Min. Hosting Requirements/Standards for all CMS Websites

Last Updated Feb 2020

# What We Will Host

RRCHNM commits to hosting the following types of websites, under the conditions laid out in the Server Sustainability Policy.

1. RRCHNM projects
2. RRCHNM-associated research projects
3. RRCHNM-associated teaching projects
4. Contracted projects under development
5. Contracted projects paying for hosting
6. Legacy projects

# Minimum Hosting Requirements

To be hosted on RRCHNM servers, all projects must ensure they (at minimum) adhere to these guidelines:

## General

1. finished projects must have documentation deposited in the Basecamp sustainability project, which includes the following information
   1. project contact(s)
   2. project purpose
   3. essential project functionality
   4. CMS/technical stack description
   5. external dependencies
   6. funders/grants list
   7. sustainability commitment given to funders/other legal entities
   8. email, social media, and GitHub accounts and project logins (as appropriate)
2. RRCHNM team members must have administrative access to the site
3. all user passwords must meet a minimum security standard of 8 characters and include 1 number or special character (e.g. not a dictionary word)
4. all sites must not be harboring malware
5. all sites must either meet WCAG 2.0 and Section 508 standards or provide justification for why portions of the site cannot be made completely accessible; alternatively, project owners can demonstrate that they are actively working towards making their sites as accessible as possible
6. new content must have been posted to the site within the past 12 months; sites that are not being updated at least once a year may be flattened at the senior staff’s discretion

## Drupal

1. all plugins must be deleted upon deactivation
2. all sites must be updated to the latest version of one of the recommended official releases of Drupal; sites that cannot be updated for more than 6 months are subject to being triaged or otherwise removed from RRCHNM servers

## Omeka and Omeka S

1. all plugins must be deleted upon deactivation
2. all sites must be updated to the latest version of Omeka or Omeka S; sites that cannot be updated for more than 6 months are subject to being triaged or otherwise removed from RRCHNM servers

## WordPress

1. install a plugin to protect against brute force attacks, with a minimum configuration of: 10 failed logins leads to a 24-hour ban
2. install a plugin to block XML-RPC, unless specifically arranged otherwise
3. install a plugin to manage spam comments or use built-in WordPress functionality to disable comments by default
4. while not required, all site creators should give serious consideration to changing/restricting access (to specific IPs or network) the wp-login and wp-admin URLs
5. neither “admin” nor the URL of the website may be a user account name; users attempting to login with either word as a user account name should be blocked
6. users must log in with email and password, not user account name and password
7. all plugins and old themes must be deleted upon deactivation
8. all sites must be promptly updated to the latest versions of the Wordpress core install, plugins, and themes; sites that cannot be updated for more than 6 months are subject to being triaged or otherwise removed from RRCHNM servers
9. Weekly scan of all websites (WordFence plugin recommended) to ensure file integrity and malware checks