SoftWare Assurance MarketPlace (SWAMP) Privacy Policy

Intended Distribution: Public

Version 1
January 13, 2014

The SoftWare Assurance MarketPlace (SWAMP) network and Continuousassurance.org website collect some information from users who utilize this service. We have developed this privacy policy to explain to you what information is collected, how and why it is used, and how it is protected.

The SWAMP is a security focused service and thus we are very diligent about the security of your information.

Authority

The SWAMP is a project created and managed by three university institutions and majorly funded by a grant from the United States Department of Homeland Security (DHS). The primary interest in its public usage is to improve the security of software to the effect that it improves national security. The system is jointly managed and developed by staff under contract from the Morgridge Institute for Research (MIR), University of Wisconsin (UW), University of Illinois (UI), and Indiana University (IU) and the project is legally represented by the Wisconsin Alumni Research Foundation (WARF). In this document the term 3rd party refers to any other organization or individual not previously mentioned.

This policy is governed by the laws of the state of Wisconsin as well as the federal laws of the United States of America.

What information we collect

Information that you give us

When you interact with our services, you may submit information such as your name, e-mail address, phone number, mailing address and where you live. Your answer to a security question for the purpose of recovering an account might also be given. All of this information is called Personally Identifiable Information (PII) and is classified and protected in a special way mentioned in the protection section below.

You may request to be part of SWAMP outreach and receive regular email updates on the SWAMP by providing us your email address or specifically requesting this when you register to

use the SWAMP.

If you register for an event organized by the SWAMP, you may be asked to register with a third party service arranged by the SWAMP to help organize that event.

Software, analysis tools and results you submit or generate

The primary function of SWAMP is to analyze software for weaknesses. Thus, any software that you submit to us for analysis or use and the weakness information generated through this service are held on our servers. This software and the analysis results will be as kept private and shared only at your request, but is subject to monitoring by SWAMP staff for malicious, stolen or unrelated code not in agreement with SWAMP's goals and policies. Source code uploaded by the user may also be viewed by SWAMP staff in order to improve SWAMP services.

Information we collect from your use of our services

Because the SWAMP is an Internet based service, there is information that we are able to see from the use of our service.

- Your Internet IP address when accessing a SWAMP service or website.
- Your geographical location when accessing a SWAMP service or website, determined from your IP address.
- Information about your web browser and any other client software you use to access the SWAMP.
- Information about the time of day/date and duration that you have accessed SWAMP services.
- Information about time of day/date and duration that is included in software/files that are uploaded to the SWAMP.
- Metadata included with software/files that are uploaded to the SWAMP.
- Your operating system name and version.
- Browser cookies that are associated with the SWAMP websites.
- Details of how you were referred to a SWAMP website including search terms used, such as a Google search query that provided a link to a SWAMP website or forum.
- Your chosen cleartext password for use when authenticating to the SWAMP before being hashed and compared. We do not store your clear text password anywhere.
- A security question that may be used for recovering a lost password or authenticating you.
- Third party authentication information used to authenticate with the SWAMP.
- Anonymous identifiers used to track your usage of the SWAMP.

How information we collect is used

The primary goal of the SWAMP is to allow users to submit software for analysis to find weaknesses in the software. We collect PII so that we can decide whether to authorize a user to utilize the SWAMP and so that we may contact the user in the event that an account is being misused. PII data is also used for notifications about service or policy changes.

Information related to your IP, web browser and operating system are used to produce generalized statistics about the overall use of the SWAMP service. It is also used to help improve SWAMP services.

Information in the SWAMP may be reviewed or audited by contracted employees working on behalf of any of the institutions mentioned in this document. These contracted employees are under the same obligations to protect your privacy as other SWAMP staff.

Any information stored on the SWAMP may be shared with the United States Department of Homeland Security and any other agency of the United States government. The main purpose of this is to gather statistical information on how effectively the SWAMP is being utilized for the purpose of improving the security of software.

If you requested to be part of SWAMP outreach, the SWAMP may use a third party to handle the process of emailing you information, meaning the SWAMP may share your email address with that party. We will only share your information with parties who agree to use it for an intended purpose and not sell it.

How information is protected

The SWAMP staff understand how important it is to protect PII data as well as the software weakness data. These are our two main priorities for data protection at the SWAMP.

The first way that we protect these types of data is to limit the exposure of this data to only those staff members that need the information in order to perform their intended function.

A second way that we protect these types of data is to identify what systems this data is stored on and passes through and isolate these systems from the rest of the network as much as possible. This reduces the opportunities for data to be exposed.

We further protect the data using standard network and system security controls such as network firewalls and intrusion detection systems, access controls for users and staff, required use of strong authentication, network and stored data encryption when possible and limitations on data retention.

Changes to Privacy Policy

Should this privacy policy change, we will notify you using your prefered contact method as chosen upon signup. If you do not have a preference, we will default to sending you an e-mail with a link to the new policy.