Third-Party Access Request Form

In order to access SDP's 3rd Party Web Applications like Confluence, JIRA, and GitHub, users need to abide by the following Rules of Behavior, and proceed to fill out the form at the bottom of this page.

Rules of Behavior and Posting Guidelines for the Use of Third-Party Web Applications.

Purpose

These rules of behavior establish the privacy and information security requirements for the use of Third Party Web Applications (TPWAs) in conjunction with the Surveillance Data Platform (SDP) Program. These rules of behavior were developed to ensure that CDC and its confidential information and technologies are not compromised, as well as protecting general CDC interests and services from risks associated with the use of TPWAs while allowing for the increased efficiencies and cost savings that come with appropriate use of third party services.

Scope

These rules of behavior and its related guidance apply to federal employees, contractors, and all external SDP users who will access TPWAs from the SDP directly or use them with non-sensitive data obtained from the SDP. All engagement with TPWAs related to the SDP will be governed by these rules of behavior, as well as to the Rules of Behavior for the Use of HHS Information Services.

Ownership

The Office of Public Health Scientific Services (OPHSS) assigns three stewards in charge of rules and policy compliance: a Business Steward, a Security Steward, and a Technical Steward. The business and security stewards are responsible for establishing policy and providing approval, while the technical steward fulfills requests from SDP users. Users requesting access to TPWAs that have not been approved yet need to assign a main and a backup point of contact (POC) with the business steward, as well as provide a justification to the security steward.

The security steward is responsible for the security of the SDP and its impact on the CDC network and compliance with CDC security policies. All users, including POCs, are responsible for adherence to this policy and associated processes. Where there is not a rule of behavior that provides explicit guidance, users must do their best to safeguard CDC and its network and services from security risks.

Rules of Behavior

All new users of the SDP must read and acknowledge these rules before using any of the approved TPWAs. This acknowledgment must be completed annually, and establishes agreement from part of the user to adhere to these rules.

- I understand that I must complete security awareness and records management training annually in order to comply with the latest security and records management policies.
- I understand that I must also follow the Rules of Behavior for use of HHS Information Resources.
- I understand that I must not use, share, or store any kind of sensitive data (health status, provision or payment of healthcare, pictures, PII, etc.) with TPWAs under **ANY** circumstance.
- I will not knowingly conceal, falsify or remove information.***This includes editing or removing the template language provided when a Github repository is created.***
- I understand that I can only use non-sensitive and/or publicly available data in TPWAs. If you are unsure of what constitutes non-sensitive information, please see guidance below.
- I understand that all passwords I create to set up TPWA accounts need to comply with CDC's password policy.
- I understand that the steward reserves the right to moderate all SDP-related data at any time.
- I understand my responsibilities to protect systems and data as specified by CDC policies.

Guidance Regarding Non-Sensitive and Publicly Available Information

As part of the SDP Program's communication plan, portions of some TPWA's are either currently open to the public or may become open to the public in the future. The following guidelines will inform and assist the user in determining that the information to be posted on a TPWA is not sensitive. The bottom line is if the content you are posting is not appropriate to post for public access, it should not be posted on any TPWA.

Before posting information that involves other CDC programs, employees, etc. to TPWA's, it is important that the poster ensures they receive approval by the relevant CDC entity to post the information.

Questions to consider before posting information include:

Do I have reservations about anyone viewing this information?	Yes	Do **not** post.
Were individuals informed that this information would be posted on Confluence?	No	Do **not** post.
Is this information directly attributed to an individual?	Yes	Do **not** post.
Does this information contain details or descriptions of CDC security systems or other sensitive infrastructures?	Yes	Do **not** post.
Does this information reflect SDP's efforts to engage and inform external partners and the public?	No	Do **not** post.

Examples of information which has been deemed **not sensitive** and may be posted on TPWA's include the following.

- Use cases
- User stories/requirements
- Process flows
- Program pain points
- Software Service Descriptions

Sensitive information, which should **not** be posted, includes (but is not limited to) the following.

- Information directly attributed to an individual
- The names or pictures of individuals
- Protected health information
- Project management material. This includes posting or discussing security documentation, implementation plans, communications regarding project specifics, etc.
- Opinions related to programs or tools, specifically those that may have an adverse impact
- Links to CDC SharePoint or other internal references
- Details on CDC internal infrastructure

If there's any question on whether information may be sensitive (such as detailed interview notes or specific references provided during a program interview), further guidance should be sought from the security steward **prior to posting the information on any TPWA.**

Enforcement

Users looking to use TPWAs as potential services of the SDP that are unable to follow these rules of behavior will not have authorization to do so. Any users that violate these rules of behavior or CDC security policies may be subject to action, up to and including revoking access to TPWAs as part of the SDP. Technical and security stewards have the right to enforce these rules of behavior based on violations at any time.

References

- Policy for Managing the Use of Third-Party Websites and Applications http://www.hhs.gov/ocio/policy/policy2013_0001.html
- Rules of Behavior for Use of HHS Information Resources http://www.hhs.gov/ocio/policy/hhs-rob.html
- Security and Awareness Training http://sat.cdc.gov/

Third-Party Setup Request Form

Contact information request form for third-party (Atlassian & Github) setup requests.

Sign in to Google to save your progress. Learn more

* Indicates required question

Name *

Your answer

Email *

Your answer

Company/Organization *

Your answer

Which tool are you requesting access to? *

- GitHub
- Atlassian (Confluence & JIRA)