WHISTLEBLOWER AND ANTI-RETALIATION POLICY

The OWASP Foundation requires directors, officers and employees 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 staff and volunteers 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 those staff, board members, or outside parties (compliance officer) to whom such information can be reported.

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, officers, 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.

No Retaliation

It is contrary to the values of the OWASP Foundation for anyone to retaliate against any board member, officer, 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. An employee or Board Member who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment or removal from office.

Reporting Procedure

The OWASP Foundation has an open door policy and suggests that employees share their questions, concerns, suggestions or complaints with their supervisor. If you are not comfortable speaking with your supervisor or you are not satisfied with your supervisor's response, you are encouraged to speak with OWASP's Executive Director, a member of the OWASP Board of Directors, or the policy Compliance Officer. Employees and Board Members are required to report complaints or concerns about suspected ethical and legal violations in writing to the OWASP Foundation's Compliance Officer, who has the responsibility to investigate all reported complaints.

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 Executive Director and Chairman of the Board of all complaints and their resolution and will report at least annually to the entire Board of Directors on an compliance activity relating to accounting or alleged financial improprieties.

A Compliance Officer shall be identified by the Board of Directors and approved by a unanimous vote by January 1 of each year. 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.

Accounting and Auditing Matters
The OWASP Foundation's 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.

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.

Handling of Reported Violations
The OWASP Foundation's Compliance Officer will notify the person who submitted a complaint and acknowledge receipt of the reported violation or suspected violation. All reports will be promptly investigated and appropriate corrective action will be taken if warranted by the investigation.

Once a final determination has been made on the veracity of the allegation and any necessary remediation actions, the Compliance Officer will complete a final report noting the actors involved, allegations, remediation actions, and rationale for the determination. The actors involved will also have opportunity to make comments on the report which will not affect the final determination, but be included in the records. This report will be submitted to the Board of Directors and Executive Director.

Policy approved by the Board of Directors on {Date}.

Insert contact information for Compliance Officer

Appendix

OWASP Foundation Code of Ethics

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote the implementation of and promote compliance with standards, procedures, controls for application security;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information

encountered in the course of professional activities;

- Discharge professional responsibilities with diligence and honesty;
- To communicate openly and honestly;
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association;
- To maintain and affirm our objectivity and independence;
- To reject inappropriate pressure from industry or others;
- Not intentionally injure or impugn the professional reputation of practice of colleagues, clients, or employers;
- Treat everyone with respect and dignity; and
- To avoid relationships that impair — or may appear to impair — OWASP's objectivity and independence.

Code of Ethics Disciplinary Action

Each of us is expected to behave according to the principles contained in the Code of Ethics. Breaches of the Code of Ethics may result in the foundation taking disciplinary action.