SCOPE: This standard applies to web applications (excluding SharePoint) developed or maintained by staff or consultants employed by or contracted with the Office of Information Technology. Reports (output with the intent of printing) and Exports are not addressed in this standard.

STRUCTURE: Standards are listed with numerical references. (Example: Standard 1.2). Supporting Details are included after each standard. These supporting details provide some Best Practices that Application Services developers have learned over the years. It also includes references, links and techniques that can be used in conjunction with the referenced standards.

STANDARD

1. Accessibility

1.1. All web applications must meet the standards established in Florida Administrative Code Rule Chapter 60-8.
1.2. All web applications must link to an Accessibility Statement.
1.2.1. A generic Accessibility Statement is available at the root of each application server. (AccessibilityStatement.htm)
1.2.2. Applications requiring additional accessibility information must create an application specific Accessibility Statement.
1.2.3. Applications using the standard Internet header and footer are covered by the Accessibility Statement found under the Web Policies and Notices link.
1.3. All web applications must provide a systematic method of installing additional software needed for the application to function.
1.4. If additional software is required to access content, provide a link on that page to a downloadable version of the software on the vendor's site.

SUPPORTING DETAILS - Section 1

Florida Administrative Code Rule Chapter 60-8 requires all State Agencies be compliant with accessibility standards based on Section 508 of the Rehabilitation Act of 1973.

SUPPORTING DETAILS – Section 1.3 and 1.4

Applications must provide easy access to the software required to view/use the content being provided. We should not expect our customers to have to search for required software when we already know where they can find it.

It is also a requirement of Florida Administrative Code Rule Chapter 60-8.002 (b) 13 that when a "web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with rule sub-subparagraphs 60EE-1.002(1)(b)1.-12, F.A.C."

Reference: **Accessibility Links** http://www.fdot.gov/agencyresources/webpoliciesandnotices.shtm

2. Fonts and Colors

2.1. All text, other than error and warning messages, must use the default hexadecimal font color(s) provided in the standard application color palettes. The Color Palette is available on the FDOT Internet at http://www.fdot.gov/OIS/docs/standards/colorpalette-10252013.htm
2.1.1. Internet Applications must use the "FDOT" color palette.
2.2. Applications must only use colors from a single palette.
2.3. The allowed uses of font colors, body backgrounds, hyperlinks, logos and error messages are defined on the standard application color palette.
2.4. Any design elements must have a WCAG 2 Level AA contrast ratio.
2.5. All error and warning messages (except for modal dialog boxes) must use the red (#FF0000) font color and be displayed on a white (#FFFFFF) background, or other background as allowed in your selected color palette.

2.5.1. The term **ERROR:** must precede the error message and render the font format of bold, red (#FF0000), and all caps.
2.5.2. The term **WARNING:** must precede the warning message and render the font format of bold, red (#FF0000), and all caps.
2.6. The font face must use the true type font family of "Arial, Helvetica, san serif" in the listed order. Unless monospace fonts are needed for alignment purposes, then the font family of "Courier New, Courier, Monospace" must be used.
2.7. Font size must fall within the ranges of Size 1 (8 point) and Size 5 (18 point).
2.8. Underline must not be used for anything other than hyperlinks.
2.9. Fonts must not blink.
2.9.1. Do not use the BLINK or MARQUEE elements. These elements are not part of any W3C specification for HTML (i.e., they are non-standard elements).
2.10. Italics must not be used.

SUPPORTING DETAILS – Section 2.1 – 2.3

Using the standard Fonts and Colors ensures that all applications share a consistent or common look and feel. A color palette sampler application is available to staff with access to the FDOT Intranet at: http://tlbstws.fdot.gov/PaletteSamples.

SUPPORTING DETAILS – Section 2.5

Providing a standard format for Error and Warning messages will assist the user with identifying issues that arise during use of the application. Using red font alone would be a violation of Florida Administrative Code, Accessible & Electronic Information Technology (AEIT), Rule Chapter: 60-8.002(1)(a)9., as you would be using color coding as the sole means of conveying information. For this reason we require the message be preceded with either the term Error or Warning. An example that shows the proper formatting for an error and warning message can be seen below:

ERROR: The City and State fields have not been completed. City and State must be completed before continuing
WARNING: The City and State fields have not been completed. Your application will be processed faster if City and State are completed

Generic Error Pages are expected to follow this standard.

SUPPORTING DETAILS – Section 2.6

Font Family defines the fonts that the text should be displayed in. If for some reason the Arial font is not available on the user's PC, the next available font in the family will be used to display the text. Using a set Font Family provides consistency across each file of the application. The Arial, Helvetica, san serif fonts are most commonly found on people's computers, and are easy to read both in the browser and in print.

The Courier New, Courier, Monospace fonts may be used when alignment of text is needed. A monospace font displays like a typewriter font meaning that all characters use the same width.

SUPPORTING DETAILS – Section 2.4

Information on understanding the WCAG 2 Level AA contrast ratio requirements see:
http://www.w3.org/TR/UNDERSTANDING-WCAG20/visual-audio-contrast-contrast.html

SUPPORTING DETAILS – Section 2.7

Limiting the font size range provides consistency across the various applications. Fonts that are smaller than the listed limit can be hard to read to users with your most basic vision problems. Fonts larger than the listed limit take up more room than needed to convey the message. The fonts should be used consistently throughout your

application. (i.e., the contact information found in the footer of each page should use the same font size(s).) Remember to keep it consistent.

SUPPORTING DETAILS – Section 2.8

Users commonly associate underlined text with a hyperlink. Restricting the use of underline to hyperlinks ensures that hyperlinks are easily recognizable and plain text is not mistaken for a hyperlink.

SUPPORTING DETAILS – Section 2.9

Not all browsers support the html <blink> tag. Techniques from "WAI Guidelines: Page Authoring" provided by the W3C provide the following information:

Avoid blinking: Technique A.7.3 Authors should avoid creating motion and blinking in a page where possible; blinking may cause seizures in some users and is annoying to many other users. They should also provide a mechanism for freezing motion. If style sheets are used to create an effect (e.g., 'text-decoration: blink'), users may cancel the effect through style sheets as well.

Reference: **WAI Guidelines: Page Authoring** http://www.w3.org/WAI/GL/wai-gl-techniques-19980918#style

SUPPORTING DETAILS – Section 2.10

Italicized text is not always easy to read. Emphasize text by rendering it as BOLD, or by setting the font weight to BOLD.

3. **Links (Hyperlinks, Images, Buttons)**
   - 3.1. A text hyperlink must not extend beyond the element to which it is related.
   - 3.2. Hyperlinks to downloadable files must include a text description that includes the file size and file type. If the resulting file size varies because the file is created on-request, then it must be stated that the file size is unknown.
   - 3.3. The destination of every hyperlink must be identified with descriptive text.
   - 3.4. Text hyperlinks not within the easily identifiable Navigational Menu must adhere to the following:
     - 3.4.1. Underline must not be disabled.

SUPPORTING DETAILS – Section 3.1

Hyperlinks that extend beyond text elements look to be made in error.

Examples:
Correct: We can find many examples of the FDOT logo. An example can be seen by visiting our FDOT Website.
Incorrect: We can find many examples of the FDOT logo. An example can be seen by visiting our FDOT Website.

SUPPORTING DETAILS – Section 3.2

Text descriptions provide information to the customer to ensure they have the proper software to view the file, and that they know when they may be attempting to download a file that is too large for their connection speed.

Example: Please review the FDOT Organizational Chart (PDF, 45.6 KB)

SUPPORTING DETAILS – Section 3.4

This standard provides screen readers and other assistive technology the information needed to convey the destination of the hyperlink to the customer. Screen readers will read the words as written, and will reference any

hyperlinks within the text. Hearing the words “Click here” followed by a URL is not as informative as hearing “FDOT Website” followed by a URL.

Examples:
Correct: We can find many examples of the FDOT logo. An example can be seen by visiting our FDOT Website.
Incorrect: We can find many examples of the FDOT logo. Click here for an example on our FDOT Website.

4. **Performance and Responsive Design**
   - 4.1. All requested content must be received by the browser within 10 seconds of the user action.
   - 4.2. All requested content received as a result of a user action must not exceed 150,000 bytes, excluding the following:
     - 4.2.1. WebResource.axd files
     - 4.2.2. Cascading Style Sheets
     - 4.2.3. JS Files implemented as Include Files
   - 4.3. All web applications must provide a responsive design.
     - 4.3.1. Web Applications are expected to render and function in a screen width range of 420px to 2304px.
     - 4.3.2. Application elements cannot overlap, unless the behavior is standard between all screen resolutions.
     - 4.3.3. Data grids may horizontally scroll, but an alternative way of viewing the entirety of the data must be provided.
     - 4.3.4. Full site navigation must be available throughout screen resolution changes.

SUPPORTING DETAILS – Section 4 through 4.3
Performance: The intent of this standard is to ensure that each user has a reliable experience in the load time of the web page. **Developers should keep in mind that a 10 second load time represents the maximum.** Developers should target response times in the sub second – 2 second range for the majority of their pages. Additionally, by keeping the requested content size within 150,000 bytes, we can provide a reasonable load time even if the user does not have broadband connectivity. Performance is one of the areas that OIT has identified as important for continued customer service and support in our OIT Business Plan.

WebResource.axd, Cascading Style Sheets and .JS Files are excluded because they are cached by the browser and are usually considered a necessary contribution to the page size.

Fiddler may be used to ensure compliance with the Performance standard. It is an approved Application Services download. Fiddler provides download time estimates for various data connections (elapsed time & round trip). Your application should be tailored to the target audience’s connection speed.

Responsive Web Design makes your web page look good on all devices (desktops, tablets, and phones). Responsive Web Design is about using CSS and HTML to resize, hide, shrink, enlarge, or move the content to make it look good on any screen.

Any multimedia embedded within an application is subject to any applicable Multimedia Standards.

5. **Printing**
   - 5.1. Pages must not override the browser’s print function. (See Section 13.4).
   - 5.2. Customized printing (“printer friendly” pages) should not interfere with the browser’s print function.
     - 5.2.1. Applications choosing to use an icon to represent a “printer friendly” print option must use the standard printer friendly icon. (See Section 6)

6. Graphics

6.1. The following logos and graphics must be placed in their needed location using relative addressing to their location on the root of the server(s). These images are located in the Image folder on the root directory of all UNIT, SYSTEM and PRODUCTION servers.

6.1.1. FDOT Logo (FDOTlogoBlackLg.png, FDOTlogoBlackSm.png, FDOTLogoGrayscaleLg.png, FDOTLogoGrayscaleSm.png, FDOTLogoLg.gif, FDOTLogoLg.png, FDOTLogoSm.gif, FDOTLogoSm.png, FDOTLogoWhiteLg.png, FDOTLogoWhiteSm.png, FDOTLogoWhiteTransLg.png, FDOTLogoWhiteTransSm.png)

6.1.1.1. FDOT logo options can be viewed at http://tlbstws.fdot.gov/FDOT-Logo-Images.htm.

6.1.2. Printer Friendly Icon (filename: print-icon.gif)

SUPPORTING DETAILS – Section 6

The use of common images contained in a centralized location allows the developers to always have access to the most current and correct version of each logo. Additionally, if a logo should change, a centralized location allows the update to occur in one place with little or no impact to the applications. It is the intent of this standard that the images be used, as provided, without being resized or altered by any means.

7. Animation

7.1. Do not use blinking or moving fonts.
7.2. Do not use animated images.
7.3. Do not create the simulation of movement by repositioning images in a web page.
7.4. Do not create the simulation of movement created by displaying a series of pictures, or frames.

SUPPORTING DETAILS – Section 7.1

Blinking fonts or moving fonts, animated images, and simulation of movement are not generally seen as necessary within a Business-related or Enterprise Level application. For this reason, Application Services has chosen to disallow their use. Contributing factors to this decision include:

a) Section 508, Subpart B, §1194.22(j) requires that “pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz”
b) The flicker rate is cumulative; therefore multiple moving graphics would increase the Hertz rate of the page.
c) Animated graphics add unneeded weight to the page and could cause problems with adhering to Application Services’ File Size standards listed in Section 4.1.

8. Copyright and Attribution

8.1. Never use text, diagrams, photographs, audio, multimedia, program source code, script or graphics from another author’s web pages unless the author explicitly states it may be freely copied or you make appropriate arrangements with the author.
8.2. When copying or paraphrasing information from another source, always make an appropriate attribution.
8.3. Placement of credit lines for text or article should be at the end of the source or article
8.4. Never hyperlink deep-links to material from another web site or on commercial web sites without giving credit. A deep link is a hyperlink that bypasses a website's home page and takes the user directly to an internal page.
8.5. Vendor logos, branding, or other company endorsements must not appear anywhere in a web application, visible or otherwise.

SUPPORTING DETAILS – Section 8

Copyright is the legal right granted to the owner of the copyright to distribute, make derivative works, or show in public the product of their work. The "work" includes software which is considered to be copyrighted in most countries by default even if it does not contain the copyright symbol identification.

Because the technology of websites allow direct links to a particular web page URL, we must pay attention to the page being linked to in order to ensure that credit is given to information shown by external authors. The credit for the work may have been given on the initial "home page", but when we directly link, we miss seeing the credit.

The programming work that we do for FDOT is considered the ownership of FDOT.

Best Practice:

a) Document, by using comments, the source of the program code when obtained from sources not within FDOT.

b) Deep links can be handled in a couple of ways: either consider linking directly to the page that gives attribution to the author, but then makes the user drill down to what you actually want them to see -OR- use an area of your web page or information boxes to give credit to what you are about to deep-link.

References: Dictionary.com basic definition of Copyright

9. **Internet Application Formatting**
   - 9.1 Internet Applications must implement the FDOT internet standard header, footer and color scheme as follows:
     - 9.1.1. All Internet applications must use the "FDOT" color palette. (See Standard 2.1.1)
     - 9.1.2. All Internet application pages that are available without login must use the FDOT internet standard header and footer. These are referred to as citizen-focused pages.
     - 9.1.3. The login pages for all Internet applications must use the FDOT internet standard header and footer.
     - 9.1.4. Internet application pages that are available after login are not required to use the FDOT internet standard header and footer, but may use them if they choose.
     - 9.1.5. Applications using the FDOT internet Standard Header and Footer are considered to have met all requirements related to Header and Footer.
     - 9.1.6. Applications that do not use the FDOT internet standard header and footer must adhere to Standards 10. Header and 11. Footer.

SUPPORTING DETAILS – Section 9

In 2013 the Department's Internet presence was redesigned. This created a consistent look and feel for all Internet content. Applications that do not require a login are considered "citizen focused". While they may be applications, the application user is simply using the site as a way of getting information. The user does not see a difference between a static page and an application. For this reason, citizen focused Internet applications must adhere to the same standards required for Internet static sites. This includes mandatory headers, footers and color schemes. The mandatory headers, footers and color scheme cannot be changed. The step of logging on gives the user an indication that they are using something more detailed than a static page. Because of this, Internet applications that require login are not required to use the standard header and footer, but are required to use a similar color scheme.

10. Header
- 10.1. A page header is required on each page.
- 10.2. The header must include but is not limited to the following:
  - 10.2.1. Application Identifier
  - 10.2.2. A link to application or page level help, with the exception of the actual Help Pages.
  - 10.2.3. (Internet) The FDOT Logo or the text/image of the words "Florida Department of Transportation" must be located in the top left corner.

10.3. (Intranet) If the FDOT Logo is used, it must be located in the top left corner of the header (see Section 6 Graphics). The FDOT logo is not required.

11. Footer

11.1. A page footer is required on each page.
11.2. The footer must include but is not limited to the following:
11.2.1. Service Desk contact information must be centered in the footer. If a Mail To link is included, provide a subject for the email that includes the Application Name.
11.2.2. (Internet) A link to MyFlorida.com.
11.2.3. A link to the Department's Web Policies and Notices located at http://www.fdot.gov/agencyresources/webpoliciesandnotices.shtm must be centered in the footer
11.2.3.1. The text for this link must be "Web Policies and Notices".
11.3. A link to an application specific Accessibility Statement may be used. If used, it must be centered in the footer.

SUPPORTING DETAILS – Section 10 & Section 11

The use of Headers and Footers provides the user with a consistent experience for all OIT developed applications. End Users learn that certain information can always be found in the Header and Footer.

It is acceptable for the Application Identifier (Section 10.2.1) to be displayed as text or graphic.

Standards relating to the placement of logos (Section 10.2.3) support the idea that OIT developed applications will be "branded" in a certain way.

12. Approved Software

12.1. The only products approved for OIT web page application development are below. Deliverables produced externally must be compatible with the following:

	Product	Purpose
12.1.1.	SharePoint Designer 2007	Classic ASP Code Maintenance
12.1.2.	Web Focus	Web Focus Reports
12.1.3.	MRE	MRE Reports
12.1.4.	Visual Studio .NET	.NET Development Tool
12.1.5.	OpenText DM	Electronic Document Management

SUPPORTING DETAILS – Section 12

Identification of a standard set of languages, tools and technologies for use by Application Services programmers allows staff to maintain multiple applications. The decision to adopt new approved software is made by Application Services and coordinated by others throughout OIT, so that we can ensure all tools fit within the enterprise and are supportable over the long term.

13. **Coding Methods and Techniques**

13.1. Frames must not be used.
13.2. Query Strings must be URL encoded.*
13.3. URLs must not exceed 255 characters.
13.4. You must not disable the browser features.
13.5. Absolute URLs must be fully qualified.*
13.6. Confidential data that is passed within or outside of the application must be encrypted.*

*****These standards are checked via the Web Application review for ASP applications and in the .NET code review for .NET applications.

SUPPORTING DETAILS – Section 13.1

Frames present a number of difficulties including:
a) Bookmarks do not work as you would expect; you can bookmark the top-level (frameset) page, but not necessarily what is displayed on your screen.
b) Frames do not usually print the way the screens look.
c) It is difficult to restyle content within frames since even simple restyling like increasing text size often results in clipping or the need for horizontal scrolling.
d) It is difficult for users utilizing voice recognition software to determine what potential changes will occur to all frames when they select a link in one particular frame.

Reference:
University of Illinois at Urbana/Chicago, Campus Information Technologies and Educational Services and Disability Resources and Education Services. http://html.cita.uiuc.edu/nav/frame/

SUPPORTING DETAILS – Section 13.2

Certain special characters have meaning when contained in a query string (spaces, ?, =, &, etc.) and may cause problems for a browser if they are not being used for their intended purpose. To be able to safely pass these characters in a query string, the string must be URL encoded. Both ASP and ASP.Net have built-in function that will encode strings for you.
For ASP use the Server.URLEncode Function
For ASP.Net use the System.Web.HttpUtility.UrlEncode Function

Unencoded string example:
Omar Shaikh <omar.shaikh@dot.state.fl.us>

Encoded string example:
Omar+Shaikh+%3comar.shaikh%40dot.state.fl.us%3e

SUPPORTING DETAILS – Section 13.3

Certain older browsers and handheld devices cannot handle URLs that exceed 255 characters. This standard ensures that all users, regardless of browser type, can access URLs generated by our applications.

SUPPORTING DETAILS – Section 13.4

People have an expectation of how a web browser will be setup. Users expect to have a home button, back and next buttons and an address bar. We want to give users the browser functionality they are accustomed to.

This is also an Accessibility courtesy. Users with disabilities often need to change browser settings such as font size and color. Altering the web browser setup takes away their ability to make those changes.

SUPPORTING DETAILS – Section 13.5

This standard ensures that links are usable by all users, including district, handheld and VPN users.

SUPPORTING DETAILS – Section 13.6

Confidential data is defined in Chapter 71A-1 (Security Policies and Standards), F.A.C. as “Information not subject to inspection by the public that may be released only to those persons and entities designated in Florida statute; information designated as confidential under provisions of federal law or rule.” Most data passed between pages is sent using either a GET or POST which puts the data in the query string or in the http request header, neither of which is secure. Sending data in this manner is highly susceptible to being read or tampered with. Encrypting the data before it is sent prevents this since the data is meaningless until it is decrypted and cannot be tampered with.

FDOT Enterprise Library Data Marshaller Component may be used to pass and encrypt data between applications.

14. Naming Convention (this includes directory and file names as they appear in the browser)

14.1. Do not use spaces.

14.2. Do not use underscores.

SUPPORTING DETAILS – Section 14.1

Some browsers interpret spaces in file names as "%20". Cutting and pasting of URLs with a file name that includes spaces can results in problems for application users.

SUPPORTING DETAILS – Section 14.2

Underscores can easily get lost within a hyperlink. The hyperlink hides that fact that there is an underscore separating two parts of the URL. When people try to retype the URL they can mistakenly put in a space instead of the underscore.

Best Practice:

- If you must visually separate a two-word file or directory name, use a dash (hyphen) rather than an underscore.

15. **New or Separate Browser Instances**

15.1. A TITLE attribute must be used to indicate the link will open another instance of the browser. The attribute value must include the text "**Opens new browser window".** Additional descriptive text may be included if desired.

SUPPORTING DETAILS – Section 15.1

Although modern screen readers and some web browsers alert users when a link opens a new browser window, old screen readers and some browsers do not. Users with cognitive disabilities may not be able to interpret what happened when a new browser window is spawned.

Reference:
UIAccess.com – Resources for Accessibility http://www.uiaccess.com/spawned.html#wcag

Web Content Accessibility Guidelines 1.0 http://www.w3.org/TR/WCAG/

16. Security & Authentication

16.1. Web Applications requiring authentication must use the login method approved for their development platform. These include:

16.1.1. OpenText DM Applications: Login is authenticated against the OpenText DM Server.

16.1.2. Intranet Web Applications:

16.1.2.1. Login is authenticated against RACF using the Standard Security Module invoked either by the Common Login for ASP or the FDOT Enterprise Library Authentication Component for ASP .NET.

16.1.2.2. Login is authenticated against Active Directory using LDAP.

16.1.3. Internet Web Applications:

16.1.3.1. The Security Disclaimer must be displayed as part of the authentication process.

16.1.3.2. Login is authenticated against RACF using the Standard Security Module invoked either by the Common Login for ASP or the FDOT Enterprise Library Authentication Component for ASP .NET.

16.1.3.3. Login is authenticated against the Internet Subscriber Account (ISA) system using the Standard Security Module invoked by the FDOT Enterprise Library Authentication Component for ASP .NET.

16.1.3.3.1. Only non-DOT staff may be authenticated using ISA.
16.1.3.3.2. The ISA Terms of Use Agreement signature control that is provided by the FDOT Enterprise Library must be incorporated.
16.1.3.4. Applications that require authentication must use Secure Sockets Layer (SSL) and disable HTTP access.
16.1.4. Single sign-on
16.1.4.1. Authentication must be established using one of the standard designated methods (as listed above).
16.1.4.2. The FDOT Enterprise Library Data Marshaller Component must be used to pass authentication credentials between web applications.

SUPPORTING DETAILS – Section 16

Standardizing the method of Authentication ensures that users are authenticated against safe, reliable and maintained authentication end points. These authentication sources are also those approved by the IT Assurance and Security Management (ITASM) Office. This is especially critical when it comes to applications hosted on the Internet. OpenText based applications use their built in data stores for authenticating users. For Intranet hosted applications written in ASP or ASP.NET, RACF and Active Directory are the only approved methods. Active Directory authentication is not currently available for Internet Applications.

Applications that require authentication via the Internet by something other than RACF should utilize the Internet Subscriber Account (ISA) System. ISA includes a standard Terms of Use (TOU) document that explains how ISA is used and the subscriber's responsibility. It is required that the subscriber acknowledge that he/she has read and agrees to the TOU.

Computer software and/or hardware can intercept and log traffic passing over the Internet. To help reduce the risk of sensitive information being intercepted and interpreted, Secure Sockets Layer (SSL) is used to encrypt the contents of the HTTP transactions.

The FDOT Enterprise Library Data Marshaller Component provides the required encryption of confidential and sensitive data between applications.

17. Browser Compatibility

17.1. Web applications must be compatible with the version of Internet Explorer currently used in FDOT's standard desktop installation, along with the latest release of Internet Explorer. In addition, they must be compatible with the latest release of Chrome, Firefox, Edge, and any other browsers required to support the application's user base.

SUPPORTING DETAILS – Section 17

Chrome, Firefox, Edge, and Internet Explorer are the most commonly used browsers. For this reason, Internet applications must be compatible with all of these. Internet Explorer is the department's standard web browser, so Internet applications written to the version of Internet Explorer currently used by FDOT will work correctly for Intranet users.

STANDARDS CHANGES, EXCEPTIONS AND COMPLIANCE

Requesting an exception or change to the standards.

1. Project Teams may request exceptions or change to the standard.
2. The exception or change requests must be provided, in writing, to the Application Services Quality Assurance Specialist by the OIT Application Coordinator of the Project. The request must include:
   2.1. Standard(s) for which they are requesting the exception or change.
   2.2. Business case justifying why the exception or change is needed.

2.3. Technical details of the non-standard implementation or the change being proposed.
2.4. Impact to the department for the exception or change.
2.5. List alternatives considered with pros and cons of each alternative.
2.6. Provide justification of why requested exception was the chosen alternative.
3. The request for exception or change will be reviewed by a team assembled by the Application Services Quality Assurance Specialist.
4. The review team will provide a written recommendation to the Application Services Manager.
5. Final decision will be determined by the Application Services Manager.

SUPPORTING DETAILS – Requesting Exceptions or Changes

The Application Development arena is constantly changing. The Application Web Standards must also change to meet the needs of our growing Application Development community. The process for requesting exceptions or changes is the method by which the Application Services Web Standards group is made aware of the possible need for changes (temporarily – as an exception, or permanently – as a standards change). Exception requests should be processed as soon as they are recognized in the Project. Project Teams requesting changes/exceptions are required to provide the listed documentation to assist in the research and understanding of their particular situation.

Compliancy Refresh
When an enhancement release is scheduled on the Application Services Work Plan, part of the scope of work must include bringing the application into compliance with the latest version of the standards. If the application has any previously granted exceptions, they must now be addressed and made compliant with the documented standard.

When a Web Standards Review is conducted, the application will be reviewed under the identified Web Application Standard for the application as a whole.

SUPPORTING DETAILS – Compliancy Refresh
As technology changes, there is a need to continue to update the Web Application Standards. Generally, our Web Application Standards are updated a minimum of twice a year. The intent of this standard is to ensure that our applications are staying current with the recent standards. The Project Team has the option of being reviewed under the standard in place at time of review, or the previous standard. If an exception was previously granted, and the application cannot be remediated to the new standard, a new exception request must be applied for.