

# OWASP Application SecurityCodes of ConductAggregated Booklet

Version 1.17 (27th March 2013) Release

© 2011-2013 OWASP Foundation

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

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

## Introduction

In order to achieve its mission, OWASP needs to take advantage of every opportunity to affect software development everywhere.

<https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project>

At the OWASP Summit 2011 in Portugal, the idea was created to try to influence various groups active in the application security space. The concept was to define a set of minimal requirements for these organizations specifying what OWASP believes to be the most effective way to support its mission. These requirements are called a “code of conduct” to imply that these are normative standards, in that they represent a minimum baseline, and are not difficult to achieve. The latest version of this document, and all the Codes of Conduct, can be found at:

<https://www.owasp.org/index.php/OWASP_Codes_of_Conduct>

## Format and content

Each Application Security Code of Conduct is comprised of a small number of mandatory items (the Code of Conduct) and a few other optional recommendations. There are six Codes of Conduct:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Page 5 [**OWASP Green Book**](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#Government_Bodies) |  | Page 9 [**OWASP Blue Book**](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#Educational_Institutions) |  | Page 13 [**OWASP Yellow Book**](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#Standards_Groups) |
| The OWASP Application Security Code of Conduct for Government Bodies |  | The OWASP Application Security Code of Conduct for Educational Institutions |  | The OWASP Application Security Code of Conduct for Standards Groups |
|  |  |  |  |  |
| Page 17 [**OWASP Purple Book**](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#Trade_Organizations) |  | Page 21 [**OWASP Red Book**](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#Certifying_Bodies) |  | Page 25 [**OWASP Gray Book**](https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#Development_Organizations) |
| The OWASP Application Security Code of Conduct for Trade Organizations |  | The OWASP Application Security Code of Conduct for Certifying Bodies |  | The OWASP Application Security Code of Conduct for Development Organizations |

## Compliance

There is no formal compliance methodology or register. 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%23compliance)

## Contributors

Special thanks to the volunteers named in each Code of Conduct, as well as all the participants in the working sessions on Outreach to Educational Institutions and Minimal AppSec Program for Universities, Governments and Standards Bodies at OWASP’s 2011 Summit, for their ideas and contributions to the Codes and this project. To become involved, please join the mailing list:

<https://lists.owasp.org/mailman/listinfo/owasp-codes-of-conduct>



# The OWASP Application Security Code of Conductfor Government Bodies

## (The OWASP “Green Book”)

Version 1.17 (27th March 2013) Release

© 2011-2013 OWASP Foundation

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

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

## Introduction

Government Bodies (national, regional and local government, departments, directorates, agencies and other types of statutory body) are massive consumers of application technology, and also have influence over the operation of many industries and the behavior of individuals. OWASP believes that Government Bodies should use this power to ensure that software applications are secure enough for their intended purposes. OWASP offers this code of conduct to help guide Government Bodies to improve the state of application security in their own applications and all those under their jurisdiction.

## Code of Conduct

1. The Government Body 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 body is now responsible for some aspect of application security. OWASP asks you to establish a standard that captures your requirements for protecting data, ensuring safety, defending citizens,, and thus support trust. OWASP does not specify the exact form or substance of this standard, only that it represents your desire for applications that affect your jurisdiction to be secure. However, OWASP recommends consideration of its Application Security Verification Standard i.

1. The Government Body 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, OWASP believes that including appropriate language in acquisition guidelines will strongly encourage the software industry to do a better job with application security. OWASP does not suggest what this language should contain, but points to its Software Security Contract Annex ii as a possible starting point.

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

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

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

Without a definition of application security, government bodies may struggle whether a particular issue should be covered or not. OWASP does not try to mandate a single definition of application security for all bodies. Rather, OWASP simply suggests that government bodies must have such a definition in place. OWASP recommends using its materials as a way to help figure out what that definition should encompass.

1. The Government Body 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 bodies demonstrate the importance of this issue in a simple and direct way. OWASP does 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.

## Recommendations

1. The Government Body SHOULD be an OWASP Supporter.

The main benefit of becoming an OWASP Supporteriii is to demonstrate your belief that application security is important and that you are working to build a robust information-age economy and providing a suitably skilled workforce that attracts investment.

1. The Government Body SHOULD assign a liaison to OWASP.

OWASP has a group that focuses on improving application security in government bodies. 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 body can define their level of participation.

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

OWASP believes 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 bodies 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”)iv. Government bodies might take the opportunity to sponsor training in application security for educational institutions.

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

OWASP has a lot to offer to government bodies. OWASP has freely available tools, documents, guidelines, and standards. OWASP has worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. OWASP even has packaged curricula, eLearning, and educational materials that are available for government bodies to use and modify free of charge. Government bodies are strongly encouraged to reach out to OWASP’s experts with their questions, ideas, and even participate in projects.

**References**

1. Application Security Verification Standard
[https://www.owasp.org/index.php/Category:OWASP\_Application\_Security\_Verification\_Standard\_Project](https://www.owasp.org/index.php/Category%3AOWASP_Application_Security_Verification_Standard_Project)
2. Software Security Contract Annex, OWASP
<https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex>
3. Membership, OWASP
<https://www.owasp.org/index.php/Membership>
4. OWASP Code of Conduct for Educational Institutions (“The OWASP Blue Book”)
<https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#tab=Educational_Institutions>

**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.

Government Bodies 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%23compliance)

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, Fabio Cerullo and Sebastien Deleersnyder for reviewing it, 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.

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>

**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>



# The OWASP Application Security Code of Conductfor Educational Institutions

## (The OWASP “Blue Book”)

Version 1.17 (27th March 2013) Release

© 2011-2013 OWASP Foundation

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

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

## 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. OWASP believes that all developers need to be exposed to application security during these critical formative years. While OWASP recognizes that not all developers will become application security experts, some level of awareness and experience is critical. OWASP also believes 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 become experts in the problem, but at least that they might recognize the problem in their work and know how 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, OWASP believes that Educational Institutions should offer an opportunity for interested students to become experts in the field. This is a topic not necessarily suitable for all students. OWASP does 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 point.

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

OWASP believes 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 OWASP would like to see Educational Institutions ensure that their students have access to an OWASP Chapteri. 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 getting it startedii.

## Recommendations

1. The Educational Institution SHOULD be an OWASP Supporter.

There is no charge for an educational institution to become an OWASP Supporteriii, and it promotes your institution on the OWASP 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 application security.

1. 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. OWASP expects the liaison to monitor the list and participate as much as they care to. The institution can define their level of participation.

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

OWASP has a lot to offer educators. OWASP has freely available tools, documents, guidelines, and standardsiv. OWASP has worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. OWASP even has packaged curricula, eLearning, and educational materials that are available for educators to use and modify free of chargeiv. Educators are strongly encouraged to reach out to OWASP’s 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. 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 the 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 never used again.

**References**

1. Chapters, OWASP
<https://www.owasp.org/index.php/OWASP_Chapter>
2. Starting a Chapter, OWASP
<https://www.owasp.org/index.php/OWASP_Chapter#Starting_a_Chapter>
3. Membership, OWASP
<https://www.owasp.org/index.php/Membership>
4. Education Project, OWASP
[https://www.owasp.org/index.php/Category:OWASP\_Education\_Project](https://www.owasp.org/index.php/Category%3AOWASP_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.

Educational Institutions 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%23compliance)

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, Fabio Cerullo and Sebastien Deleersnyder for reviewing it, 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.

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>

**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>



# The OWASP Application Security Code of Conductfor Standards Groups

## (The OWASP “Yellow Book”)

Version 1.17 (27th March 2013) Release

© 2011-2013 OWASP Foundation

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

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

## Introduction

The world of information technology is driven largely by standards groups such as BS, ENISA, IETF, ISO, ITU, NIST, OASIS, PCI SSC, W3C, and many more. OWASP believes 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 groups and has considerable resources to help standards groups make good decisions and get application security right.

## Code of Conduct

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

OWASP believes that the most important way to ensure that application security is considered during the development of any technical standard related to software 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 creation process.

1. The Standards Group MUST provide OWASP a “notice and comment” period when releasing standards that include an application security aspect.

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

1. The Standards Group MUST define or adopt a definition of Application Security.

Without a definition of application security, standards groups may struggle whether a particular issue should be covered or not. OWASP does not try to mandate a single definition of application security for all standards groups. Rather, OWASP simply suggests that standards groups must have such a definition in place. OWASP recommends using its materials as a way to help figure out what that definition should encompass.

## Recommendations

1. The Standards Group SHOULD be an OWASP Supporter.

The main benefit of becoming an OWASP Supporterii is to demonstrate your belief that application security is important and that you are working to help your constituents properly address application security in the projects affected by the standards you develop.

1. The Standards Group SHOULD assign a liaison to OWASP.

OWASP has a group that focuses on improving application security in standards. 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 standards group can define their level of participation.

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

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

1. The Standards Group 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, it may not understand your domain fully. However, OWASP believes there is huge value in having a security expert available to assist with threat modeling, vulnerability analysis, risk assessment, and other security activities that should be applied during the creation of any technical standard.

**References**

1. Membership, OWASP
<https://www.owasp.org/index.php/Membership>
2. Projects, OWASP
[https://www.owasp.org/index.php/Category:OWASP\_Project](https://www.owasp.org/index.php/Category%3AOWASP_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.

Standards Groups 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%23compliance)

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, Fabio Cerullo, Larry Conklin and Sebastien Deleersnyder for reviewing it, 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.

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>

**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>



# The OWASP Application Security Code of Conductfor Trade Organizations

## (The OWASP “Purple Book”)

Version 1.17 (27th March 2013) Release

© 2011-2013 OWASP Foundation

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

1. 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

1. The Trade Organization SHOULD be an OWASP Supporter.

The main benefit of becoming an OWASP Supporteri 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.

1. 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.

1. 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.

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

Participation in OWASP projectsii 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**

1. Membership, OWASP
<https://www.owasp.org/index.php/Membership>
2. Projects, OWASP
[https://www.owasp.org/index.php/Category:OWASP\_Project](https://www.owasp.org/index.php/Category%3AOWASP_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%23compliance)

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>

**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>



# The OWASP Application Security Code of Conductfor Certifying Bodies

## (The OWASP “Red Book”)

Version 1.17 (27th March 2013) Release

© 2011-2013 OWASP Foundation

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

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

## Introduction

As understanding of application security becomes a critical part of an individual’s skill set, organizations are eagerly seeking guidance in identifying knowledgeable individuals in application security. OWASP believes that Certifying Bodies can play a role to empower organizations to identify security-minded individuals. While OWASP will ***never*** endorse or support any particular certification, OWASP offers this code of conduct to help guide Certifying Bodies to better serve organizations that are ready to embrace an application security certification.

## Code of Conduct

1. The Certifying Body MUST NOT misrepresent its certification as being endorsed or supported by OWASP.

While OWASP recognizes the need of organizations to identify individuals with an understanding of application security, OWASP will not endorse any Certifying Body or their certification. One of the bedrock principles of OWASP is to maintain a vendor-neutral position and any endorsement of a Certifying Body or their certification is in direct contradiction of this core value. OWASP respects your desire to fill a void in the application security space and expects that you will in return respect OWASP’s core values and brand name.

1. The Certifying Body MUST include a visible disclaimer when the certification is “based on OWASP materials”.

OWASP will not allow its brand name to be used in the certification title. However, OWASP welcomes a Certifying Body to leverage tools, documents, guidelines, and standards that are freely available from OWASPi. OWASP recognizes that in such cases, a Certifying Body may wish to inform their audience that their certification is “based on OWASP materials”. OWASP is honored by your desire to leverage OWASP materials, but asks that you honor the OWASP name and clearly disclaim that your use of OWASP materials does not represent an endorsement or association with OWASP.

## Recommendations

1. The Certifying Body SHOULD collect and publish feedback from certification applicants, recipients, and organizations recognizing the certification.

Certifications represent the Certifying Body’s assertion that the recipient meets some minimal criteria, as defined by the Certifying Body. Organizations depend on that assertion when recognizing a Certifying Body’s certification. OWASP believes that organizations need feedback to effectively determine the value of a certification. OWASP does not suggest what feedback should be solicited, nor the exact form or method for this publication; only that it represents your desire to honestly communicate the value and esteem or your certification.

1. The Certifying Body SHOULD utilize questions, answers, evaluation material and processes that are open and freely available to the general public.

Organizations around the world depend on Certifying Bodies to help identify individuals who understand application security. Supplying open questions and answers allows organizations to evaluate for themselves whether or not a certification adequately satisfies their need. OWASP asks you to publish the bank of all questions and answers for any examination-based certification. OWASP does not specify the exact form or method for administering the exam nor for publishing the questions and answers; only that it represents your desire to enable organizations to understand and evaluate the substance of your examination as it pertains to their organizational needs. OWASP suggests that the certifying body uses questions and answers developed by the OWASP community.

1. The Certifying Body SHOULD be an OWASP Supporter.

The main benefit of becoming an OWASP Supporterii is to demonstrate your belief that application security is important and that you are working to help improve the state of application security in the world.

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

OWASP has a lot to offer Certifying Bodies. OWASP has freely available tools, documents, guidelines, and standards. OWASP has worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. OWASP even has packaged curricula, eLearning, and educational materials that are available for potential applicants to use and modify free of charge. Certifying Bodies are strongly encouraged to reach out to OWASP’s experts with their questions, ideas, and even participate in projects.

**References**

1. Projects, OWASP
[https://www.owasp.org/index.php/Category:OWASP\_Project](https://www.owasp.org/index.php/Category%3AOWASP_Project)
2. Membership, OWASP
<https://www.owasp.org/index.php/Membership>

**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.

Certifying Bodies 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%23compliance)

Special thanks to Jason Taylor and Jason Li for creating this document, with contributions from Matthew Chalmers, Martin Knobloch and Justin Searle, and to Fabio Cerullo, Larry Conklin and Sebastien Deleersnyder for reviewing it, and to all the participants in the work session on Certification at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

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>

**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>



# The OWASP Application Security Code of Conductfor Development Organizations

## (The OWASP “Gray Book”)

Version 1.17 (27th March 2013) Release

© 2012-2013 OWASP Foundation

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

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

## Introduction

Software applications are at the heart of information systems and business processes. Organizations rely on these applications to undertake their business and process valuable data, yet the applications often have weak, or poorly selected, security mechanisms. Organizations that want to develop software must ensure that the users of their code are protected. Development organizations may be developing their own software or producing software for use by others. OWASP has unparalleled resources available to help organizations acquire, develop and operate applications securely.

## Code of Conduct

1. The Development Organization MUST have an application security awareness program for software developers and managers.

Training is a fundamental starting point for any software security initiative. The application security training for software developers, architects, managers, and other information technology staff should be tailored to the individual’s role. The training should include guidance on the importance of application security to the business as well as both conceptual and technical information. It must be linked with the Development Organization’s standards, technologies, controls, processes, compliance requirements and the relevant risks.

1. The Development Organization MUST identify and mitigate application security risks as a core part of their software engineering process.

The identification and mitigation of application security risks must be addressed through activities that fit into each development team’s engineering processes. Commonly they would include steps to assess threats, define security requirements, develop secure architectures and undertake secure coding practices. OWASP does not specify what these should be precisely nor how they should be performed; each Development Organization/team can define what fits their risks, process and culture.

1. The Development Organization MUST independently verify that appropriate security controls are present, robust, and used properly in every application.

Whatever security controls are identified, Development Organization/teams must get independent assurance that there are processes in place to verify them. This verification is likely to include security code review, security testing, security architecture review, threat modeling, code release integrity checks, configuration checks, audits, vulnerability management, etc. These activities are most cost effective when performed throughout the development lifecycle, as opposed to a big review before delivery. As risks change over time, and as code undergoes changes, it is also important these activities continue and are managed throughout the operational life of the application.

## Recommendations

1. The Development Organization SHOULD build application security into software acquisition processes.

Software development utilizes frameworks, modules, libraries, components and other code from third parties. Some development may be sub-contracted or outsourced. The Development Organization should have a process to define security requirements, ensure integrity in the supply chain and to evaluate software before purchase or use; this may require some contract language. OWASP does not suggest what this language should contain, but point to OWASP’s Software Security Contract Annex as a possible starting point.

1. The Development Organization SHOULD be an OWASP Supporter.

The main benefit of becoming an OWASP Supporter is to demonstrate your belief that application security is important and that you are working to build a robust information-age economy and providing a suitably skilled workforce that attracts investment. In addition, your support goes directly to help researchers drive progress in application security to help protect the entire information technology ecosystem.

1. The Development Organization SHOULD assign a liaison to OWASP.

OWASP has a group that focuses on improving application security in organizations that undertake development. 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 Development Organization can define their level of participation.

1. The Development Organization SHOULD encourage relevant trade organizations to focus on application security.

Improving application security across a whole sector benefits all organizations by increasing the skills of the available workforce and by raising standards in the software supply chain. It could also reduce the risk of increased legislation and regulation. OWASP believes that organizations in all sectors have the ability to influence their peers and raise standards in their markets. They can influence their own trade organizations to focus on application security and hopefully get in line with the OWASP Code of Conduct for Trade Organizations (“The OWASP Purple Book”) iii.

1. The Development Organization SHOULD leverage OWASP by attending events, using materials, and asking experts for help.

OWASP has a lot to offer organizations that undertake development. OWASP has freely available tools, documents, guidelines, and standards. OWASP has worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in training courses. OWASP even has packaged curricula, eLearning, and educational materials that are available for development teams to use and modify free of charge. Organizations are strongly encouraged to reach out to OWASP’s experts with their questions, ideas, and even participate in projects.

**References**

1. Software Security Contract Annex, OWASP
<https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex>
2. Membership, OWASP
<https://www.owasp.org/index.php/Membership>
3. OWASP Code of Conduct for Trade Organizations (“The OWASP Purple Book”)
<https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#tab=Trade_Organizations>

**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.

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%23compliance)

Special thanks to Jeff Williams and Colin Watson for creating this document, Fabio Cerullo, Larry Conklin and Sebastien Deleersnyder for reviewing it, and to 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>