Tigerscheme® Members code of Conduct

September 2014

1. The Member owes a duty of professional care to the organisation for which testing is being conducted:

   a. Members are only to conduct or supervise testing for which they have adequate training, experience and equipment.

   b. Members are to advise the customer where they feel the scope of the test requested will not allow them to form an adequate opinion of the system security[1].

   c. Reports produced by Members are to reflect their best professional opinion of the security of the system(s) tested.

   d. All vulnerabilities discovered or inferred are to be reported to the customer. False positive results are also to be noted.

   e. Where testing is conducted on in-production systems, due care is to be taken to minimise the risk of system and service outages, Members are to assist in the recovery of any systems or services.

   f. Destructive testing or active exploitation against business critical systems is not to be conducted without the express permission of the system owner and, if a separate organisation, the operator.

2. The Member owes a duty of care to society:

   a. Appropriate written permission is to be obtained for all testing[2].

   b. The Member is to ensure that only systems within the test scope are targeted for testing and that only test types permitted by the scope or other formal agreement are employed.

   c. The legislative regime(s) relating to attacks against computer systems are to be complied with. As a minimum, this would include the laws and (if any) regulatory rules of:

      i. the jurisdiction in which the Member is domiciled.

      ii. the jurisdiction from which the Member conducts the testing.

      iii. the jurisdiction(s) in which the target systems are located.

      iv. any jurisdiction(s) through which test traffic passes.

[1] Where testing is being conducted according to a formal public testing scheme (such as CHECK) at the request of the customer, it is sufficient to insert an appropriate disclaimer into the test report.
[2] Where a Member is an employee of the system or service owner, this may be waived if permissions are granted within the organisations operating procedures.

USW Commercial Services Ltd, Pontypridd, CF37 1DL
Company Registration No: 2683025
Web:- www.tigerscheme.org

d. Test tools and processes are to be employed in a manner which ensures that active user input is required before active security testing is conducted against any system or service[3].

e. Destructive testing or active exploitation must not be conducted against safety critical in-production systems.

f. Denial of Service or resource exhaustion attacks must not be conducted across public networks.

g. Report versions designed for public release or marketing purposes must reflect the tester's honest professional opinion of the security of the system(s) tested on the date of latest test reported.

h. Members must report breaches or suspected breaches of this code, accidental or deliberate, by themselves or any other scheme Member, to the Operating Authority (USW Commercial Services Ltd).

3. The Member owes a duty of confidentiality to their employer(s) and customer(s):

a. No Member is to release details of any testing conducted except:

i. as required by the contract governing that test (which includes the rules of any test scheme(s) under which the testing was conducted).

ii. as permitted by the contract between the Member (or their employer) and the organisation for which the test is conducted.

iii. as permitted under national legislation relating to the release of confidential material of vital public interest[4].

iv. Where a new vulnerability or class of vulnerabilities is discovered during a test the release of that vulnerability is permitted, with the permission of the organisation for which the test was conducted. No identifying details of the system tested are to be released.

b. No Member is to disclose that they have conducted a test for any organisation without the written permission of the organisation.

c. No Member is to disclose that they have conducted tests on a specific system or service without the written permission of the system or service owner.

4. The Member owes a duty of care to Tigerscheme®.

a. Members are not to make public statements relating to Tigerscheme®, except statements limited to their level of membership and their memberships of committees or panels, without the permission of the Operating Authority.

[3] Use of scripted or scheduled testing is permitted, as is the use of automated system or service discovery tools. However, for example, the transfer of system addresses from a discovery tool to a previously scheduled security scan would require tester confirmation in order to be acceptable under this rule.
[4] The tester is to make all efforts to ensure that material released is the minimum necessary to meet the legal obligation.

b. Members are, where reasonable, to encourage professional testers and organisations employing testers, to participate in the scheme.

c. Members are to pay all dues required under the scheme as invoiced.

5. Members shall not engage in any activity likely to bring them, Tigerscheme®, USW Commercial Services Ltd, University of South Wales or GCHQ into disrepute nor engage in any activity which could call the results of their work into question, such as:

a. Accepting or soliciting inducements.

b. Failing to report to Tigerscheme® a change of circumstances which might call into doubt their professional integrity.

c. Failing to set out for the customer's benefit, prior to any work being undertaken, circumstances where a conflict of interest might arise or be perceived.

Breach of professional code of conduct

6. Breach, or suspected breach, by any Member of this Code, or any of its clauses, are to be reported to the Operating Authority, for the attention of the Business Development Manager. The Operating Authority will appoint a Disciplinary Panel consisting of the following:

- a panel consisting of a minimum of three (3) persons for the purpose of the hearing, to consider the reported breach and recommend appropriate sanctions to the Operating Authority.

7. Appeals against the findings or decision of a Disciplinary Panel are to be made to the Business Development Manager and will be heard by the Industry Oversight Committee.

8. Members of Tigerscheme® are not entitled to legal or trade union representation at Disciplinary Panel or Appeal hearings. If, under exceptional circumstances, a Member feels that a lack of representation will unfairly prejudice their hearing, they must set out their case, in writing to the Business Development Manager.

Limitations of Applicability

9. Where work is formally conducted under the rules of another testing scheme (e.g. CHECK) and is properly conducted under that scheme, one or more articles of this Code may not be applicable, provided that neither the relevant bid nor contract documentation mentions Tigerscheme®.

10. Where work conducted under Tigerscheme® is subject to law enforcement warrant or court order and the Member is given a written instruction (or questioned under oath) to conduct activity or release material that would breach this Code, the legal instruction should be given priority.

USW Commercial Services Ltd, Pontypridd, CF37 1DL
Company Registration No: 2683025
Web:- www.tigerscheme.org