Users should also be aware that their uses of Duke Medicine computing resources are not completely private. The normal operation and maintenance of Web Service's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. Web service providers may also specifically monitor the activity and accounts of individual users of Web services computing resources, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public, such as by posting to Usenet or a Web page;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of Duke Medicine or other computing resources or to protect Duke Medicine from liability;
- There is reasonable cause to believe that the user has violated or is violating this policy;
- An account appears to be engaged in unusual or unusually excessive activity; or it is otherwise required or permitted by law.

Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate person or committee in consultation with the Office of the General Counsel. Duke Medicine, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate personnel or law enforcement agencies and may use those results in appropriate disciplinary proceedings. Communications made by means of Duke Medicine computing resources are also generally subject to the same laws as they would be if made on paper.

Visitors to Duke Medicine websites who are not currently Duke Medicine students, faculty, staff or affiliates should refer to the Privacy Policy section for privacy information.

Every website and application must have a security design plan. Websites and applications containing SEI must have a certified security design plan prior to launch. All new websites must undergo a security assessment by the Web Steering Committee prior to launch.

The collection of Sensitive Electronic Information (SEI) is discouraged and must have the approval of the Information Security Officer (ISO). All SEI must be encrypted when stored in a system, application or database and transmitted over the Internet (SSL). Examples of SEI include birthday, passwords, etc.

2.2 Information Security

Please visit DHTS Information Security Office for comprehensive information on Information Security Policies and Standards (https://www.iso.duke.edu). This section covers the role of Web Service providers for protecting Sensitive Electronic Information on Web Sites and Applications.

Sensitive Electronic Information is information that requires a high degree of security and is stored or transmitted electronically. This includes Protected Health Information (PHI), as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), "identifying information" (which includes Social Security numbers), under the North Carolina Identity Theft Protection Act of 2005, authentication credentials for accessing other Sensitive Electronic Information, and other information as identified in the Duke Medicine Information Security Standard for Sensitive Electronic Information.

Following are the three key categories of Sensitive Electronic Information that Web Services Provider must pay attention to. Any web site or application containing these categories of information must have a Security Design Plan approved by Information Security Office. Such information must reside in protected web directories, databases or document repositories behind the health system firewall and served through serialization instead of absolute paths wherever applicable.
Web Policies and Standards

All Sensitive Electronic Information must be transmitted over the HTTPS protocol using SSL. Login pages to the web sites and applications that have sensitive electronic information must also use SSL encryption. Content owners that desire to purchase or renew a digital certificate should follow the instructions given on the "Duke University OIT Security Obtaining digital certificates for University servers" website: [http://www.security.duke.edu/digital-certificates.html](http://www.security.duke.edu/digital-certificates.html).

Any exceptions have to be approved by the Duke Medicine CIO or Web Steering Committee.

### 2.2.1 Protected Health Information (PHI)

HIPAA regulations define health information as “any information, whether oral or recorded in any form or medium” that

- “[i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse”; and

- “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”

All systems and applications that contain or transmit PHI must be hosted by Duke Internal Web Service Providers or have approval of the Duke Medicine CIO and Web Steering Committee for outside hosting.

If the application will only be accessed by Duke Medicine employees, it will be located in the PHI zone. If the application has access for both public and Duke Medicine employees, then the database should reside in the PHI zone and the application server in the DMZ.

### 2.2.2 Social Security Numbers

Social Security numbers must not be used for authentication, authorization, and identification purposes; instead, authentication keys generated with partial identity information should be used. For Duke Employees, the Duke Unique ID should be used as a unique identifier.

### 2.2.3 Confidential Information

Financial information, such as financial reports or notes around financial information that is deemed as confidential, shall be secured by web sites and applications. Research information and documentation that is deemed as confidential, also belongs to this category. Distribution of confidential messages and information or of inappropriate content is prohibited (ex: discussion forums, blogs, document repositories, web site content) unless the application or website is specifically secured for this type of information. These types of collaborative applications must be monitored by application and site owners on a regular basis to ensure compliance.

### 2.2.4 Privacy

Duke Medicine is responsible for insuring the privacy of our users. All websites must have a privacy policy clearly identified on every page of the website. The privacy policy must communicate what information is being collected and how it will be used as it relates to the website visitor. Even if the website does not collect personal information, the usage patterns and IP address of the user is logged for security and tracking purposes. The privacy policy must provide contact information so that visitors to the site can contact the site owner regarding their privacy.

If any information is being collected by the website, the privacy policy must communicate who will have access to that information and how it will be used. Because visitors to Duke Medicine websites may submit protected health information even though the website is not explicitly requesting it, the privacy policy must communicate who will have access to that information. The privacy policy must contain a brief description of HIPAA or a reference link to HIPAA information.

### 2.3 Access

#### 2.3.1 Authentication/Login

For Duke users and content authors, applications and Content Management Systems should use NetID using webauth for authentication.
Web Policies and Standards

For applications that require access from non-Duke users, the following standard should be implemented:

- Email address should be verified by sending a verification link to the email address submitted by the user
- Passwords should be encrypted in the database
- Ideally, passwords should be system generated. If not possible, then passwords should be set by the user with sufficient complexity to comply with the ISO’s password policy.

Authentication using Duke Identity (NetID, Active Directory IDs etc.) must be protected through SSL.

2.3.2 Authorization

Authorizations to web server level configurations to applications and web sites must be limited and shall be approved by web service provider team leads based on duties and skills of authorized persons. Such authorizations to mission critical web sites and applications (impact critical business events such as patient care, admissions, grant submissions without alternatives) must be approved by the Web Steering Committee.

Application and content administrators of web sites and applications must take caution when adding users to roles for application functionality or web site content. Application and content owners/administrators must follow departmental policies in approving authorization to specific functionality of the application and maintenance of content.

Web sites and applications must have the ability to produce reports for authenticated and authorized users. Access to Sensitive Electronic Information must be audited with elements such as user who accessed, date and time, specific resource/data accessed.

3 Web Sites

3.1 Web site registration

All websites for Duke Medicine must be registered with Duke Health Technology Solutions (DHTS). The registration information provides DHTS with website inventory, governance control and ownership information. The information required for registration:

- URL
- Hosting information
- Technical contact(s)
- Content administrator contact information
- Owner contact information

Websites’ registration information is maintained on the DHTS Web Service’s Intranet site.

3.2 Domain Naming

All domain names and URL’s have to be approved by the Web Steering Committee when requesting a new website. Third level domains follow the Domain Name Policy and Process defined by Duke University Office of Information Technology group – see [http://www.netcom.duke.edu/domain.html](http://www.netcom.duke.edu/domain.html) - and are typically reserved for Departments.

It is recommended that web sites targeting information for patients have a prefix to dukehealth.org, and sites targeting education and research have a prefix to duke.edu.

All Domain Name System (DNS) services must be provided by Duke Health Technology Solutions. No DNS services for Duke Medicine websites can be outside of DHTS. On behalf of site owners, a Duke Web Services Provider will contact DHTS ENS at host-reg@mc.duke.edu for assistance in domain and cname registration and DNS service.

Some independent research institutes (multi-university research institutes) and major health entities (centers) may be allowed a .org domain, but it must be approved by the Web Steering Committee. Domain names such as .COM and .NET, .TV etc. are not allowed, as they do not portray the academic and non-profit nature of Duke Medicine’s web presence and are confusing to users.

3.3 Branding

Branding defines web site look and feel to be consistent with web presence across Duke Medicine. Please visit [http://branding.dukemedicine.org](http://branding.dukemedicine.org) for detailed information on Branding. This section covers summary of Branding.
Web Policies and Standards

guidelines for web sites, and also provides ideas on how different elements of branding can be used to bring your own unique appeal to your site.

3.4 Development

NOTE: This section is targeted to web site developers; others may wish to skip to Section 4, which covers content.

Please visit http://branding.dukemedicine.org for detailed information on design guidelines. This section covers development-specific guidelines and best practices for web services providers in developing web sites and user interfaces.

3.4.1 General Guidelines

• When using CSS elements, cross-browser checking should be done to ensure expected behavior is present. IE 6 continues to be used widely throughout Duke Medicine.
• All images that contain words or are provided for user selection MUST have an ALT tag description
• All content areas should be titled and contain metadata.
• Images not controlled by the stylesheet will have height and width parameters and will be optimized GIF, JPG or PNG files
• Include alt tags for all images (blank alt tags should be used for spacer images)
• Include title text for all hrefs
• Do not use frames (i.e. virtual windows) unless absolutely necessary.
• Any files hosted at DHTS Web Services will adhere to standard file naming conventions (alpha, numeric, hyphen and underscore characters only)
• Provide option to increase text sizes for ADA compliance

3.4.2 Display

As of January, 2009 - 36% of users were operating with a 1024x768 resolution monitor.

<table>
<thead>
<tr>
<th>Date</th>
<th>Higher</th>
<th>1024x768</th>
<th>800x600</th>
<th>640x480</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2009</td>
<td>57%</td>
<td>36%</td>
<td>4%</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>January 2008</td>
<td>38%</td>
<td>48%</td>
<td>8%</td>
<td>0%</td>
<td>6%</td>
</tr>
<tr>
<td>January 2007</td>
<td>26%</td>
<td>54%</td>
<td>14%</td>
<td>0%</td>
<td>6%</td>
</tr>
<tr>
<td>January 2006</td>
<td>17%</td>
<td>57%</td>
<td>20%</td>
<td>0%</td>
<td>6%</td>
</tr>
<tr>
<td>January 2005</td>
<td>12%</td>
<td>53%</td>
<td>30%</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>January 2004</td>
<td>10%</td>
<td>47%</td>
<td>37%</td>
<td>1%</td>
<td>5%</td>
</tr>
<tr>
<td>January 2003</td>
<td>6%</td>
<td>40%</td>
<td>47%</td>
<td>2%</td>
<td>5%</td>
</tr>
<tr>
<td>January 2002</td>
<td>6%</td>
<td>34%</td>
<td>52%</td>
<td>3%</td>
<td>5%</td>
</tr>
<tr>
<td>January 2001</td>
<td>5%</td>
<td>29%</td>
<td>55%</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>January 2000</td>
<td>4%</td>
<td>25%</td>
<td>56%</td>
<td>11%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: http://www.w3schools.com/browsers/browsers_display.asp
Ensuring your site’s content is optimized for fixed display at 1024x768px screen resolution, without the appearance of horizontal scroll bars in the browser window, will add to the integrity of the Duke brand and provide the best viewing experience for all users.

• The minimum supported window size for content displayed is 1024 x 768 pixels.
• Pages displayed at this resolution must not under any circumstances or on any platforms display a horizontal scroll bar.
• It is deemed acceptable that a horizontal scroll bar appears at lower screen resolutions. E.g. 800 x 600 pixels.

However with the dramatic increase in adoption of mobile technology, it is advisable to provide an alternative format (or stylesheet) to support small screen devices. New devices such as netbooks support widescreen resolution formats such as 1024x600 or iPhones support automatic scaling of web content to compensate for small form factor. Automatic detection of these devices and appropriate resizing is recommended.
Web Policies and Standards

Note: 1024 x 768 refers to the target monitor resolution. The actual amount of screen space available to the developer will be less than this depending upon the configuration of the user’s browser. It is the responsibility of the creative developer to test on all target platforms to ensure compliance.

3.4.3 Generating Unique Titles

Each page must have a unique browser title that contains the key concept or topic of the page.

Browser titles should follow this format: Most Detailed Info - General Topic - More General - Most General
Example: Residency Program - Division of Dermatology - Department of Medicine - Duke University School of Medicine

For those Duke Websites using the DHTS Web Publishing Platform, this will automatically be done for you. If you are authoring your own site, you will need to make sure that each page has a unique name that accurately reflects the content on that page. This will help substantially with search engine indexing of your site.

3.4.4 DOCTYPE Declaration

There is not just one type of HTML, there are actually many: HTML 4.01 Strict, HTML 4.01 Transitional, XHTML 1.0 Strict, and many more. All these types of HTML are defined in their respective W3C specifications, but they are also defined in a machine-readable language specifying the legal structure, elements and attributes of a type of HTML.

Such a definition is called a "Document Type Definition", or, for short, DTD.

Tools which process HTML documents, such as Web browsers, need to know which DTD an (X)HTML document is actually using: this is why each (X)HTML document needs, at the beginning, a DTD declaration (or "Doctype"), such as:

≔!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"

You should specify a doctype because it defines which version of (X)HTML your document is actually using, and this is a critical piece of information needed by browsers or other tools processing the document.

For example, specifying the doctype of your document allows you to use tools such as the Markup Validator to check the syntax of your (X)HTML (and hence discovers errors that may affect the way your page is rendered by various browsers). Such tools won't be able to work if they do not know what kind of document you are using.

But the most important thing is that with most families of browsers, a doctype declaration will make a lot of guessing unnecessary, and will thus trigger a "standard" parsing mode, where the understanding (and, as a result, the display) of the document is not only faster, it is also consistent and free of any bad surprise that documents without doctype will create.

The syntax is as follows:
HTML  TopElement  Availability "Registration//Organization//Type Label//Definition  Language""URL"

Possible Values

TopElement: Specifies the top-level element type declared in the DTD. This corresponds to the Standard Generalized Markup Language (SGML) document type being declared.
HTML Default- HTML.

Availability: Specifies whether the formal public identifier (FPI) is a publicly accessible object or a system resource.
PUBLIC Default. Publicly accessible object.
SYSTEM System resource, such as a local file or URL.

Registration: Specifies whether the organization is registered by the International Organization for Standardization (ISO).
Default. Organization name is registered.
Organization name is not registered. The Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) are not registered ISO organizations.

Organization: Specifies a unique label indicating the name of the entity or organization responsible for the creation and maintenance of the DTD being referenced by the !DOCTYPE declaration—the OwnerID.
IETF IETF.
W3C W3C.
Web Policies and Standards

**Type:** Specifies the public text class, the type of object being referenced.

**DTD** Default. DTD.

**Label:** Specifies the public text description, a unique descriptive name for the public text being referenced. Can be appended with the version number of the public text.

**HTML** Default. HTML.

**Definition:** Specifies the document type definition.

**Frameset** frameSet documents.

**Strict:** Excludes the presentation attributes and elements that the W3C expects to phase out as support for style sheets matures.

**Transitional:** Contains everything except frameSet elements.

**Language** Specifies the public text language, the natural language encoding system used in the creation of the referenced object. It is written as an ISO 639 Non-Microsoft link language code (uppercase, two letters).

**EN** Default. English language.

**URL:** Specifies the location of the referenced object.

3.4.5 Metadata

3.4.5.1 Overview

Metadata's most important function is to provide identification, indexing and cataloguing of web documents and to create visibility within search engines.

Metadata helps your audience to find your content when they are using the site search function. Metadata content and context should be developed by (or in co-ordination with) the Site (page) Owner.

3.4.5.2 Adding Metadata to your Content

If you're using Web Services' Content Management System to update and add content to your website, there is a Metadata section built into the content components. Use the information below as a guideline for populating meta-tags as a means of increasing your site's visibility to search engines. Note that search engines do not rely solely on meta data in indexing and ranking a site. For more on Search Engine Optimization, see article at http://webservices.dhts.duke.edu/modules/webserv_resource/index.php?id=4

**Title meta tag**

- Format `<META NAME="TITLE" CONTENT=" ">` (when authoring your own pages)
- Presentation of title - Duke University School of Medicine to always appear first followed by the Site title and the page level title e.g.: Duke University School of Medicine - Department of Medicine - Division of Dermatology
- Title must be page specific (no generic titles across the site).
- No punctuation other than "-" hyphen

**Description meta tag**

- Format `<META NAME="DESCRIPTION" CONTENT=" ">` (when authoring your own pages)
- Description must be short and informative
- Page specific (no generic descriptions across the site).
- Total character length ~ 150 to 200
- Begin sentences with capital letter and end with a full stop

**Keywords meta tag**

- Format `<META NAME="KEYWORDS" CONTENT=" ">` (when authoring your own pages)
- Page specific keywords - do not use general terms that could be found on many sites
- Separate keywords with semi-colons
Web Policies and Standards

- Do not repeat words unnecessarily
- Lower case
- If commonly known use upper case e.g. ABC
- Include common misspellings (e.g. BigPond, Big Pond, bigpond, Bigpond)
- Remember “less is best”

3.4.6 Cascading Style Sheets

Cascading Style Sheets (CSS) are bits used to interpret the display of text.

Cascading Style Sheets, level 2 (CSS2) is a style sheet language that allows authors and users to attach style (e.g., fonts, spacing, and aural cues) to structured documents (e.g., HTML documents and XML applications).

By separating the presentation style of documents from the content of documents, CSS2 simplifies Web authoring and site maintenance. CSS2 builds on CSS1 and, with very few exceptions; all valid CSS1 style sheets are valid CSS2 style sheets. CSS2 supports media-specific style sheets so that authors may tailor the presentation of their documents to visual browsers, aural devices, printers, Braille devices, handheld devices, etc.

This specification also supports content positioning, downloadable fonts, table layout, features for internationalization, automatic counters and numbering, and some properties related to user interface. There is a style sheet for each of the levels of presentation. While each of the styles (classes) is named the same, the style is changed to reflect the level of the site. In future releases there will also be a style sheet for alternative devices like handheld PDAs or phones.

Download the CSS files to apply theme to Duke affiliated web sites. Files are available at DHTS Sample Web Site (http://webserv2.duhs.duke.edu/samplesite/html/wysiwyg/downloads/template.zip)*

* This resource is only accessible from within the Duke network.

3.4.7 Syndication (RSS)

3.4.7.1 Overview of RSS

RSS (Really Simple Syndication) is often used to provide items containing short descriptions of web content together with a link to the full version of the content. This information is delivered as an XML file called RSS feed, RSS stream, or RSS channel. An orange rectangle with the letters XML or RSS is often used as a link to a site’s RSS feed.

In 2004 and 2005, use of RSS spread to many major news organizations, including Reuters and the Associated Press, after several years of use by web logs, technology publications and other early adopters. Under various usage agreements, providers allow other websites to incorporate their *syndicated* headline or headline-and-short-summary feeds.

RSS is widely used by the weblog community to share the latest entries’ headlines or their full text, and even attached multimedia files. (See podcasting, broadcasting and MP3 blogs.)

A program known as a feed reader or aggregator can check RSS-enabled web pages on behalf of a user and display any updated articles that it finds. RSS saves users from having to repeatedly visit favorite websites to check for new content or be notified of updates via email. It is now very common to find RSS feeds on most major web sites, as well as many smaller ones.

Duke Medicine’s www.dukehealth.org currently offers multiple RSS feeds ranging from news items to advices for patients.

3.4.8 Headers and Footers

3.4.8.1 Header Guidelines

- Titles should be fully written out.
- If full name cannot fit, it should be scaled accordingly.
- Co-branding (additional logos) are not allowed in the header.
Web Policies and Standards

- Photoshop files, fonts and example HTML for headers are available for download at DHTS Sample Web Site (http://webserv2.duhs.duke.edu/samplesite/html/wysiwyg/downloads/template.zip)

3.4.8.2 Footer Guidelines

The footer appears at the bottom of every page and must include the following three elements. It is not subject to modification by site maintainers.

- Disclaimer
- Privacy Policy
- Copyright Information

3.4.9 Labeling Systems (Headings)

3.4.9.1 Headings for your Content

Every page's main text column begins with an <H1> headline, unique to the page, that expresses the main thought or topic in, ideally, one line of text. A clever turn of phrase grabs reader attention.

3.4.9.2 Headline Writing

The headline concept parallels the browser title of the page. Headlines should convey the main concept of the page. Main headlines should be active and promotional. They should not duplicate the header branding text, or use "Welcome to...." or "Our mission is....". Use Capitals for the First Letter of Each Word in a Headline. Small connective words like "the," "a," "an," "for" and so on can remain all lower-case. Headlines do not have to be complete sentences, and should not end with a period.

3.4.9.3 Structure Your Page

By using the appropriate descending headline settings, you will indicate not only content sections, but the relative importance of sections to users and search engines and accessibility tools for the disabled. Long pages should be broken into "chapters." Only the top headline should use Heading 1<H1>. The next subhead should be an <H2> or <H3>. Subsections should have <H3>, <H4> or <H5> headlines, and so on.

3.4.10 Navigation and Links

3.4.10.1 Hyperlinks

A hyperlink is any image or text that, when clicked, will cause the browser to display either a new page or jump to a specified point within a page.

Hypertext links may be used either within copy to provide a contextual link or on their own as in the links section of the site. Wherever possible, use specific deep links that take users to individual resources as they specifically relate to users' goals and enhance usability. It is generally preferable to include links as a list after a paragraph of copy rather than linking text within the paragraph, to aid readability. Annotated links in a list will enhance usability.

3.4.10.2 Visual appearance

All hyperlinks in the page body are displayed as underlined text to be compliant with expected browser behavior.

3.4.10.3 Text Labels

Use the following guidelines when linking text:

- Text that is NOT a link must not be underlined.
- Link text should be brief but meaningful when read out of context – it should describe what a user will find when the link is followed.
- Begin each link with the most important keyword
- Use action evoking verbs (e.g. read press release)
- Link text should aid scanning
- Where multiple links on a page use the same link text but point to different targets, use the title attribute to provide differentiation (e.g. More...)
- If linking to the same target multiple times on a page, use the same link text in all cases. (e.g. Return to top of page link)
Web Policies and Standards

- Use links to remove secondary information from the bulk of text
- Links to pages on other, external web sites should open in a new browser window. Links to document files should also open in a new window.
- If the link spawns a new window you should include the new window icon in the text editor which includes the alt tag "opens a new window" for accessibility compliance (WCAG 1.0, 10.1 and 13.1)
- Don’t use generic phrases such as Click Here, or Go to XX to find out More, rephrase the copy. For example don’t say Click here for org chart. Simply use Org Chart as the link.
- Don’t use a URL as link text (e.g. http://webservices.dhts.duke.edu) as it is not sufficiently descriptive to help a user determine whether they want to visit the page. Where this is unavoidable, provide a title attribute description.
- Don’t use links to split articles into sequential sections (Users will often prefer to print information rather than read it on screen).
- Consider adding a secured content icon (e.g. padlock) if a link takes the user to a secured section of the site, or advising a user if a plug-in is required to view specific content as this reduces frustration, and enhances the user experience.
- Use conventional graphic icons to denote any link that is a different file type than an html document.

3.4.10.4 Web Site Navigation

The Duke sites have four types of navigation:
- Global
- Local
- Contextual
- Breadcrumb

The Global Navigation is the same for all Duke Properties and serves to tie all the properties together. From any Duke site, visitors should be able to access the Duke.edu site, the Dukehealth.org site and the Duke University School of Medicine Site.

Local navigation is specific to the Duke property being presented. This navigation should be geared to the intended audience and appear in a column at the left of the screen. When there are two main audiences, the navigation should be split so that the labels related to each audience are clearly marked.

Contextual navigation refers to subdivisions of labeled content. The contextual navigation is located at the top of each titled content area or in a right-hand sidebar.

Breadcrumbs are used to show the hierarchy of a unit of content relative to the Home Page and appear horizontally below the site's masthead.

Photoshop files, fonts and example HTML for headers are available for download at DHTS Sample Web Site (http://webserv2.duhs.duke.edu/samplesite/html/wysiwyg/downloads/template.zip)

Local Navigation

The Navigation for the site shall appear on all pages at left side. Each label in this navigation column should represent major sections of the site.

Section tabs

- must all remain clickable on every page of the site
- must only link to child pages of the site, they must not to link to other sites (unless it is an intranet or directly related site (like Department Chair's page) which would appear to the user as a same site even though it is installed as a separate site.
- may include an expandable drop down menu of links to sub-sections.
- must not be used for functionality within the site.
Web Policies and Standards

Visual appearance

- All font, style, size and color specifications are contained in the standard stylesheet.
- Calls to CSS classes within the templates must not be altered.
- It is recommended there be a minimum of two and a maximum of nine Section Tabs.
- The current Section being viewed in your site is indicated with the corresponding Section tab being highlighted.

3.4.11 Body and Text Formatting

3.4.11.1 Formatting your Content

Paragraphs, HTML Style

The paragraph format must be applied for the normal style of text. The bulk of your page's text should be in this format. Paragraphs always have a double space in between them. You can apply Bold, embed hyperlinks, indent paragraphs, and use numbered lists or bulleted lists.

Pasting from Word

When using the DHTS Web Publishing Platform and copying content from Word, Excel or another web page to the WYSIWYG editor, use the "Paste from Word" option. This will clear 99% of the extraneous styles from the content being pasted and will allow the stylesheet to properly display your content.

3.4.11.2 Fonts

The pages should be constructed in a manner such that they will resist breaking if a user manually specifies a dramatically smaller or larger font size in their browser. Style sheets will establish default point sizes for various content areas. The default font face will be "Verdana". If a different font is used, it should be a standard one that is accessible from all computers. Initial suggestion for the sliding scale of suggested fonts is, Verdana, Arial, Helvetica, sans-serif.

3.4.12 Accessibility Guidelines

Accessibility guidelines are provided for web and application developers. Duke Medicine sites shall follow ADA (American Disability Act) compliance requirements for readability of web sites by visually impaired people. ADA compliant web site development also facilitates readability by speech readers that translate web pages into speech for the visually impaired.

Detailed information on implementing ADA guidelines is included in Appendix A.

3.4.13 Tables and Lists

Tables are used for both page structure and for presenting grids of text and/or images. Tables can be nested within one another. Both tables and lists can be used to structure and relate bits of information.

**Tables**

Style settings apply to various table elements that do not have a special class applied. Here are the native table styles:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;th&gt;</code></td>
<td>Table heading looks like this - 14px Verdana</td>
</tr>
<tr>
<td><code>&lt;td&gt;</code> No format - 12px Verdana</td>
<td>Text within table cells without paragraph or headline formatting is smaller than normal</td>
</tr>
<tr>
<td><code>&lt;td&gt;</code> Paragraph format - 12px Verdana</td>
<td>Adding the paragraph format using <code>&lt;p&gt;&lt;/p&gt;</code> tags applies paragraph style</td>
</tr>
<tr>
<td><code>&lt;td&gt;</code> <code>&lt;H3&gt;</code> format - 14px Verdana</td>
<td>Adding headline format using <code>&lt;Hx&gt;&lt;/Hx&gt;</code> tags applies headline style</td>
</tr>
</tbody>
</table>

Reminder: Table element backgrounds won't be visible in Netscape unless they contain text (&nbsp; doesn't count) or
Web Policies and Standards

Lists
Lists provide a quick and convenient way to order and structure text items. The same settings apply to both unordered lists (UL, bullet lists) and ordered lists (OL, 1,2,3 lists), 12px Verdana.

- <UL> Unordered
  - lists look
  - like this

- or add paragraph
- format <p></p>
- for double spacing

<blockquote> Blockquotes indent text but have no font settings of their own. In this example, the text picks up the <td> style, 12px Verdana By applying a paragraph format, this line of text blockquote text has been made to appear in 12px Verdana paragraph style
Likewise, this <H3> headline picks up the headline style

3.4.14 Navigation Link Boxes & Highlight Boxes

Topic boxes can be used to lift out information, feature a short blurb, link to related resources, link to anchored sections on the page below, display an image, and in many other ways.

The default color scheme can be seen in branding section. Topic Boxes with images and alternate color schemes need to be developed in conjunction with branding guidelines. Topic boxes must be 221 pixels wide and have no height requirement.

3.4.15 Frames

Today, browser support of frames is nearly ubiquitous so that should not be a concern if it is ever utilized. (See W3C Accessibility comments in this document for additional requirements)

However, frames can offer a number of challenges to both the developer and the user. Because of this, it is not recommended to use frames. It also poses significant security threats for cross side scripting (however can be managed with meticulous development and cross session validations). If a special exception arises and a need can be legitimately justified, their use will be considered.

3.5 Server Configurations

Server configuration plays a critical role in determining how your content is displayed, what content is accessible, and who can access content under what circumstances. Each configuration is typically application specific - the purpose of this document is not to outline a specific plan of action. Instead, this document outlines general guidelines and items to consider when configuring your web server.

1. Disable any services not currently in use on your server.

   Maintaining security is difficult enough on the services you are required to run. Services which are not required for a particular application should not be active. Services which are not frequently used are subject to attack and vulnerabilities may be overlooked due to this infrequent use.

2. Implement security in as granular a fashion as is practical.

   Access should be as restricted as possible while still allowing the system to function as intended. This means that users only have access to the content/services they need to perform their required tasks. Access can be granted on a group basis but that group must be actively managed and its user's authenticated using a trusted
Web Policies and Standards

3. Monitor your logs regularly.

Unauthorized access is frequently overlooked unless server logs are actively being monitored. Use of automated tools to aid with intrusion detection is recommended.

4. Enforce strong password requirements.

Strong passwords are difficult for users to remember but they are a critical component to security. Require strong passwords when a custom authentication method is required. Use a recommended authentication when possible <link to source>

5. Segregate public and private data.

Public and private data should be separated by as many security layers as possible. This should be via configuration, programmatic, and physical means. For example:

- Configuration: IP restriction at the web server level to prevent access from unauthorized addresses.
- Programmatic: Require a valid authenticated and authorized user session to access data.
- Physical: Separate public and private data on separate servers, each utilizing different configurations.

6. Assume worst case dispersal of public content and plan accordingly.

When making anything available via the web, assuming a worst case scenario of content dispersal, meaning:

- The content is available to everyone.
- The content is archived forever by a 3rd party (such as a search engine)
- The content has changed from its original format and can no longer be controlled (for example, from a PDF to text)

7. Prevent public indexing of content, unless that is a requirement.

Some web servers may be configured to allow a directory listing of contents of web directories. This can have unintended consequences that users may get the impression that their content is a private file share when it is instead a public listing. Turning off the directory index will at least mitigate the risk that unlinked documents will become public.

8. Security through obscurity is no security at all.

Even if a directory index is not available, documents placed in a public web directory are still public. Access without a link, however unlikely, is still possible and should be treated as though the content has been exposed.

9. Monitor your platform for vulnerabilities from the vendor.

Subscribe to lists to get up to date information on vulnerabilities at the Operating System (Linux/Windows) and Application (Apache/IIS/PHP/.NET) level. Patch regularly.

3.6 Hosting

All websites must be hosted by DHTS. DHTS Web Services will maintain and support all websites for Duke Medicine unless approved by Duke Medicine Vice-President and CIO (DHTS) or his designee. All websites must be hosted on DHTS supported servers under the standard DHTS platforms. DHTS will host Duke Medicine departments, divisions, centers, labs, programs, and other Duke Medicine related entities on DHTS approved servers.

When hosting the website outside of DHTS

- Any hosting of websites outside of DHTS must be approved by the by the Web Steering Committee and Duke Medicine Vice-President and CIO (DHTS) or his designee
- Any hosting of websites outside of DHTS must be from an approved vendor.
4 Web Content

4.1 General Rules

In general, Duke Medicine policies and regulations that apply to the content of publications and communications also apply to content published on Duke Medicine websites.

All Duke Medicine content must:
- Comply with all laws governing copyrights, intellectual property, libel and privacy,
- Not violate any policy, rule or regulation of Duke Medicine or Duke University,
- Not be used for non-Duke Medicine commercial activities.
- Additionally, all sites are strongly encouraged to comply with the Americans with Disabilities Act (ADA) standards or provide text-only alternate versions.

4.2 Content Authoring and Maintenance

All Duke Medicine websites that require login must be provided with the Duke NetID authentication method. To administer content, an editor will need a NetID. To post comments to news and announcements, to login to a staff intranet or to access any private areas of a SOM website, users must have a NetID. Get more information on the Duke NetID from Duke OIT.

Once a content author/editor has logged in using NetID, she will be given access to any area the NetID is authenticated for. If authenticated to maintain content on a site, the content editor will see [edit] and [add] links for any content that is able to maintain.

Without a solid and logical organizational foundation, a web site will not function well even if basic content is accurate, attractive, and well written. Cognitive psychologists have known for decades that most people can hold only about four to seven discrete chunks of information in short-term memory. The way people seek and use reference information also suggests that smaller, discrete units of information are more functional and easier to handle than long, undifferentiated tracts.

Here are some basic steps in organizing your information as content owner:

1. Divide your content into logical units
2. Establish a hierarchy of importance among the units
3. Use the hierarchy to structure relations among units
4. Populate the units closely following your information structure
5. Analyze and review your units for consistency.

Duke Medicine entities are responsible for developing and maintaining the content on their websites. Home page content should be reviewed by working with Duke Marketing (Office of Creative Services) and DHTS Web Services Department. It is the responsibility of the designated representatives in departments, divisions, programs and labs to ensure that all information in their electronic (Web) publications is accurate, current and adheres to Duke Medicine policies.

All content posted on Duke Medicine websites is the property of Duke Medicine. Any content that is not the property of Duke Medicine must have the approval of the content owner for posting on a Duke Medicine website. For sites that host content that is not the property of Duke Medicine, the website must have a disclaimer stating that purpose of the content to the visitor and how the information should be used. The content must have the appropriate copyright information.

4.3 Multi-media Content

4.3.1 Images

The use of images should not be gratuitous. A good use of images may be the inclusion of a diagram to aid in the explanation of a concept. It is recommended that large images should not be used at the top of the body area of a page where they push textural content down below the bottom of the screen at 1024x768 resolutions, as this frustrates the user and forces them to scroll down to get to the key text-based information.

Site-specific images may be placed anywhere within the web content area. Photographic images should not include images that are not relevant to the site's content or that compromise the brand of Duke Health.
Web Policies and Standards

4.3.1.1 Image Tags Attributes and ALT Tags

HTML image references must include the following arguments, “height”, “width” and “alt”. Where the image is used as a hyperlink, the border attribute should be specified as border="0"

Alt text

- All images with the exception of bullet, spacer, and panel corner curve graphics must include meaningful content in the “alt” tag argument. (Bullet, spacer and panel corner curves must have empty alt tags alt="").
- All image maps (if you must use them) must provide alt text for hot spot regions.
- Alt tags arguments should use lower case except where real names or brand names (nouns) are used, such as Duke or Executive Health Program.

Specific alt text arguments

- Pictorial Images – alt text must provide a description of the image it refers to.
- Graphical menu items – alt text must replicate the text as it appears on the related graphic. (example thermometer for progress thru web application)
- Up / down arrows - alt text must read “up” for up arrows and “down” for down arrows.
- Go icons - “go” icons associated with drop down menus (or as a graphical icon) must use the following “alt” text – “go to selected text”.
- General HTML and graphical buttons – alt text must be the same as the text on the button
- Next, Back, Save and Previous buttons – next should be used in preference to forward.
- Repeated buttons or icons on a page

“More...” icons and buttons that are repeated multiple times on a webpage require more specific alt text to differentiate clearly. In each case it is important to indicate “what” the icon/button is referring to in the alt text. (Other common examples include “View More News Articles” and “Download Patient Forms”)

4.3.1.2 Photography

Compliance will be subjectively measured by checking:

- Photographs are presented that comply with the requirements of this standard
- Copyright for use of any purchased stock art has been obtained and registered.
- Photos contain no HIPAA violations and have all appropriate patient release forms signed.

4.3.2 Videos and Flash

Video content must be hosted on OIT servers with streaming capabilities and views shall be provided using flash video player. If videos are hosted on third party sites such as You Tube, the authenticity of the videos must be validated prior to providing views on web sites. Related videos or multi-media content must be thoroughly checked for relevance before linking from web pages.

Multi-media files sometimes carry Trojan horses that are security threats. These files must be scanned before placed on the web sites. They are a bandwidth strain, are very difficult on people with alternative devices such as screen readers, and flash navigation cannot be indexed by search engines.

4.4 Content Usage or Abuse

User generated content at Duke creates a number of unique risks which can be mitigated by following proper policies and procedures.

1. Content posted by an anonymous user is strictly forbidden. This includes (but is not limited to) comments, images, videos, and links.
2. Content posted by account holders who are not associated with Duke (e.g. not faculty, staff, affiliate, etc.) must have all content moderated prior to being released to the public. Moderation is defined as being reviewed and approved by a Duke affiliate prior to public release.
3. Content posted by Duke affiliates need not be moderated, however, the following rules must be followed:
   a. The Duke affiliate needs to be granted explicit access by a manager or otherwise authorized person to post the content.
   b. Content must adhere to the Duke standards and represent Duke accordingly. Private or sensitive information should never be released to the public. This includes PHI, student information, or financial information.
c. Content should be posted in a way that adheres to Duke best practices. For example, video content should be streamed from an appropriate video server, images should be posted to the appropriate gallery, etc.

d. Under no circumstances should content of a personal nature be posted for public consumption or personal use.

e. The Duke affiliate must have read and understood this document.

4. Content should not be emailed to non-Duke individuals unless the sender has fulfilled the following requirements:

a. The email must be user initiated (e.g. requested by clicking a link) or the recipient must have given explicit permission to receive email (e.g. “opt in”)

b. If receiving email from a list, the recipient must have a way of:
   i. Unsubscribing from the list
   ii. Obtaining the physical address of the entity sending the message
   iii. Obtaining information on the method by which they were put on the list

c. Information of a sensitive nature should never be emailed (for passwords, see the ISO’s password policy).

4.4.1 Files of larger size

The web server is not a file or document management repository. Larger files significantly reduce readability and effect performance of the web server. Content owners shall not abuse the file space permitted by web server storage and look at the alternative file storage locations and link the files to the web sites instead of uploading. Unused files must be verified frequently and purged or archived to storage such as hard disks, CD/DVD discs or tape disks.

Web service providers must ensure the proper use of DHTS infrastructure and storage space when allowing content owners to upload large files. Usually, 2MB file size can be adequate. Web service providers shall advise content owners to compress files, convert to low resolutions or size efficient file formats.

4.4.2 Power Point Presentations

Microsoft Power point files may contain protected Health information, especially in “hidden parts” of images in those files. Because many Power point presentations are shared on the web, the Duke Compliance Offices required an audit of files shared on Duke's web presence. No PHI or other sensitive information should be placed on personal web spaces for distribution, and be cautious about distributing files that are derived from PHI. After thoroughly checking power point slides for PHI information, file must be converted to PDF file for posting on web sites.

4.5 Search

The location for search, if provided, should be on the right side of the masthead.

Web service providers should provide search at the site and search should not yield any protected documents or content hidden for authorized roles. Upon customer’s request, web service providers must be able to provide search statistics for the pages, keywords etc so that customers can be able to fine tune search engine optimization. For more on Search Engine Optimization, see article at http://webservices.dhts.duke.edu/modules/webserv_resource/index.php?id=4

4.6 Copyrights

All Duke Medicine content is the property of and copyrighted by the Duke University Health System or Duke University unless otherwise stated. Any content that is not the property of Duke Medicine must have the approval of the content owner for posting on a Duke Medicine website. For sites that host content that is not the property of Duke Medicine, the website must have a disclaimer stating that purpose of the content to the visitor and how the information should be used. The content must have the appropriate copyright information.

A creative work, be it an e-mail message or a doctoral dissertation, is copyrighted from the moment it is fixed in a tangible medium. No statement or registration is required. Nevertheless, in order to let others know a work is copyrighted and to deter possible infringements, DHTS Web Services requires that the following general copyright statement be applied to top level pages of the Duke Medicine Web structure:

© Copyright 2009, Duke University Health System

The entire website is covered by this statement, and therefore the statement does not need to be included on every Web page. However, if an author feels that his or her pages will be widely used by those outside the Duke Medicine community, we recommend that this or a similar copyright statement be attached.
Web Policies and Standards

As your Web pages change over time, you should extend the copyright date to cover all relevant years, i.e., © Copyright 1996-2009, Duke University Health System.

For more information about copyright in general, consult the U.S. Copyright Office (http://www.copyright.gov/)

4.7 Terms & Conditions

Every website must have Terms & Conditions. The Terms & Conditions should outline the following:

- Rules of Online Conduct
- Permission to Use Materials
- Limitations of Use
- Disclaimer of Warranty/Limitation of Liability
- Use of trademarks
- Indemnification
- Account Responsibilities.

4.8 Advertising and Commercial Activity

Advertising, such as banner ads, sponsored links, sponsoring organization information or links to other sites that promote any goods or services that is not directly associated with Duke Medicine must be approved by Duke Marketing (Office of Creative Services).

As per the Duke University E-Commerce Management Policy, Web pages residing on Duke Medicine servers are prohibited from accepting credit card numbers or other related personal information such as name on card or card expiration date. All on-line transactions involving credit cards must use the Duke University Web payment transaction server.

E-Commerce activities must be approved by the Web Steering Committee, Office of the Treasury and Internal Audit. Duke Medicine needs to comply with the e-commerce policy as provided by Duke University. This Duke University Office of Information Technology, in cooperation with the Office of the Treasure and Internal maintain the policy at http://www.oit.duke.edu/ows/duke_web_services_ecommerce.html.

4.9 Gifts and Donations

If you wish to request donations or gifts on your site, you are required to coordinate the gift request with the Development Office.

4.10 Intranet Content

Intranet content must be IP restricted and visible to Duke Internal users only. Intranet content must be further categorized, authenticated and authorized for site owners, content editors and viewers.

5 Application Functionality on Web Sites

5.1 Validations

Cross-site scripting vulnerabilities allow malicious attackers to take advantage of web server scripts that do not adequately filter data sent along with page requests to inject JavaScript or HTML code that is executed on the client-side browser. These flaws occur anywhere a web application uses input from a user in the output it generates without validating it. Any type of variable that comes from a user or comes from a place where you do not control needs to be validated. This malicious code will appear to come from your web application when it runs in the browser of an unsuspecting user.

Do not rely on client-side scripting to validate input (users can circumvent this easily); do additional server side checking.

- Every instance of user input is fully validated.
- If the application displays user supplied input, the data is displayed by a function that either escapes or converts the data into appropriate output.
- Character set encoding is explicitly set for each page generated by the web server.
- Special characters are identified.
- Dynamic output elements are encoded.
- Specific characters in dynamic elements are filtered.
- Cookies are examined and validated.
- All input is validated after Unicode, URL encode, and HTML encode has occurred, before processing.
- A centralized validation function is used to validate user input (rather than having multiple validation functions).
Web Policies and Standards

Web applications that do not properly sanitize user input before passing it to a database system are vulnerable to SQL injection. This could potentially allow a malicious user to read and/or modify any data that the application has access to.

The applications' scripts properly validate user input before passing it to the underlying database system.
- External interpreters are not used
- Bind variables are used wherever possible. Where not possible, all user variables are escaped.
- Pattern matching is used to verify user input is an expected value.
- Access is limited for the web account that is accessing the database.
- Stored procedures are used to insert records and update data; the application does not have direct access to the tables.
- The application is limited to READ-only access where possible.

5.2 Development Best Practices

The following best practices are recommended for all web application functions:

- Include security in the initial design phase of the software development life cycle (SDLC).
- Use a sandboxed or managed code environment for development.
- Use de-identified data for development and testing.
- Disable path traversal and directory browsing; place index files in each of the web directories.
- Encrypt any data passed to a client; data passed to a client (cookies, session ids, hidden fields) are modifiable by the client.
- Follow the principle of least privilege, meaning that applications have access to do only what they need to.
- If the application needs a username and/or password to log into some other service as part of its function, those credentials should not be stored in the same file as the program source code.
- If the application stores user password information, it must do so as a salted, cryptographically secure hash.
- Applications should not execute OS shell commands, and especially not pass user input to the shell.
- Applications should not write to the file system. If an application needs to store persistent state information, it should use a backend database.
- If a web application is using Duke Credentials, verify that all exchanges of usernames/passwords are encrypted from the web server to other Duke servers.
- A code review by someone other than the developer(s) should be performed before an application is moved into production.
- Remove comments and commented code from all production applications.
- Audit web directories for unused files and remove them, do not use web directories as file share.
- Remove sample scripts from all production applications.
- Remove development tools from all production applications.
- Log all access to the application, including: authentication and access control, account lockouts, accessed resources and reasons for denial of access, session termination, policy violations, data reads, writes, and deletes, failed queries, file not found errors, unexpected states, db connection failures, timeouts or performance related messages, refererrer entries. Logs entries should include user id, timestamp, source IP, description of the event, and error codes. When setting up logging, think about correlation with other logs in the case of a security incident. If using a logging API, use a commercial or open source API rather than writing your own.
- Maintain and monitor all web access logs; follow your internal policy on log creation, retention, rotation, and audit.
- Avoid generic accounts (such as DukeUser1) in production applications.
- Restrict or remove administrative access to production applications when possible. If administrator's access is built-in (for applications that require such access) consider stricter controls for such access.
- Do not rely on robots.txt files for security - it is a map to interesting pages for some users.
- Do not post production code that might provide configuration information to public mailing lists.
- Protect against all the top vulnerabilities on the current OWASP list.
- Web application programmers/developers must keep up-to-date with emerging security threats that affect web applications and should complete annual security awareness training on secure web application development. It is recommended that web application developers achieve (and keep current) certification for secure programming or web application security through SANS or other professional organizations.

The following best practices are recommended for all web servers:

- Isolate and harden web and database servers according to the CIS benchmarks and the ITSO server standard. Additional layers of security can be added, depending on the OS and application framework (mod_security or urlscan, for examples).
- Include the web application framework in the patch cycle (php, ruby, etc).
- Use a web application firewall.
- Deny HTTP PUT; allow only GET and POST.
Web Policies and Standards

- Deny access for the web server account to other parts of the web server file system.

6 Technical Standards

There is no single tool or set of tools can meet variety of needs for web sites and applications in entire Duke Medicine. DHTS recognizes that and allows flexibility for technical standards. However the economies of scale around Duke Medicine need to achieved through some measures in standardization. That measure is the standardization of tools and approaches specific to business functionality. DHTS defines the technical standards based on business functionality domain in following table.

<table>
<thead>
<tr>
<th>Functionality / Domain</th>
<th>Process Standards</th>
<th>Tool Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management</td>
<td>Agile, PMP, RUP</td>
<td>Clarity, Sharepoint, Collabnet</td>
</tr>
<tr>
<td>Application/Data Design</td>
<td>UML, ER Diagrams</td>
<td>Visio, IDE based</td>
</tr>
<tr>
<td>Application Development</td>
<td>IDEs</td>
<td>Eclipse, Visual Studio</td>
</tr>
<tr>
<td>Programming Languages</td>
<td>IDEs</td>
<td>Opensource (PHP, Ruby, Python)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mainstream (C/C++, J2EE, .NET)</td>
</tr>
<tr>
<td>Application Testing</td>
<td>Unit, Integration, Stress</td>
<td>Team Studio, Mercury, Eclipse</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Version management, builds</td>
<td>CVS, Visual Source Safe, SVN</td>
</tr>
<tr>
<td>Issue/Support Management</td>
<td>Integrated knowledge base</td>
<td>Remedy, Clarity, Collabnet, Sharepoint</td>
</tr>
<tr>
<td>Content Management</td>
<td>Content Authoring, Approval and Editing</td>
<td>Opensource (Xoops, Plone)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Commercial (WCM, Sharepoint)</td>
</tr>
<tr>
<td>Application Servers</td>
<td>Framework based, Clustering support, Load balancing</td>
<td>Opensource (Ruby on Rails, Tomcat)</td>
</tr>
<tr>
<td>Web Servers</td>
<td>Clustering support, Load balancing</td>
<td>WAS, IIS, Apache</td>
</tr>
<tr>
<td>Operating Systems</td>
<td></td>
<td>Redhat Linux, Windows</td>
</tr>
<tr>
<td>Database Servers</td>
<td>Clustering support, Load balancing</td>
<td>MySQL, Oracle, SQL Server</td>
</tr>
<tr>
<td>Directory Services</td>
<td>Active Directory, Net 1D based</td>
<td>Web Auth, Tivoli Access Manager</td>
</tr>
<tr>
<td>Network/Application Management</td>
<td>Fault Management, Configuration management</td>
<td>Nagios</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Google Appliance</td>
</tr>
<tr>
<td>Log Analysis</td>
<td></td>
<td>Google Analytics</td>
</tr>
</tbody>
</table>

7 Vendors

7.1 External Vendors

7.1.1 Vendor Engagement Process

External vendors who develop web sites/applications/portals for Duke Medicine constituents (researchers, faculty, students, care providers, staff) must be:
- Approved to do business with Duke Medicine by finance and must be on approved vendors list
- Must follow Duke vendor management policies, compliance guidelines, security standards
- Must comply with Duke branding guidelines. Any deviations must be approved by Director of Creative Services and Marketing department at Duke Medicine
- The company must sign a Business Associate Agreement
- All source code belongs to Duke Medicine, and must be provided
- All source code must be reviewed by DHTS before site is launched
- Must adhere to the Duke Medicine web standards
- Must adhere to the Duke Medicine Information Security Standards
- Must have a system security plan that documents that controls that are required by the Duke Medicine Information Security Standards

Duke constituents who engage vendors for web services must comply with above guidelines for ensuring Duke branding, security and compliance. There must be two or more competitive bids, evaluations before deciding on vendors. Code of ethics and integrity defined by compliance office will apply in engaging vendors and working with them.

7.1.2 External Hosting of Duke Web Sites

All outside contractors and service providers must be aware of this policy and HIPAA regulations as they relate to the website and web application development. Regular security scans must be performed to protect any SEI (Sensitive Electronic Information such as social security, monetary and personal health information), and reports must be submitted frequently to Duke Customers. Upon requests, vendors must be able to provide usage and audit reports and web stats. External hosting of web sites with any SEI must be approved by Duke Medicine Vice President and CIO (DHTS) or his
7.2 **Duke Employees as External Vendors**

Internal web service providers are paid Duke employees, or volunteers, whose regular job is to provide web development, hosting or management to Duke staff.

A paid employee of Duke Medicine who has extensive experience in professional web development and would like to provide fee-based web development services as an external vendor to Duke Medicine entities, programs or departments—not as part of regular job—must meet all of the above criteria for vendors, PLUS the following:

1. Must demonstrate that your external, paid development services would not create a conflict of interest with the work that comprises your regular Duke Medicine responsibilities. Specifics:
   - Must obtain express, written permission from direct supervisor or manager to do paid web development work for Duke Medicine on own time.
   - May not undertake web development work for one's own department/college/unit as an outside vendor; i.e. may not charge one's own department for work on its web site.
   - Must undertake ALL fee-based work outside Duke Medicine work hours, off-campus, using own hardware, software and other equipment, etc. See below.

2. Must agree not to actively solicit clients or “advertise” services on campus (i.e. the only permissible means of spreading the word is listing name under “approved vendors,” and word-of-mouth). Must agree to comply with and participate in the regular bid process that is used for external vendors, not using “insider” knowledge or existing relationships to gain an unfair advantage in the project bidding process.

3. Must agree to do ALL of your paid web development work on own time, off campus. This includes project planning and consultation. (It is understandable that some communications/phone calls/e-mails may need to take place during regular business hours. In these cases, one must ensure that any time away from regular job takes place during regular lunch hour, or that the time is promptly made up with no disruption to regular responsibilities.

4. Must agree not to use any Duke University and/or Duke Medicine computers or related hardware/software/media in fee-based web development work. Internal vendor must personally purchase and use own computer system and all necessary software for web development.

5. Must agree not to use any component of the Duke Medicine web site design, standards, templates or guidelines to advertise or promote web development services to clients or potential clients.

6. Must agree to complete your paid development work in good faith even if your regular employment status at Duke Medicine changes during your work on an outside web project.

7. Must agree to provide brief and reasonable (1 or 2 sessions) site-maintenance training to a designated Duke Medicine employee upon completion of project, upon departure from Duke Medicine, or upon reasonable request (option to be selected by Duke Medicine).

8. Must have a signed copy of the Duke Medicine Employee-Vendor Agreement on file with the Director of Web Services before bidding on any Duke Medicine web projects.

8 **Governance**

The Web Steering Committee is responsible for ensuring all public web sites adhere to all Duke Medicine policies, standards and guidelines. The steering committee is made up of leadership from DUHS, the School of Medicine, Marketing & Communications office and Duke Health Technology Solutions. The committee meets on a monthly basis.

All sites represent Duke Medicine's image, brand and reputation. All sites have to be approved for development and approved for launch by the Web Steering Committee.

8.1.1 **Approval for Development**

To evaluate the need for the website, that the website will be properly maintained and supported, a request has to be made to the Web Steering Committee for approval to develop.
Web Policies and Standards

The information required by the committee includes:

- Purpose
- Intended Audience
- Requestor's contact information
- Primary Owner
- Primary Department/Division/Center/Lab/Program
- URL of existing site
- Proposed URL (must adhere to the Domain Name Policy and Process)
- Functionality overview
- Technical overview
- Hosting requirements

All requests must be submitted to the DHTS or Marketing Web service department directors. The Web Steering Committee will review the submitted information. All questions from the committee will be directed to the requestor's contact information submitted. The committee will review the information and provide the final decision on the website within 10 business days. If the website is approved by the committee, any changes during the development process must be communicated back to the committee.

8.1.2 Approval for Launch

Prior to launching the website, a request for launch must be approved by a member of the Web Steering Committee. The committee will review the site to ensure it meets domain naming convention, all policies, standards and guidelines. The committee will also perform a security assessment to ensure that the website is secure. Only after the committee has reviewed the site and approved it for launch may the site go live. Failure to receive launch approval will result in the site being turned off. The Web Steering Committee will respond to all launch requests within 10 business days.

For websites that are denied approval for development or launch, the decision may be appealed by requesting a meeting with the Web Steering Committee.

9 Appendix A – Detailed Accessibility Guidelines for Developers

Provide a text equivalent for every non-text element.

Some types of information may not be directly accessible to everyone. Images, for example, are not directly accessible by someone who cannot see, and audio files are not directly accessible by someone who cannot hear. Information provided in the form of a Flash movie will not be directly accessible by someone using a browser that can't handle Flash. So it is important to provide the same information in an alternative format, to ensure that everyone can access the information in a format that suits their own needs, and which is compatible with their web browsing technology.

Text is the most universally accessible and flexible medium, and as a result is the format most used for providing alternatives to other media. This does not mean, however, that graphics and multimedia elements should be replaced by text - they greatly enrich the user's browsing experience, and can aid the user's comprehension of the information and services being offered on a website. It does mean that, where non-text elements are used, the same information should be provided in a textual format, to enable all users to access it.

For example - an option available to low-vision users is a speech browser or a screen reader. This software will read out, in a synthesized voice via the sound system on the PC, the contents of a web page. Graphic images are obviously not directly accessible to this kind of software, but the addition of a text alternative through the use of the ALT attribute provides text which can be accessed by speech browsers, screen readers and text-only browsers. The addition of meaningful alt text to images is one of the most basic techniques for making the content of a web page accessible to a wider range of users.

Here are examples of how to provide appropriate alternative textual content for non-text elements in a website:

**Images which convey information** - If the actual content of the image is what is important, then that is what should be relayed, succinctly, in the ALT text - e.g. "Photograph of the Chief Executive".

**Purely decorative images** - If the image does not convey any information and has no function other than as part of the visual appearance or decoration of the web page (i.e. it is simply part of the "window dressing", sometimes referred to as "eye candy"), it should be given null or empty alt text, i.e. alt="" or alt=" ".

**Functional images** - If the image performs a function, such as being a hyperlink or a button to activate a selection or submit a form, it should be given alt text which describes that function. In the case of an image which is a link, the alt text should indicate the link destination, e.g. "Home", "About us"; etc. A form Submit button, on the other hand, could be given alt text which reflects the purpose of submitting the form, such as "Search now", "Go", etc.
Images of text - Best practice is to avoid using images of text - instead, actual text should be used wherever possible. If the text consists of more than a few words, it should certainly be presented in text format rather than as an image. If images of text are used, however, the alt text should be the same as the text displayed in the image.

Layout images - These are images whose only purpose is to help define and control the visual layout of the web page. Usually invisible (i.e. consisting of a single color set to be transparent), these images are commonly named "spacer.gif", "trans.gif" or "shim.gif". These images should be given null or empty alt text, i.e. alt="" or alt=" ". Best practice, however, is to phase out the use of such images in favor of using CSS to format the layout of a web page. The use of these images should certainly be kept to a minimum.

Structural images - These are images which are used, often in place of more appropriate HTML coding, to provide the user with information about the structure of the content in which they appear. For example, a list of items might be presented in a table, with a bullet graphic preceding each item, thus visually defining the material as a list. Or a graphic might be used to visually indicate the end of one section of a page and the start of another. Best practice is to dispense with this practice, and use appropriate HTML coding to accurately code the structure of the content. CSS formatting can then be used to create the desired visual appearance. So, for example, a list could be coded as an actual bulleted list using UL, with LI used to define each list item, and CSS formatting can then be used to specify the desired bullet graphic. However, where structural images are used, the alt text should reflect the structural nature of the image rather than its visual appearance. So a list bullet graphic could, for example, be given the alt text "*" (i.e. a textual representation of a bullet), "bullet" or "item".

Complex images - Some images, such as charts or graphs, may present more information than can be presented using the alt attribute, since alt text should be short and succinct, no more than a short phrase or sentence. These images should be given a short alt text (e.g. "Graph showing the steady growth in share prices over the past five years"), and a more detailed description of the information presented in the image should be provided in one of several possible ways:

- In the accompanying text on the same page.
- On a separate page, with a link to that page placed next to the image (e.g. "Full text description of the information presented in graph A above"), or with the image itself providing a link to the fuller text description - this fact should then be included in the image alt text (e.g. "Graph showing steady growth of share prices over the past 5 years - link to full description").
- On a separate page, with a link to that page provided via the longdesc attribute for the image. Note that not all browsers or screen readers can be guaranteed to work with the longdesc attribute, so it should not be used as the sole means of linking to the fuller text description of the image.
- On a separate page, with a "D" (for "description") link provided immediately adjacent to the image (literally the letter "D", hyperlinked to the page containing the long text description).

Image maps - The main image being used as an image map should be given alt text which reflects the overall theme of the image map, e.g. "Site navigation links" or "Map of wards in XXX district". Each AREA element which defines a "hotspot" on the image map should then be given alt text indicating the link destination associated with that hotspot. For various reasons such as maintainability, etc. image maps have generally fallen out of favor and their use is discouraged.

Java applets - The opening <applet> tag should be given an alt attribute with a brief description of the applet. In addition, however, you should provide a true alternative to the content and functionality of the applet wherever possible. While this can be placed between the opening and closing APPLET tags, and will, when placed there, be presented to anyone using a browser unable to handle Java applets, that is of little use to someone using a browser which can handle applets but with assistive technology which can't. So in many cases it will be preferable to provide an HTML alternative either on the same page as the Java applet or on a separate page and provide a clear link to the alternative page close to the applet.

Flash objects - Flash items are presented within web pages through the use of the OBJECT element. OBJECT does not permit the use of an alt attribute, but alternative content can be provided between the opening and closing OBJECT tags. However this presents the same problem as with Java applets, and so again it is best to provide a link to an HTML alternative close to the Flash item, or on the preceding page (e.g. gives users the choice of Flash or HTML content). In the case of purely decorative Flash items, however, it is acceptable simply to provide a brief text alternative between the opening and closing OBJECT tags.

Audio files - In general, a text transcript should be provided for all audio content (the exception being music, where a simple description is acceptable). A clear link should be provided to the transcript, close to the link to the audio content itself. If much spoken audio content is used, serious consideration should be given to incorporating it with a visual track showing the content being conveyed in sign language.

Video files - Again, the simplest solution is to provide a text transcript of the audio-visual material. However, depending on the nature of the content, serious consideration should be given to creating a true multimedia presentation, with a spoken audio description of the visual content, and captions or sub-titles showing the audio content, all synchronized into a single presentation.
Web Policies and Standards

If frames are used, provide meaningful, useful NOFRAMES content.

Frames - "sub-windows" which divide the screen into two or more separately sections which can be changed and scrolled independently - cause all sorts of problems for users. They make it difficult for users to bookmark pages they wish to come back to. They are also inherently graphic and visual - users of text-based browsers can only access one frame at a time, which may make using the site more difficult and complicated.

We recommend avoiding frames altogether, but if they are used, it is important to provide alternative, non-framed access to the same content. This involves using the NOFRAMES element to provide meaningful content and links to enable the user to access the rest of the site outside of frames.

Iframes are "inline frames" embedded within an otherwise standard web page. There is no NOFRAMES option for iframes, but alternative content can and should be presented between the opening and closing IFRAME tags. At its simplest, this can consist of a link to the content which would otherwise be displayed within the iframe.

Provide redundant text links for each active region of an image map.

Most current assistive technology can handle and identify the different sections of image maps (a single image with multiple “hotspots” or hyperlinked areas). However the ability to manage image maps isn't yet universal and they can also present a problem for users who are partially sighted and who rely on the browser to enlarge text to make it readable, since this won't work with a graphic. To provide maximum versatility, therefore, we recommend that additional, text links be provided, either on the same page or, if that isn't feasible, on an alternative, linked page.

Ensure that all information conveyed with color is also available without color.

It is important to avoid relying solely on colors to convey information. People with sight problems (e.g. color blind or partially sighted users), users of non-graphic browsers (e.g. text or speech browsers) and users of some mobile internet devices (e.g. palmtops with black & white displays) may be unable to distinguish the colors differences, and may therefore be excluded from relevant and/or important information. This doesn't mean that colors should not be used to convey information - it is a highly effective means of communication for those who can perceive it. It should not be relied on as the sole means of conveying specific information however - additional means of conveying the same information should be used. So, for example, when highlighting those sections of a form which are mandatory, as well as using color an asterisk can be added to the text labels of those sections of the form which must be filled in. That way, all users will receive that information.

Ensure that foreground and background color combinations provide sufficient contrast (particularly for images).

Partially sighted users have widely varying needs when it comes to color combinations and font sizes. One requirement that is important to everyone, however, is that there is adequate contrast between text and background, or between different parts of an image. While users may be able to use their browser settings to choose their preferred text and background color settings, designers should still aim to provide good contrast as part of their design - this will make the content easier and quicker to access for all users. This is particularly important when images are used to convey information, since users generally have no way of changing how an image is displayed.

Avoid the use of images of text wherever possible, and provide equivalent text links for links which consist of images.

Some users require larger (or smaller) text, and some need to use their own choice of text and background colors for legibility (e.g. through choosing high contrast color combinations like yellow on black). When a graphic of text is used instead of text itself, these choices are unavailable to the user - the size and colors of the graphic can't be changed. For users of screen magnification software, graphics of text present a different problem - as the degree of magnification is increased, the text contained in such graphics becomes increasingly blurred and pixellated, becoming more and more difficult to read. Actual text, on the other hand, can be scaled smoothly by the screen magnification software, ensuring that it remains legible even at high levels of magnification.

As a result we recommend either using actual text instead of a graphic of text, or (in the case of graphics which are also links) to provide the same links in text form on the same page (e.g. at the bottom of the page).

Use relative rather than absolute units in markup language attribute values and style sheet property values, and ensure that information can still be accessed if the user changes the font size.

One option available to people with poor sight is to use the settings in their browser to display web pages using their own choice of font face, font size and foreground and background colors. If absolute font sizes (i.e. sizes defined in points or pixels) are used, it can make it more difficult for the user to do this. While it is possible (though still difficult) for users of more recent browser versions to override absolute font sizes, those using older browsers may not be able to do so. It is preferable to use relative font sizes that take account of the user's preferences, and which can be overridden by the user.

Care should also be taken when specifying the size of tables and table components (rows, columns and cells), and when using CSS to position sections of content on the page (e.g. when using DIVs for drop down menus, etc). Relative units (e.g. percentages or 'em' values) should be used wherever possible to accommodate different user requirements and
settings. If absolute units are used, the page should be checked using a wide range of resolutions and browser settings to ensure that sufficient flexibility is provided in the page design to accommodate user requirements (e.g. large font sizes and low resolutions) without resulting in truncated or overlapping sections of content.

If the CSS "line-height" property is defined using absolute units such as pixels, the spacing between consecutive lines of text will remain fixed even when the text size is changed in the browser. The result, if the text size is increased, is often overlapping lines of text. So it is advisable to use relative units (such as "em" units) to specify properties of this nature.

**Use heading elements to convey document structure and not for visual formatting.**

WCAG1 reference(s): Checkpoint 3.5 (priority 2).

Some forms of assistive technology can present the user with additional information about the content of a web page, based on the structure coded into the page. For example, the user may be able to access a summary outline of the page based on the headings and sub-headings present in the page. This feature can't operate when the structure of a web page is represented purely by visual formatting, rather than by the appropriate use of heading tags (H1, H2, etc). Similarly, it can be extremely confusing to anyone trying to use the heading structure to gain an overview of the page content if elements that are not headings have been coded as headings (e.g. simply for the purpose of visual text formatting).

For consistency, even where a page only has one top level heading, we still recommend coding that properly uses H1.

**For data tables, identify row and column headers.**

While fully sighted users can view all or most of a table at once, and refer back to row and column headings quickly, non-sighted users must access tables in a linear fashion. To aid these users in orienting themselves within a table and in understanding the information being presented, some screen readers provide table navigation capabilities. These features depend, however, on table row and column headings being properly identified in the page code - if 'td' ("table data") is used to code every cell throughout the table, there is no way for the browser to identify heading information and relay it to the user. As a result, when tables are used to present genuinely tabular information, it is essential that heading information is properly coded using the 'th' ("table header") element. This can be used to code both column and, where appropriate, row headings - the position of the cell within the table makes it clear to the assistive software which type of heading it contains.

**Complex tables:** HTML 4 contains additional code intended to enable the accurate coding of complex, multi-level headings through the use of 'scope', 'id' and 'headers' attributes for table cells. Unfortunately, few screen readers pick up on this information at present, and we recommend that complex tables be broken down into a series of simple tables, with just a single row of column headings. Row headings should be kept similarly simple. This will not only ensure that screen reader users can access the table, but will make the information easier for all users to understand.

**Do not use tables for layout unless the table makes sense when linearized.**

Those using text-only, speech or Braille technologies to access web pages will receive the page content in a linear stream, very different from the way in which users of graphic browsers experience the page. It is important that care is taken to ensure that, when presented in this linear way, the content of the page is presented in a logical sequence. In most software, the content of a table will be presented cell by cell across each row, from the top row downwards, and the table (plus any nested tables) should be designed so that this will result in the content being presented in the correct order.

This also has in important impact on the TAB sequence through the links and form elements on a page. In most cases where the TAB sequence is illogical, the cause is poor layout table structure. If the table structure is corrected, the TAB sequence will also be corrected.

**If a table is used for layout, do not use any structural markup for the purpose of visual formatting.**

The use of "table heading" HTML code (th) is generally handled by graphic browsers by centering the content and displaying it in bold format. However, since structural coding of this sort is used by assistive software to convey contextual information to users, it should not be used simply to achieve a desired visual effect in a table which is there solely to control the visual layout of the page, as this can become extremely confusing to these users. The cells in layout tables should be coded throughout the table using the 'td' element, and style sheet formatting can then be used to achieve the desired visual effect.

Similarly, the CAPTION element is intended to provide a caption for data tables, not a caption for, for example, an image which is contained within a layout table.

**Organize documents so they may be read without style sheets, and ensure that information can still be accessed if the user changes the text and background colors.**
Web Policies and Standards

When a style sheet is used to position the various elements on the page, it is important to ensure that order in which the page content is listed in the HTML code is logical and makes sense. If someone accesses the page using a browser or other technology which does not use style sheets, or if the user has selected to use their own style sheet to make pages more easily readable, they will be presented with the content in the same order in which it appears in the HTML code.

Most graphic browsers allow the user to change the text, background and link colors. If pages are designed only to function correctly when viewed using the colors specified in the page (e.g. with images which have transparent backgrounds and which depend on a specific background color being used to ensure legibility), users may have difficulty accessing the information if they choose their own color settings. This is a particular issue with images of text. While we recommend avoiding these wherever possible, if images are used which display text, they should have an opaque background so that legibility is maintained if the user changes the text and background colors used to display the page.

It is also important to define either all or none of the text, background and link colors in a site, and to keep the color definitions either all in the HTML formatting or all in the CSS styles. Users may have non-standard colors set up as the default colors in their browser, but only activate these colors on specific, badly designed sites. If a page has a defined background color but no default text color defined, the page will be displayed using the defined background color and the user's default text color. This can result in unreadable text! For example, if the user has a default setting of yellow text on a black background, then a page which has a white background color but no default text color will be displayed using yellow text on a white background - completely unreadable. It is preferable to define all of the colors on the page and ensure that these colors provide reasonable contrast between text and background. Those who require using their own special color scheme will override these page settings while other users will be able to access the page as it is designed. Note that a similar problem can arise if the color definitions are split between HTML and CSS formatting - if the user switches off support for style sheets in their browser, only some of the text, background and link colors will be defined, resulting in potentially illegible text.

**When providing information in PDF format, provide the same information in an alternative, accessible format (e.g. HTML or text) or provide links to the tools provided on the Adobe website.**

While PDF files and the Adobe Acrobat Reader software continue to improve with regard to accessibility and their compatibility with assistive technologies (e.g. screen reader software), they are still not universally accessible. New PDF documents should be produced using the latest available version of Adobe Acrobat and following Adobe's guidelines on creating accessible PDFs (see [http://www.adobe.com/products/acrobat/solutionsacc.html](http://www.adobe.com/products/acrobat/solutionsacc.html)). Best practice is still, however, to provide the same information in other formats that are accessible, like HTML or text. Where PDF documents are offered, a link should also be provided to the tools available on the Adobe website ([at http://www.adobe.com/products/acrobat/access_onlinetools.html](http://www.adobe.com/products/acrobat/access_onlinetools.html)), where tools are available to help users access the content of PDFs. This link should either be provided wherever PDFs are offered in the site, or, if there is a Help page on the site relating to how to access PDFs, the link can be provided there.

**Avoid causing the screen to flicker.**

Some people are highly susceptible to certain types of strobe or flickering effects. It is therefore important that programmers avoid creating special visual effects which would result in the screen, or substantial parts of it, flickering or changing rapidly and rhythmically. The following is a quote from the WAI core techniques document ([at http://www.w3.org/TR/WCAG10-CORE-TECHS/#flicker](http://www.w3.org/TR/WCAG10-CORE-TECHS/#flicker)):

"A flickering or flashing screen may cause seizures in users with photosensitive epilepsy and content developers should thus avoid causing the screen to flicker. Seizures can be triggered by flickering or flashing in the 4 to 59 flashes per second (Hertz) range with a peak sensitivity at 20 flashes per second as well as quick changes from dark to light (like strobe lights)."

**Do not automatically refresh, redirect or timeout pages without warning the user.**

When accessing a page visually, the fact that it refreshes periodically may not cause a problem, since the sighted user can simply resume reading the page at the point they had reached before the refresh. However, someone accessing the page aurally will be returned to the start of the page when it refreshes. Listening to a page tends to be a slower process than viewing it, and some users may never manage to access all of the information on a page which is continuously being refreshed. If no process can be found for allowing the user to determine the period between refreshes (this should include the option of “no refresh”), then it may be necessary to offer an alternative page which doesn't refresh automatically, leaving it up to the user to refresh the page information via their browser's Refresh command.

A similar though lesser problem is presented by pages which use the meta refresh tag to redirect the browser to a different page. Here, the user is likely to have difficulty in using their browser's BACK command to return to previous pages, since they may be unaware that a redirect has occurred. A screen reader user may also hear the start of the redirect page being announced, only to find themselves being bounced on to another page without having done anything to cause it. To avoid these problems, redirects should be set up on the server, so that they are transparent to the end user.

Timeouts are commonly used on banking websites to safeguard the user's confidential information in the event that they are using a computer to which others have access. However it is important that the user is fully informed that a timeout...
Web Policies and Standards

feature is in place, and how long they have to carry out any particular action. If possible, consideration should be given to allowing the user to adjust the timeout limit, to accommodate the possibility that they require longer to carry out the necessary actions.

Ensure that links and controls are keyboard navigable, and create a logical tab order through links, form controls, and objects.

For those who can't use a mouse or other pointing device, it is essential that pages are navigable using the keyboard. Navigation features which can only be accessed using a mouse can render most or all of a site "out of bounds" to any user who relies on the keyboard. So it is important to ensure that all of the site's navigation and functionality can be accessed through the use of a keyboard.

For those who rely on the keyboard for navigation, the TAB key (or equivalent) is how they skip through the links and form elements on a page. The default order in which the TAB key will cycle through these elements is the order in which these elements appear in the HTML code. In most cases, this is also the most logical and intuitive order, but occasionally, because of how the page has been structured, it is necessary to set the order artificially in order to ensure that the sequence is sensible. This can be done using the 'tabindex' attribute - each element is assigned a number with this attribute, and the TAB sequence will then run from the lowest through to the highest numbered page element, regardless of the order in which these elements are listed in the HTML code.

Do not cause pop-ups or other windows to appear, and do not change the current window, without informing the user.

While fully sighted users can see at once that a link has opened a new window, blind and partially sighted users can't, and while some assistive software will inform the user that a new window has been opened, not all of the assistive software does this. This can cause a great deal of confusion for the user - it may take them some time to work out why the BACK command on their browser won't take them back to the previous page. As a result, it is preferable to minimize the proliferation of browser windows if possible, or at least to inform users as to which links will open in a new browser window.

Ensure that all form controls have labels and that these labels are properly positioned.

Users of speech and Braille output systems rely on the correct association of text labels with form elements (input boxes, drop-down lists, radio buttons, etc) to enable their software to provide them with the information they need in order to fill in online forms. If no text labels are provided, it may not be obvious to the user what information should be entered into a particular form element. The text labels for checkboxes and radio buttons should follow these elements (i.e. the text should be immediately to the right or below these elements), while the text labels for all other form elements (text entry boxes, drop-down lists, etc) should come immediately before these elements (i.e. the text should be immediately to the left or above these elements).

In addition, thought should be given to the layout of forms, with instructions being presented before the form elements to which they refer, rather than after.

Clearly identify the target of each link.

Many browsers and screen readers provide the user with the facility of listing all of the links on a web page. This can be a useful method of quickly finding and accessing one link out of many on a page. When taken out of context in this way, however, it is important that the link text clearly conveys the destination of the link. While the 'title' attribute can be used to provide additional information about a link, best practice is for the link text itself to provide clear information about the nature and content of the link destination.

Give each page a unique TITLE to aid users in orienting themselves within the site.

For fully sighted users using a graphic browser to access the web, it is usually easy to see if a new page has been loaded in response to activating a link or form button. It also rarely takes more than a few seconds to identify if the new page is the one the user expected or wanted to reach.

Users of text and speech based software, however, are much more dependent on the first few words or phrases on the page as an indicator that they have reached the page they want. For many of these users, the page title is the first item they see or hear. When (as is often the case) there are many identical links repeated at the start of every page, the title becomes a very important indicator as to which page is being accessed.

If many pages share the same title, it can substantially increase the length of the time the user must spend listening to or reading the first part of the page in order to determine what page has been loaded. It also becomes difficult for the user to build a clear mental map of the site and to orient them within the site. As a result, we recommend that all pages have their own identifiable and succinct title.

Additional suggestions
Web Policies and Standards

Specify the main language used on a web page.
It is good practice to identify the primary language of a web page, especially when dealing with pages which include more than one language. The primary language can be identified by adding a 'lang' attribute to the opening 'html' tag, as follows: <html lang="en">

A range of two letter codes are available to specify languages. Commonly used codes include:
- **en** = English
- **cy** = Welsh
- **fr** = French
- **de** = German
- **it** = Italian
- **es** = Spanish
- **pt** = Portuguese

Include a valid doctype declaration at the start of the page code, and ensure that the HTML code is valid and correctly structured.

We recommend including a doctype declaration on each page, and using a code validator to check that the page code is valid and free of errors. While this in no way guarantees an accessible page, it is a good way of ensuring that invalid or "browser specific" code, which can cause accessibility problems, is avoided. Browsers vary in how forgiving they are of coding errors, and ensuring that the code is clean and valid is a good initial step towards ensuring that the page will function as intended in all browsers and access technologies.

The doctype declaration refers to a published code standard (Document Type Definition or DTD) to which the page claims conformance, and its provision can enable modern browsers to better render the content being provided.

The simplest initial choice of doctype is currently 'HTML 4.01 Transitional':

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
```

On frameset pages, the 'HTML 4.01 Frameset' DTD should be used:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
```

The doctype declaration should be the very first item of code in the page, with nothing preceding it (including blank lines).

Web access centre: Document Type

Provide a 'skip to main content' link at the start of each page.

We recommend adding a "skip to main content" link at the start of each page. This will benefit screen reader and text browser users, enabling them to jump over lengthy, repeated navigation menus, and go straight to the content on the page. This technique can also be used to skip over groups of links repeated on each page. To do this locate a 1x1 pixel transparent image at the start of each page with the alt text "Skip to main content", and make it a link to a bookmark at the start of the page content.

**Note 1:** We recommend using the phrase "Skip to main content" rather than just "Skip to content" since research has shown that screen readers often pronounce "Skip to content" with the emphasis on the second syllable in "content", confusing many inexperienced users, whereas the addition of the word "main" leads the screen reader software to pronounce the word correctly.

**Note 2:** This technique should be used sparingly, as it creates a "hidden" link, which has the potential to be confusing for sighted users who use the keyboard to navigate around the page. When they press the TAB key to move from one link to the next, the effect of a hidden "Skip" link is that the visible focus vanishes, and they have to press the TAB key again to move the focus to the next visible link or form element.

Best practice would be to make the "Skip to main content" link visible, so that all users can benefit, and avoiding the problem of "hidden" links mentioned above. For example, someone using screen magnification will welcome a "fast track" route to the page content rather than having to scroll down for what can be quite a long way when the page is greatly magnified.

Ensure the text content is legible.

Capital letters
Web Policies and Standards

Whole phrases, sentences and paragraphs in capital letters can be difficult to read for some users (the shapes of lower case letters are easier to see) and, in the context of online communication, appear TO BE VERY LOUD - it creates the feeling of being shouted at! Text should be presented in standard sentence case.

**Italics**

Italics work well in print, which is a fixed, high resolution medium. On a monitor screen, however, the resolution is much lower, and the fact that the screen image is being refreshed many times a second can, for some people, create a shimmering effect with italic letters which makes them much more difficult to read. Occasional individual words in italics can be acceptable, but as with the use of capital letters, it should be avoided for whole phrases, sentences or paragraphs. This is commonly seen in Terms & Conditions, Privacy Policies and other legal documents which have been designed initially for print, and simply placed on a website unaltered. These documents should be reformatted before being placed on a website.

**Underline**

Underlining whole phrases, sentences or paragraphs can also produce similar problems with legibility, since it obscures part of the shape of letters. It should also generally be avoided except in the case of hyperlinked text, since underlining is commonly understood to indicate a hyperlink. The use of underline for text which is not a hyperlink therefore has the potential to confuse users.

**Justified text**

We also recommend avoiding the use of justified text, as it doesn't work well online, with large variations in the gaps between words, making the content difficult to read. In particular, the often large gaps between words in justified text can cause real problems for those using screen magnification, who can be 'fooled' by the large gaps into thinking they have reached the end of the line of text and move down to the start of the next line, only to find that it doesn't make sense, since they have actually missed one or more words at the end of the previous line. Until browsers become generally better at rendering justified text, it is best avoided.

**Acronyms and abbreviations**

As well as using the 'acronym' and 'abbr' elements to give the expanded form of acronyms and abbreviations, it is good practice to use the expanded form when the acronym or abbreviation is first used on a page, with the contracted form following it in brackets. The contracted form can then be used elsewhere on the page.

For example, we normally refer to the "Royal National Institute of the Blind (RNIB)" when first mentioning the organization, then subsequently refer to it as "RNIB".

Common sense should be used, however, since some acronyms are so well known and commonly used that it may be not necessary to give the full form (for example, ‘BBC’, ‘UNESCO’, etc).

**Explain the session timeout feature to users.**

If no warning is given that a site will ‘timeout’ a user session, it can be very confusing for the user, when they return to the PC, to find that they are on a different page to the one they were viewing when they left the PC. This is particularly true for those who cannot see the screen, and for them, even if they are sitting at the PC when the timeout is triggered, they may not be sure of what is happening. It is therefore very important that adequate warning and explanation is provided to ensure that users are aware of the fact that they have a time limit for completing some actions, and to ensure that they are aware of what will happen when the timeout feature is triggered. We recommend that you include information about this on the entry page to the area where a timeout feature is present, and in the “Help” or “About this site” section, so that users are aware of this feature.

Once a user has been logged out, they should be provided with clear instruction as to how or where to log in again.

**Use the clearest and simplest language appropriate for the site’s content.**

Clear and simple language is essential for the usability of the site for all users, not only those with low-vision, dyslexia or cognitive problems. Aside from the content itself clear language includes relevant headings, link text and succinct instructions. Also ensure that the topic is stated at the start of a paragraph or sentence and paragraphs are limited to one main idea. This will help both people who are scanning the page visually, and also people using screen readers.

"Scanning" with speech means the user can jump from heading to heading, or paragraph to paragraph and assess quickly whether the information (heading, paragraph, link, etc.) is relevant to them.

Long complex sentences also should be avoided. Other problem areas include slang, jargon, and specialized meanings of familiar words. These all cause problems unless defined within your document.

Care must be taken to ensure that forms have clear and succinct instruction. It is important that instructions are not given at the end of the form as users with screen readers and screen magnification will not be aware of this information until they reach the end of the form. Also insure that instructions are not dependent on vision i.e. “click on the left hand button to view the page”. Users with text browsers and screen readers will be left none the wiser as to where what they...
Web Policies and Standards

are looking for on a page is. Visual instructions should be avoided and all instruction placed next to the element that it refers to, or should refer to items by name rather than by position.

**Hide JavaScript functionality that is not crucial to the site.**

Some sites offer JavaScript functionality that simply duplicates functionality available in the browser. For example links to print or bookmark a page, or to close a browser window. This is not a problem in terms of accessibility, since the user can access these functions through their browser. However it is annoying to be presented with a link or page element which won't work. To avoid this we recommend using JavaScript to present the link or page element, so that if a user does not have JavaScript enabled, the item will not be displayed. For example:

```html
<script type="text/javascript"><!--
document.write("html code")
-->
</script>
```

This way, the item will only be displayed to those whose browser can make use of it, and will not be displayed in circumstances where it won't work.

**Use LABEL to associate form elements with the accompanying text.**

While it is important to ensure that text labels for form elements are correctly positioned, it is good practice, and for some users helpful, to use the 'label' element to explicitly associate a form element with the appropriate text. Increasingly, screen reader software can use this explicit association to ensure that the appropriate text is read out in relation to the form element. An added benefit is the fact that the use of 'label' makes the label text "clickable" as well as the form element, which, in the case of checkboxes and radio buttons, provides users with a larger area to click on - those who have difficulty with small, accurate mouse movements will benefit from this.

**Add a page menu and 'Back to top' links to long pages.**

We recommend adding a page menu and regularly spaced 'Back to top' links to all pages that have a large amount of content and which would otherwise require a lot of scrolling. This will make it easier for users to move up and down through the page content.

**Make the links to and from the text version of a site specific to the pages from which they lead.**

When a text-only version of a site is offered, it is frustrating to find that, no matter what page of the graphic version one is on, the link to the text-only version links to the home page in that version. The user then has to remember the route and re-navigate to the page they had reached. Similar frustration is caused when the links to the graphic version that are provided throughout the text version also all lead to the home page. It is much more helpful and usable if links pointed directly to the appropriate version of the page currently being accessed. So, for example, if the user is viewing the graphic version of the site map, it is more helpful if the "Text version" link on that page actually takes the user to the text version of the site map, rather than to the text version of the home page.

**Mark up list items correctly.**

Coding a list as a list (e.g. using 'ul' for a bulleted list or 'ol' for a numbered list) makes the structure of the content available to the user in a way that can help them understand the content better. When a list is actually coded using a layout table with each list item on a separate table row, and perhaps with a column just for bullet graphics, the actual structure of the information, while presented visually, can be obscured or lost for those who are not using a graphic browser.

Best practice is to code lists using the appropriate HTML code. CSS can be used to specify a desired bullet graphic for bulleted lists, rather than relying on the browser default bullets.

**Text-only versions can be useful, but should not be seen as a solution for an inaccessible site.**

Our policy is to discourage the use of text-only versions of a site, because in too many cases, that is seen as all that needs to be done to make a site accessible. This simply isn't true, and in fact the whole thrust of the WAI guidelines and our own recommendations are geared towards the creation of a single site which is accessible to all users. Historically, text-only versions have also presented problems - they often don't contain all of the same content or functionality as the graphic version of the site, or the content gets out of date and isn't updated as frequently as the content in the graphic version.

Having said that, however, it is true that some of these problems are addressed by the introduction of content management systems and dynamic server-side scripting, which can present the same content in different formats as required. Where such systems are used, a text-only version of a site can be a useful "added value" feature which is made
available to users, but only as long as the graphic version of the site is also made fully accessible, so that users genuinely have a choice as to which version they use, rather than being forced to use one version or another.

When planning the creation of a text-only version of a site, thought needs to be given to the relationship between the graphic version and the text-only version. For example, content which might be relevant in the context of the graphic version (such as "Please refer to the graph below") may have no relevance, and may even be confusing, when presented in a text-only version.

It is also important to take account of the fact that, usually because of the problems historically associated with text-only versions, many users see a text-based version as exclusive rather than inclusive; they want to use the same site and have equal access to the same information as everybody else. A graphic site built with accessibility in mind should be able to achieve this.

**Provide a text based site map.**

A site map is an invaluable tool for all users, particularly on large and complex sites. It helps the user to understand the structure of the site, to orient themselves within the site, and to find the page or information they want, quickly. If it is not in text format, however, it may not be accessible by all users. Headings and nested lists can be used to create clear, easy to understand text-based site maps.

**Make links easy to find.**

Some links are easy to find because they are grouped together in menus on the page. Links which are embedded within the body of the page content, however, need to be clearly indicated in some way. If they are not, users may not realize that they are there, or are forced to hunt for them, making the page and the site that much more difficult to use. The use of color, bold text and underlining can help to ensure that these links are easy to spot, and will be appreciated by users. In particular, the use of underlining is so well known and recognized as an indicator for link text, that it should only be dispensed with after serious consideration. If you are thinking of formatting these links to remove the underlining, you should consider providing users with the option of turning it back on if they wish. While graphic browsers generally offer this as an option, this is still not fully functional and so cannot be relied on. For example, Internet Explorer provides the option for users to specify that links should always be underlined, but this currently will not override the 'text-decoration: none' CSS style.

**Use Cascading Style Sheets (CSS) for all visual formatting.**

Browser support for CSS grows with each new version that is issued, and is now sufficiently robust to make it feasible to drop the use of HTML formatting code, and use CSS for all visual formatting.

The use of CSS for all formatting brings several benefits:

- Future redesigns become much quicker and simpler, since it should only be necessary to change the style sheet being used, rather than change the HTML code on every page.

- The site becomes much more likely to display adequately on a wide range of technologies, rather than different versions being required for each new technology as it emerges.

- And it offers the possibility of being able to offer a wide degree of user personalization in terms of how the site is presented to them - several styles of presentation can be offered in the form of a range of different style sheets.

**Be consistent in how links are presented.**

Keep the navigation features in the site as consistent as possible. This will aid users in becoming confident about being able to find their way around the site. Site and section navigation menus should be in the same position on each page, and should function in the same way across the whole site. If links are provided to documents in formats other than HTML (e.g. PDF files, Word documents, etc), the link text should have a consistent format. For example: "Document title (format, file size)".