# The OWASP Application Security Code of Conduct for Educational Institutions

# (The OWASP "Blue Book")

Version 1.1 (20th July 2011) Draft

## Introduction

Educational Institutions have an unparalleled opportunity to help improve application security worldwide. For many software developers and others studying information technology, their core thought patterns, ethics, and values are defined during their educational experience. We believe that all developers need to be exposed to application security during these critical formative years. While we recognize that not all developers will become application security experts, some level of awareness and experience is critical. We also believe that there is critical demand for application security experts, and that Educational Institutions are uniquely positioned to provide students with the proper foundation and awareness to develop these skills.

## Code of Conduct

1. **The Educational Institution MUST include application security content somewhere in the standard computer science curriculum.**

   *This requirement is intended to expose all students studying computer science and other information technology degrees to some level of application security. At a minimum, they should be exposed to the most critical application security risks. This should not imply that they are experts in the problem, but at least that they might recognize the problem in their work and know to get additional assistance or perform additional research.*

2. **The Educational Institution MUST offer at least one course dedicated to application security annually.**

   *To support the critical demand for application security experts, we believe that Educational Institutions should offer an opportunity for interested students to become experts in the field. This is not a topic that is necessarily suitable for all students. We do not attempt to specify the exact coverage for this application security course, other than that the general content of the most popular OWASP projects would be very good starting points.*

3. **The Educational Institution MUST ensure that an OWASP Chapter is available to their students and support it.**

   *We believe that an important part of application security is staying on top of the latest threats and technologies. This exposes students to a different kind of learning experience from great speakers and real-world practitioner experiences in application security as well as creating social connections. So we would like to see Educational Institutions ensure that their students have access to an OWASP Chapter available[i]. If there is already a local OWASP Chapter, then the institution simply needs to help students find it. If no local Chapter is available, the process to set up a student-run Chapter is very simple and OWASP will help get it started[ii].*

## Recommendations

### A. The Educational Institution SHOULD be an OWASP Supporter.

*There is no charge for an educational institution to become an OWASP Supporter[iii], and it promotes your institution on our website. The main benefit of becoming an OWASP Supporter is to demonstrate your belief that application security is important and that you are working to prepare your students to understand security and write secure code.*

### B. The Educational Institution SHOULD assign a liaison to OWASP.

*OWASP has a group that focuses on improving application security in educational institutions. The group collaborates via email and at OWASP events worldwide. We expect the liaison to monitor the list and participate as much as they care to. The institution can define their level of participation.*

### C. The Educational Institution SHOULD leverage OWASP by attending our events, using our materials, and asking our experts for help.

*OWASP has a lot to offer educators. We have freely available tools, documents, guidelines, and standards[iv]. We have worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. We even have packaged curricula, eLearning, and educational materials that are available for educators to use and modify free of charge[iv]. Educators are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.*

### D. The Educational Institution SHOULD encourage interested students to participate in OWASP.

*Participation in OWASP projects is a fantastic way for students to build their skills, enhance their resume, and learn from real-world practitioners. All OWASP projects are open to student participation simply by joining a mailing list, asking what needs to be done, and volunteering. Membership is not necessary. Motivated students can start new OWASP projects and get advice and guidance from the world's leading experts. Given the early state of application security, there are many opportunities for groundbreaking research in our field. Consider working on OWASP projects as classroom assignments, such as contributing new iOS, Java or .NET lessons to WebGoat, or developing or improving articles at OWASP on application security subjects. Imagine the enthusiasm of your students when their homework will live on as a contribution to the world, rather than simply being graded and discarded.*

## References


i. Chapters, OWASP
https://www.owasp.org/index.php/OWASP_Chapter

ii. Starting a Chapter, OWASP
https://www.owasp.org/index.php/OWASP_Chapter#Starting_a_Chapter

iii. Membership, OWASP
https://www.owasp.org/index.php/Membership

iv. Education Project, OWASP
https://www.owasp.org/index.php/Category:OWASP_Education_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.

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, and all the participants in the working sessions on Outreach to Educational Institutions, and Minimal AppSec Program for Universities, Governments and Standards Bodies at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

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