August 23, 2017

NOAA GitHub.com Usage Guidelines

PURPOSE

This document provides the National Oceanic and Atmospheric Administration (NOAA) with guidance for how to use GitHub. NOAA allows use of GitHub to share code and content in the spirit of collaboration and open government. This guidance covers the accounts of NOAA employees and their use of GitHub.com.

OTHER POLICIES AND GUIDANCE

All official activities online are subject to applicable Federal law, ethics regulations, and agency policies. Existing policies and guidance for accessibility, privacy, external site links, cookies, and writing style apply to GitHub and other social media tools as well. GitHub use must comply with the Department of Commerce Policy on the Approval and Use of Social Media and Web 2.0.

WHAT IS GITHUB?

GitHub is a third-party website that offers code repositories that developers can use to collaborate on software development projects in real-time. Many users also use GitHub to publish and track documents, such as style guides and policies. In addition, GitHub provides social networking features that allow developers to follow open source projects, share code, and learn how code changes are made throughout the development process. The public can submit suggested changes to a developer's content that the developer can accept and integrate. GitHub is so named because it uses the open source version control system called Git.

ACCEPTABLE CONTENT

Users should refer to the authorization memo from the NOAA CIO for more details regarding the type of content that is acceptable for posting on GitHub. Users should confirm with their senior management official if they have any questions or concerns regarding the appropriateness of the public release of their specific content.

NOAA ORGANIZATIONAL ACCOUNT ON GITHUB

NOAA has created an organizational account with GitHub (@NOAAGov), which allows an unlimited number of public repositories. NOAA staff interested in using GitHub to post content may create their repository within this NOAA account. Repositories that are not created within the NOAA account but which are contributed to by NOAA staff must be registered with the @NOAAGov "NOAA Affiliated Projects" repository, by adding the repository name, description, and GitHub address to the README.md file of this repository. If users need access to this file or have questions regarding the process of registering their repository, they should contact their respective NOAA GitHub administrator.

All @NOAAGov users of GitHub shall utilize a different password than that associated with any NOAA Account (NEMS, ICAM, etc.) and utilize dual-factor authentication. Ensure all GitHub users are properly assigned by role and function and receive proper rights/permissions.

ROLES AND RESPONSIBILITIES

Roles[1]:

- **General User** – a GitHub user that does not have permission to post content.
- **Team Member** – NOAA-specified representatives that can post NOAA content on GitHub.
- **Team Member Sponsor** – A federal employee team member's direct supervisor, who is responsible for monitoring their employees' accounts, or a contractor's or grantee's government sponsor.
- **Contribution Reviewer** – Team member that shall review and either accept or reject a pull request on NOAA GitHub repositories.
- **Repository Owner** – the NOAA representative that is responsible for a NOAA GitHub repository; the repository owner may work on one repository or a group of repositories.
- **Information Owner** – often a project's Principal Investigator, the individual in a scientific organization that owns the data; they must provide permission to post NOAA data to a GitHub repository; appoint or utilize an existing Repository Owner.
- **System Owner** – a federal employee responsible for leading mission-unique services. Ensure IT systems possess current end FISMA-compliant Authorization and Accreditation documentation packages.
- **NOAA GitHub Administrator** – An NOAA representative who monitors the repositories on NOAA's GitHub account and is responsible for conducting scans and audits of all NOAA owned repositories.

Other Responsibilities:

- **Team Member Sponsor:**
    - Complete the NOAA GitHub Checklist annually

[1] Unless otherwise specified, these roles can be filled by either a NOAA Federal employee or a NOAA Affiliate

- **Team member:**
  - Enable two-factor authentication for their GitHub account which is registered to their NOAA-affiliated e-mail
  - Comply with the DOC social media policy
  - Request access from the Information Owner
  - Agree to the NOAA and DOC acceptable use policies
  - Agree to the access and release policy established by the Information Owner
  - Complete the NOAA GitHub Checklist annually

- **Repository Owner:**
  - Ensures that repository content contains no proprietary code or information, based on information provided by the NOAA GitHub Administrator.
  - Confirms that there is no PII or BII included with the content, nor any information that would allow access to PII or BII.

- **Information Owner:**
  - Comply with the DOC social media policy
  - Authorize all access to the repository
  - Maintain a list of everyone that has access to the repository and review at least annually
  - Review all published code
  - Ensure repositories are replicated back to a NOAA FISMA system and a copy of the model data is maintained for 1 year
  - Agree to the NOAA and DOC acceptable use policies
  - Establish a access/release policy for this repository
  - Sign the risk assessment memo
  - Complete the NOAA GitHub Checklist annually

- **NOAA GitHub Administrator:**
  - Monitors, scans, and conducts audits on all external repositories on NOAA's GitHub account and on the internal NOAA repository
  - Maintains a "gold copy" of all repositories in the internal NOAA repository

ADMINISTRATIVE AND WRITE ACCESS

NOAA federal employees may be repository owners with administrative level rights, giving them the ability to create repositories and assign team members to GitHub projects under the NOAAGov organization. Both NOAA federal employees and authorized contractors may be team members able to contribute content to existing NOAA repositories. Under no circumstances may non-Department of Commerce staff, unauthorized contractors, or members of the public become team members of repositories under the NOAAGov organization. NOAA uses GitHub in the spirit of Open Government, and allows the public to make pull requests, comment, and suggest edits. Pull requests are the heart of collaboration on GitHub; when GitHub members make a pull request, they are proposing their changes to the NOAA content and requesting that NOAA "pull" in their contribution. Those changes do not become part of the content until and unless the NOAA team that is responsible for the project performs a review and approves the

suggested changes, including an assessment of scientific value and a successful security scan.

SCIENTIFIC COLLABORATION WITH NON-DEPARTMENT OF COMMERCE INDIVIDUALS

NOAA has a strong history of scientific collaboration, coordination, and close engagement with other government partners, non-government organizations, academic institutions, international colleagues, and other members of the scientific research community. The guidelines provided in the previous section apply only to the NOAAGov GitHub organizational account and any repositories created under that account.

SUPPORT

It is expected that any NOAA organization publishing content on GitHub.com will facilitate access to the GitHub.com tool from NOAA resources, and to support users, team members, repository owners, contribution reviewers and administrators that support the publication of NOAA owned software or data on GitHub.com. This includes working with NOAA GitHub Administrators on providing documentation on permissions and postings to github.com, facilitation of security scans to NOAA owned repositories, and other responsibilities as outlined above.

APPROVAL STEPS

- Team Member gets approval from their Sponsor to proceed.
- Repository Owner creates a GitHub repository. All Team Members must register with their work email and should maintain independence from any personal activities and accounts they may have on GitHub.
- Team Member obtains written approval from the Information Owner of the NOAA software or code that they want to put on GitHub (in most cases, the Information Owner will be a Team Member). Approval from the Information Owner ensures that NOAA allows the information to be placed on GitHub public repositories for collaboration, public comment, and public use.
- In addition to the initial approval from their Sponsor, Team Members and their Sponsor should agree on a plan and schedule for regular updates and notification of activities on GitHub. In an ideal situation, the Team Member's Sponsor would have an account on GitHub and 'watch' the user's projects. In most situations, however, a quarterly update to their user to their sponsor should suffice.

POSTING NOAA CONTENT TO GITHUB PUBLIC REPOSITORIES

The NOAAGov GitHub account can be used to publish NOAA software, design patterns, style guides, documents, and code related to scientific products and research as open source, making the content available for external developers to fork and build upon for their own projects.

External developers can also help the project by commenting on their content with suggested improvements and questions. In order to follow the Department of Commerce's Social Media Policy, data and software code posted in a public repository on GitHub must be available on DOC's public website or a DOC bureau's public website. If a Team Member is publishing to a public repository on NOAAGov's main GitHub account, then they must download a quarterly copy of that content from the GitHub repository and publish it on the public DOC or DOC Bureau's website after appropriate review and scanning.

Before posting content, an employee must ensure that any content created by a NOAA contractor has been released to NOAA and the contractor does not claim any rights to the content. It is the Repository Owner's responsibility to ensure code in their repository contains no proprietary code or information. Failure to do so could lead to legal ramifications for the project and the Department. Project plans must include quarterly download and publication for every quarter that there are changes made to the GitHub repository.

All projects posted to the NOAAGov GitHub public repository must include a link to the location where the project code resides on the DOC or DOC bureau public website, as well as the following disclaimer in a README file:

"This repository is a scientific product and is not official communication of the National Oceanic and Atmospheric Administration, or the United States Department of Commerce. All NOAA GitHub project code is provided on an 'as is' basis and the user assumes responsibility for its use. Any claims against the Department of Commerce or Department of Commerce bureaus stemming from the use of this GitHub project will be governed by all applicable Federal law. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation or favoring by the Department of Commerce. The Department of Commerce seal and logo, or the seal and logo of a DOC bureau, shall not be used in any manner to imply endorsement of any commercial product or activity by DOC or the United States Government."

INTERNAL "GOLD STANDARD" COPY OF CONTENT

All NOAA generated content published externally on GitHub must also reside on a NOAA-controlled server within a NOAA boundary. This ensures that a "gold standard" copy of all content is maintained, to which only NOAA users have access. External submissions should be incorporated into the internal NOAA repository only after careful review and testing by the Information Owner and a scan by a NOAA GitHub Administrator.

SECURITY SCAN WITH GIT-SECRETS

The git-secrets plugin for git provides an easy means of automating a security scan when content is added to the user's repository. The installation and implementation of the git-secrets plugin is required with all repositories published on GitHub.

NOTIFY NOAAGov GITHUB ADMINISTRATORS

After users have published their content to a NOAAGov GitHub repository, they should notify one of the NOAAGov administrators so that they can monitor the user's repository and be

notified of updates. NOAAGov administrators will do this by selecting the "Watch" button at the top of the user's repository. All NOAAGov public repositories should be "watched" by NOAAGov GitHub administrators so that they appear on the administrators' dashboards; however, responsibility for ensuring that the repositories contain only acceptable content is assumed by the Repository Owner, not the NOAAGov administrators.

LICENSING AND MAKING AVAILABLE TO THE PUBLIC

Any code posted to a NOAAGov GitHub public repository must be accompanied by the following statement, in a LICENSE file in the repository:

"Software code created by U.S. Government employees is not subject to copyright in the United States (17 U.S.C. §105). The United States/Department of Commerce reserve all rights to seek and obtain copyright protection in countries other than the United States for Software authored in its entirety by the Department of Commerce. To this end, the Department of Commerce hereby grants to Recipient a royalty-free, nonexclusive license to use, copy, and create derivative works of the Software outside of the United States."

By publishing government content to a public GitHub repository, the Information Owner is making it freely available to the public for download and use. It is the Repository Owner's responsibility to ensure their code contains no proprietary code or information. Failure to do so could lead to legal ramifications for the project and the Department.

WHAT NOT TO POST ON GITHUB

When considering what content to post on GitHub, no distinction should be made between public and private GitHub repositories, regardless of ownership. GitHub private repositories are only meant to provide a closed environment for working projects not yet ready for public use and should never contain sensitive code. All NOAA projects hosted on GitHub should be suitable for public access and must contain no nonpublic information. For questions about the NOAAGov GitHub account or this guidance document, please contact one of the NOAAGov GitHub administrators.

FOLLOW FEDERAL REQUIREMENTS

Section 508

Social Media tools, like other web-based applications, whether inside the DOC network or in the other areas of the Web, must make every effort to comply with Section 508 and other policies on accessibility, privacy, and record keeping. In some rare instances, it's not possible to redesign an outside system to be accessible, but it's usually possible to link back to equivalent information on a DOC website. A DOC email address must always be visible on a DOC or DOC bureau GitHub site for users who require alternative methods of accessing the information posted.

Privacy Policy

The Department of Commerce's Privacy Policy applies to any DOC or DOC bureau GitHub site or repository.

Comment Policy

GitHub comments from and to the public will adhere to DOC's Comment Policy.