

# The OWASP Application Security Code of Conduct Idea

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 agencies, and standards bodies. 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 baseline, and that they are not difficult to achieve.

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, and all the participants at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.



# The OWASP Application Security Code of Conductfor Educational Institutions

## (The OWASP “Blue Book”)



# The OWASP Application Security Code of Conductfor Educational Institutions

## (The OWASP “Blue Book”)

## 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 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.

1. 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 a very good starting points.

1. 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. 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.

1. The Educational Institution MUST be an OWASP Supporter.

There is no charge for an educational institution to become an OWASP Supporter, 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.

1. The Educational Institution MUST assign a liaison to the OWASP Educational Institution Executive Council.

The OWASP Educational Institution Executive Council is 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 own level of participation. The Liaison will be considered an OWASP Leader and eligible for free attendance at our worldwide events.

1. 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. 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. Educators are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

1. 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. 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.



# The OWASP Application Security Code of Conductfor Government Agencies

## (The OWASP “Green Book”)



# The OWASP Application Security Code of Conductfor Government Agencies

## (The OWASP “Green Book”)

## Introduction

Government Institutions are massive consumers of application technology, and also have influence over the operation of many industries and the behavior of individuals. We believe that Government Institutions should use this power to ensure that software applications are secure enough for their intended purposes. We offer this code of conduct to help guide Government Institutions to improve the state of application security in their own applications and all those under their jurisdiction.

## Code of Conduct

1. The Government Institution MUST establish and enforce a standard that requires application security for organizations and applications under their jurisdiction.

Given the rapid influence of application technology over all aspects of modern life, virtually every government institution is now responsible for some aspect of application security. We ask you to establish a standard that captures your requirements for protecting data, ensuring safety, defending citizens, etc… We do not a specify the exact form or substance of this standard, only that it represent your desire for applications that affect your jurisdiction to be secure.

1. The Government Institution MUST build application security into software acquisition guidelines.

One of the most powerful forces in the information technology industry is the buying power of governments worldwide. As a massive consumer of application technology, we believe that including appropriate language in acquisition guidelines will strongly encourage the software industry to do a better job with application security. We do not suggest what this language should contain, but point to our Software Security Contract Annex as a possible starting point.

1. The Government Institution MUST be an OWASP Supporter.

There is no charge for an educational institution to become an OWASP Supporter, 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.

1. The Government Institution MUST assign a liaison to the OWASP Government Institution Executive Council.

The OWASP Government Institution Executive Council is a group that focuses on improving application security in government 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 own level of participation. The Liaison will be considered an OWASP Leader and eligible for free attendance at our worldwide events.

1. The Government Institution MUST provide OWASP a “notice and comment” period when releasing laws and regulations that are relevant to application security.

OWASP wants to help government institutions create laws and regulations that will result in improvements in application security. Ideally, we would be involved from the beginning in the creating of the laws and regulations, but we believe it is critical that we have an opportunity to provide comments and guidance to help shape the final result.

1. The Government Institution MUST define or adopt a definition of application security.

Without a definition of application security, government institutions may struggle with whether a particular issue should be covered or not. We do not try to mandate a single definition of application security for all institutions. Rather, we simply suggest that government institutions must have such a definition in place. We recommend using OWASP as a way to help figure out what that definition should encompass.

1. The Government Institution MUST create and promote public service messages focused on application security.

By creating and promoting a public service message that focuses on application security, government demonstrates the importance of this issue in a simple and direct way. We do not attempt to specify the exact form or substance of the message, simply that it should encourage all organizations and individuals to understand the risks and take appropriate action.

1. The Government Institution SHOULD encourage educational institutions to focus on application security.

We believe that educational institutions represent a unique opportunity to influence software developers and other information technology students while they are still forming their ideas, ethics, and values. Government agencies can influence these organizations to focus on application security and hopefully get their institution in line with the OWASP Code of Conduct for Educational Institutions (“The OWASP Blue Book”). Government organizations might take the opportunity to sponsor training in application security for educational institutions.

1. The Government 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. 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. Educators are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.



# The OWASP Application Security Code of Conductfor Standards Bodies

## (The OWASP “Yellow Book”)



# The OWASP Application Security Code of Conductfor Standards Bodies

## (The OWASP “Yellow Book”)

## Introduction

The world of information technology is driven largely by standards bodies such as the IETF, ENISA, PCI, ISO, W3C, OASIS, and many more. We believe that every technical standard that involves software in any way should take the time to consider possible application security risks and, if necessary, address them in the standard. OWASP is ready to work with standards bodies and has considerable resources to help standards bodies make good decisions and get application security right.

## Code of Conduct

1. The Standards Body MUST include an “Application Security” section in each technical standard.

We believe that the most important way to ensure that application security is considered during the development of a technical standard is to require a section focusing on that topic. Even for standards that do not have any need for specific application security requirements, the process of considering possible application security implications and documenting the outcome is a critical part of the standards process.

1. The Standards Body MUST provide OWASP a “notice and comment” period when releasing standards.

OWASP wants to help standards bodies create strong standards that will in secure technologies. Ideally, we would be involved from the beginning in the creating of the standard, but we believe it is critical that we have an opportunity to provide comments and guidance to help shape the final result.

1. The Standards Body MUST be an OWASP Supporter.

There is no charge for a standards body to become an OWASP Supporter, and it promotes your organization 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.

1. The Standards Body MUST assign a liaison to the OWASP Standards Body Executive Council.

The OWASP Standards Body Institution Executive Council is a group that focuses on improving application security in standards bodies. 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 own level of participation. The Liaison will be considered an OWASP Leader and eligible for free attendance at our worldwide events.

1. The Standards Body SHOULD define or adopt a definition of Application Security

Without a definition of application security, government institutions may struggle with whether a particular issue should be covered or not. We do not try to mandate a single definition of application security for all standards bodies. Rather, we simply suggest that standards bodies must have such a definition in place. We recommend using OWASP as a way to help figure out what that definition should encompass.

1. The Standards Body SHOULD leverage OWASP by attending our events, using our materials, and asking our experts for help.

OWASP has a lot to offer standards bodies. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded. Participants are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

1. The Standards Body SHOULD involve a security expert early in their standard definition process.

Organizations creating standards may want to include a security expert to assist throughout the process of creating a standard. While OWASP does have experts with a very broad array of expertise, we may not understand your domain fully. However, we believe there is huge value in having a security expert available to assist with threat modeling, vulnerability analysis, risk assessment, and other security techniques.