WHISTLEBLOWER AND ANTI-RETALIATION POLICY

The OWASP Foundation requires board members, employees, and volunteers to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. As employees and representatives of the OWASP Foundation, we must practice honesty and integrity in fulfilling our responsibilities and comply with all applicable laws and regulations. The purpose of this policy is to encourage any concerned parties to come forward with credible information on illegal practices or violations of adopted policies of the organization. The policy specifies that the organization will protect the individual from retaliation and identifies the appropriate procedure(s) for reporting these issues.

I. Reporting Responsibility

This Whistleblower Policy is intended to encourage and enable employees and others to raise serious concerns internally so that the OWASP Foundation can address and correct inappropriate conduct and actions. It is the responsibility of all board members, employees and volunteers to report concerns about violations of the OWASP Foundation's code of ethics or suspected violations of law or regulations that govern the OWASP Foundation's operations.

II. No Retaliation

It is contrary to the values of the OWASP Foundation for anyone to retaliate against any board member, employee, or volunteer who in good faith reports an ethics violation, or a suspected violation of law, such as a complaint of discrimination, or suspected fraud, or suspected violation of any regulation governing the operations of the OWASP Foundation. Anyone who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment, removal from office, and revocation of membership.

III. Initiating an Informal Complaint

A. Employees

The OWASP Foundation has an open door policy and suggests that employees share their questions, concerns, suggestions or complaints with their supervisor. If they are not comfortable speaking with their supervisor or are not satisfied with their supervisor's response, they are encouraged to speak with OWASP's Executive Director, a member of the OWASP Board of Directors, or the appointed Compliance Officer. This person will then serve as their point-of-contact during the Whistleblower process, as well as the

person responsible for capturing and archiving all related evidence, unless a conflict of interest is identified. If a conflict of interest is identified, the point-of-contact will defer responsibility to either the Chairman of the Board or the Compliance Officer.

B. Non-Employees

The same open door policy that applies to OWASP Foundation employees also applies to board members and volunteers. All individuals are encouraged to share questions, concerns, suggestions, or complaints with OWASP's Executive Director, a member of the OWASP Board of Directors, or the appointed Compliance Officer. This person will then serve as their point-of-contact during the Whistleblower process, as well as the person responsible for capturing and archiving all related evidence, unless a conflict of interest is identified. If a conflict of interest is identified, the point-of-contact will defer responsibility to either the Chairman of the Board or the Compliance Officer.

IV. Commitment to Peaceful Conflict Resolution

The OWASP Foundation recognizes that conflict between contributors participating in such a diverse community will happen from time to time. Our commitment is to attempt to prevent or resolve conflict before it escalates to the point of a formal complaint. Thus, if both parties agree, we will appoint either a neutral internal mediator (approved by both parties) or a neutral third-party mediator to help the parties reach a peaceful resolution. We strongly encourage all board members, employees, and volunteers to attempt mediation as a means for conflict resolution prior to submitting a formal complaint as outlined below.

V. Initiating a Formal Complaint

At any point in time, an OWASP Foundation board member, employee, or volunteer may choose to file a formal complaint regarding the ethical or legal violations of another member of our community. This complaint must be submitted in writing (non-verbal) to the OWASP Foundation Compliance Officer. A valid complaint must include all background information necessary to evaluate the request, a list of each ethical or legal violation, as well as all evidence to support the claims. Upon submission, the Compliance Officer will evaluate that the complaint is valid and will respond back that either the complaint has been accepted, or it is lacking information necessary to properly evaluate (specifying what it is lacking).

Once a complaint has been determined as valid, the complainant is asked to cease direct contact with the individual whom they are making the complaint against. Attempts to facilitate direct contact, especially regarding the complaint in question, may result in the complaint being dismissed by the Compliance Officer. At this time, we also ask that the complainant refrain from speaking on the matter with anyone other than the Compliance Officer, in order to ensure the utmost amount of confidentiality and integrity on the matter. Disregarding this request may also result in the complaint being dismissed by the Compliance Officer. The Compliance Officer will notify the OWASP Foundation Board of Directors that a formal complaint has been filed, the date it was filed, the complainant's name, and the party or parties named in the complaint.

VI. Investigating a Formal Complaint

After the Compliance Officer has determined that a complaint is valid, and has notified the OWASP Foundation Board of Directors as outlined above, they will initiate an investigation into the complaint. At this stage, the Compliance Officer, or their designee, will perform an interview of the complainant and any witnesses to the events alleged in the complaint. Additionally, the Compliance Officer will provide the subject of the complaint with a summary of the complaint against them (not an actual copy of the complaint) and allow them sufficient time to prepare for an interview with the Compliance Officer, or their designee. All interviews will be conducted either in a written question and answer format or recorded in an audio format in order to preserve evidence and ensure the objectivity and integrity of the investigation. All individuals involved in the investigation are expected to maintain confidentiality to the extent possible consistent with the need to conduct an adequate investigation, and will refrain from speaking or posting publicly about the complaint or the investigation.

VII. Concluding an Investigation

Once the Compliance Officer is satisfied that they have spoken to all concerned parties, and feels that they have enough information necessary to make a recommendation, they will begin to create a final report noting the allegations, the actors involved, their determination as to the veracity of the allegations, any remedial actions recommended, and any rationale for their determinations. Once complete, the final report will be provided to the complainant, the subject of the complaint, and any actors, individually, involved in order to allow them the opportunity to comment on the final report, which will not affect the final determination. They will be given 72 hours to respond, at which point, all responses will be aggregated alongside the final report, and any evidence collected during the investigation, and provided to the Executive Director and the OWASP Foundation Board of Directors by the Compliance Officer. At this point, the investigation can be considered closed.

VIII. Determination by the Board

Once the OWASP Foundation Board of Directors receives the final report, actor comments, and supporting evidence, they will require sufficient time to review and discuss all aspects of the situation and investigation. They should strongly consider the recommendations of the Compliance Officer, but are by no means required to follow them. From here, the standard OWASP Foundation process for Board of Director proposals and voting will apply except that any Director named in the complaint will not be allowed to vote. Once an outcome has been agreed to, a formal decision will be written up and made public, via a post on the OWASP Blog and the OWASP Leaders List, within two weeks of the vote, along with the report provided by the Compliance Officer. Appropriate corrective action will be taken if warranted by the investigation.

IX. Compliance Officer

The OWASP Foundation's Compliance Officer is responsible for ensuring that all complaints about unethical or illegal conduct are investigated and resolved. The Compliance Officer will advise the Board of Directors on all complaints and their resolution and will report at least annually on any compliance activity relating to accounting or alleged financial improprieties. The Compliance Officer is empowered to

conduct their investigations in isolation of the Board in order to maintain independence, but are free to involve members of the Board as necessary. It is solely the Compliance Officer's charge to determine whether or not a complaint can be considered valid for investigation though any individual may submit a complaint as noted above.

The Compliance Officer shall immediately notify the Board of Directors and Executive Director of any concerns or complaint regarding corporate accounting practices, internal controls or auditing and work with the committee until the matter is resolved.

A Compliance Officer shall be identified by the Board of Directors and approved by a unanimous vote by January 1 of each year. A member of the OWASP Board of Directors may not also serve as the Compliance Officer during their tenure on the Board. If the Board of Directors is not able to unanimously agree on the Compliance Officer, a neutral, third-party executive ombuds services will be contracted to serve in this role.

X. Confidentiality

Violations or suspected violations may be submitted on a confidential basis by the complainant. Reports of violations or suspected violations will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation.

Policy approved by the Board of Directors on 12/10/2014.

Current Compliance Officer
Martin Knobloch
martin.knobloch@owasp.org

Supporting Policies and Documentation

OWASP Foundation Bylaws

https://www.owasp.org/index.php/OWASP_Foundation_ByLaws

OWASP Foundation Code of Ethics

https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project#Code_of_Ethics

OWASP Foundation Employee Handbook

https://www.owasp.org/images/2/28/EmployeeHandbook2014.pdf