AIRS & Legacy Websites

WEBSITE CHECKLIST

Release Date: 1 May 2018

U.S Coast Guard Auxiliary
Information Technology Group
User Support & Services

Requirements (Must be Met)

1. Both the website's <title tag> and the caption at the top of the home page must identify the unit, division, and district as well as the geographic location of the unit. (e.g. U.S. Coast Guard Auxiliary Flotilla 1-8 Milton Florida District 8CR)
2. Use canonical unit numbers (e.g., 1-5, 7-3, 12-13, 3-15) to describe your flotilla. (Note: existing sites with traditional numbers such as "Flotilla 78" should try to upgrade as page changes are made).
3. When using photographs or graphic images, include an "alt tag" (i.e. alternative text) text identification with each image.
4. Check that your website displays correctly and consistently using IE 8 and above, Chrome (all), Firefox 3 and above, and Safari 4 and above.
5. The site shall not contain any commercial advertisements, nor appear to endorse any commercial product. Sites must not contain inappropriate information, including specific advice, endorsement or approval of a product or service, or sponsorship information
6. The site shall present a professional web appearance, and must not bring discredit or embarrassment to the Coast Guard or the Auxiliary.
7. Make sure your site does not include materials that infringe on the rights or privacy of an individual or violate copyright restrictions. (Note: Auxiliary websites are not copyrightable – any material may be copied from other Auxiliary web sites).
8. Make sure your site does not display the "official" Auxiliary or Coast Guard Seal. The Auxiliary logo is OK.
9. Make sure there is contact information for your unit on your website.
10. The site shall not contain any blank pages or under construction notices, and all links must be live (i.e., no dead links).
11. The site may not play auto-start music or video, nor display animated GIFs. Rotating slide shows (without audio) are acceptable.
12. All persons who have personal email addresses or phone numbers posted on any non-protected portion of the website must have given you written or email permission to post their information or they have opted in at AuxDirectory (AuxOfficer).
13. Any outside links must support Auxiliary objectives. Make sure they are in good taste and assure that they do not bring discredit to the Auxiliary.
14. Make sure your site limits access to sensitive information by implementing Member Zone password protection using a provided Aux Officer API kit. No private passwords systems are allowed.

15. Check and make sure your site does not violate Operational Security (OPSEC) guidelines, which are the same for protected as well as non-protected pages.
16. Make sure your site properly displays the NTAS and MARSEC threat level logos, pulled directly from the proper DHS locations. (Automatic if using the Auxiliary Templates). Logos may not be cached locally.
17. Make sure your site provides links to the national Website, and other relevant district, division, and flotilla websites.
18. Make sure your links to onsite material are permalinks (i.e. a7029.pdf vs. a7029H-Rev2.pdf).
19. Make sure you have parental permission for any pictures of minors displayed on the site, along with a signed copy of the CGAux Parental Release form.
20. Your site may provide links to the national Forms Warehouse, or to individual forms hosted on the Forms Warehouse, but may not copy any national form and host a static copy on your site. You may not post any locally developed forms meant for gathering data for AUXDATA entry.

Best Practices (Should be met)

1. Crop and reduce your photographs to their final size; do not resize them in your code.
2. Make sure none of your links to on-site materials contain embedded spaces.
3. If you have an *About This Unit* page, consider having at least one officer show a phone number or email address. This counts as "contact information" from the requirements above.
4. Alt tags should be descriptive, and generally kept to 50 characters or less.

National Approval of New Websites and Previously Unapproved Websites

In order to complete the formal National approval process in a timely manner, a time limit of one year will be imposed for all approval requests that need to have compliance issues addressed. The National IT staff will provide a 60-day notice to the contact person that the request for approval will be deleted at the one-year mark. After that time, the SNF (Site Notification Form) will be deleted and the approval process will have to be initiated anew.