



# **The OWASP Application Security Code of Conduct for Trade Organizations**

## **(The OWASP “Purple Book”)**

Version 1.18 (19<sup>th</sup> May 2015) Release

© 2011-2015 OWASP Foundation

This document is released under the Creative Commons Attribution [ShareAlike 3.0 license](https://creativecommons.org/licenses/by/3.0/).

For any reuse or distribution, you must make clear to others the license terms of this work

## Introduction

Modern businesses in every sector require software applications for day-to-day operation. Trade Organizations (also known as trade, industry or sector associations or groups) are pivotal in the definition and enforcement of mandatory good practices within their sphere of influence. Higher standards of security benefit member organizations through reduced costs, better compliance with legislation and other mandates, and reduced risk of reputational damage. The trade organization also benefits from the enhanced reputation of its membership. OWASP is ready to work with trade organizations and has considerable resources to help trade organizations and their members make good decisions and get application security right.

## Code of Conduct

### 1. The Trade Organization **MUST** include an “Application Security” section in its own membership requirements.

*OWASP asks that each Trade Organization establish a membership requirement that captures the need for protecting data, ensuring safety, preventing fraud, defending clients & customers, etc. OWASP does not specify the exact form or substance of this requirement, only that it represent your desire for applications that affect your members to be secure.*

### 2. The Trade Organization **MUST** provide OWASP a “notice and comment” period when releasing requirements that include an application security aspect.

*OWASP wants to help Trade Organizations create membership requirements (policies, codes of practice, rules, bylaws, etc) that will secure technologies. Ideally, OWASP would be involved from the beginning in its definition, but believes it is critical that OWASP has an opportunity to provide comments and guidance to help shape the final result.*

## Recommendations

### A. The Trade Organization **SHOULD** be an OWASP Supporter.

*The main benefit of becoming an OWASP Supporter<sup>1</sup> is to demonstrate your belief that application security is important and that you are working to help your members properly address application security risk in their businesses.*

### B. The Trade Organization **SHOULD** assign a liaison to OWASP.

*OWASP has a group that focuses on improving application security in trade organizations. The group collaborates via email and at OWASP events worldwide. OWASP expects the liaison to monitor the list and participate as much as they care to. The Trade Organization can define their level of participation.*

### C. The Trade Organization **SHOULD** leverage OWASP by attending events, using materials, and asking experts for help.

*OWASP has a lot to offer to Trade Organizations. OWASP has freely available tools, documents, guidelines, and standards. OWASP has worldwide events that are open to everyone and all the*

*presentations are recorded. Trade Organizations are strongly encouraged to reach out to OWASP's experts with their questions, ideas, and even participate in projects.*

**D. The Trade Organization SHOULD encourage interested members to participate in OWASP.**

*Participation in OWASP projects<sup>ii</sup> is a fantastic way for your members to share sector-specific knowledge which helps their colleagues, partners, suppliers and customers, and improves application security throughout the whole supply chain. All OWASP projects are open to participation simply by joining a mailing list, asking what needs to be done, and volunteering. Helping with a project does not necessarily involve technical research or programming skills – many projects need assistance with design, testing, review, creating documentation and tutorials and promotion. Being a participant does not require membership. Participants may want to start a sector-specific OWASP project of their own and OWASP will help get this started.*

## References

- i. Membership, OWASP  
<https://www.owasp.org/index.php/Membership>
- ii. Projects, OWASP  
[https://www.owasp.org/index.php/Category:OWASP\\_Project](https://www.owasp.org/index.php/Category:OWASP_Project)

## OWASP Application Security Codes of Conduct

In order to achieve our mission, OWASP needs to take advantage of every opportunity to affect software development everywhere. At the OWASP Summit 2011 in Portugal, the idea was created to try to influence educational institutions, government bodies, standards groups, trade organizations and groups active in the application security space. We set out to define a set of minimal requirements for these organizations specifying what we believe to be the most effective ways to support our mission. We call these requirements a “code of conduct” to imply that these are normative standards, they represent a minimum baseline, and that they are not difficult to achieve.

Trade Organizations wishing to announce their compliance with this Code of Conduct should read the associated information on statements of compliance:

[https://www.owasp.org/index.php/OWASP\\_Codes\\_of\\_Conduct#compliance](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#compliance)

Special thanks to Colin Watson for creating this document, Fabio Cerullo and Sebastien Deleersnyder for reviewing it, and to all the participants in the working sessions at the OWASP Summit 2011 in Portugal for their ideas and contributions in the related Codes that inspired this one.

The latest version of this document, and the other Codes of Conduct, can be found at:

[https://www.owasp.org/index.php/OWASP\\_Codes\\_of\\_Conduct](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct)

## About OWASP

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

<https://www.owasp.org>