INFORMATION SYSTEMS SECURITY ASSOCIATION (ISSA)
POLICIES AND PROCEDURES

Ethics Complaint Review Process

Intent: As an association of information security professionals, ISSA encourages its members to act in an ethical fashion for the benefit of the profession, the companies to whom we provide professional services and the public as outlined in the Association Code of Ethics. The defined process provides a mechanism for reviewing situations in which members are accused of failing to uphold this standard. Except in situations requiring protection of confidential proceedings, sensitive business plans and negotiations or other matters where a reasonable need for confidentiality applies, the operations and business of the ISSA shall be conducted so as to assure maximum transparency to its membership.

Policy: It is the responsibility of the Ethics Committee to review and act upon charges of ethics violations on the part of its members, when these cannot be resolved at the local chapter level.

Independence

ISSA Ethics Committee members and International Board officers are not permitted to be a part of any ethics violation incident they will be responsible for reviewing. Any member who is so involved will recuse him/herself from the review process. No Committee member should participate in an alleged incident in any way prior to the receipt of a formal complaint.

Complaint Submission

Any person may submit a complaint to the Ethics Committee about an ISSA member via the ethics@issa.org e-mail address. The complaint must include the following at a minimum and follow the format of Appendix A:

1. A narrative description of the circumstances around the complaint
2. The section of the ethical code that was violated
3. Any supporting information or evidence
4. Names and contact information of those involved and those familiar with the incident

The e-mail complaint will be forwarded to an assigned Ethics Committee member for review, and to an assigned member of the International Board. Once a completed form has been received and acknowledged, the complaint will be placed on the Ethics Committee Agenda for the next monthly meeting. In case of sensitive timing concerns, an Emergency Meeting may be convened.

Notice and Opportunity to Reply

If the information supporting the complaint is deemed to be sufficient for formal review, the parties will be informed via registered mail or email, which notice shall be generally in the form of Appendix B hereto. The charged member will be given 30 days to reply in writing to the complaint and to submit in writing any and all evidence and information he/she may have in support of their position. Effort will be made to obtain objective written or tangible evidence for inclusion in the record and to obtain additional pertinent information concerning the complaint.

If no reply is received, the committee will understand that the charges are valid, and the charged member has waived all objection to the proceedings and action. The Ethics Committee will move to determine if and what sanction is appropriate. The charged party shall be notified in the Notice of Formal Review of the consequences of failing to reply and to participate in the Hearing, if any. If a reply is received, a hearing will be scheduled involving an Ethics Review Board and the parties to the complaint.

12.8.4 Mediator

The Ethics Committee may request that a Mediator invites the charged individual and complainant to alternatively resolve the issue. The Mediator will be a neutral member selected from the ISSA International Board.

12.8.5 Review

At its monthly meeting, the Ethics Committee will discuss the complaint. Any committee member who is involved in or has ties to those involved in the complaint will absent himself or herself from the discussion.

If the committee determines that additional information or evidence is required from either the complainant or the charged member, the involved parties will be informed. If the complaint is deemed to be without merit, the charges will be denied, and the parties involved will be so informed.

If the complaint is deemed to be worthy of review, the parties will be notified. In a case were timing is crucial, parties will be informed via e-mail. The charged member will be given 30 days to reply in writing to the complaint. If no reply is received, the committee will assume that the charges are valid, and will move to implement an appropriate penalty.

If a reply is received, a hearing will be scheduled involving an Ethics Review Board and the parties to the complaint.

12.8.6 Hearing

An Ethics Review Board will be impaneled consisting of:

- Four members of the Ethics Committee (Voting members)
- A member of the International Board (Voting member)
- A sitting chapter officer (Voting member)
- The Association legal resource (Non-voting member)

Both the charged individual and the complainant will be required to attend a conference call with the Review Board to discuss the charges. Both sides will be permitted to express their views of the situation.

12.8.7 Decision

At the close of discussion, the parties to the dispute will be asked to drop off of the conference call. The Review Board members will then discuss the situation and attempt to reach a decision.

A super majority (2/3 – 4 members) affirmative vote is required within the Review Board to find a member guilty of an ethics violation.

If the member is found guilty of an ethics violation, the Review Board will advise the International Board to consider an appropriate penalty based upon the severity of the offense. Penalties may include:

- Written reprimand
- 1-year probation
- Expulsion from membership

The parties will be notified by registered mail of the decision of the Review Board. The Review Board will also formally notify the International Board of its decision through a report giving all known facts, the findings, and the recommended penalty

12.8.8 Confidentiality

Decisions involving membership and ethics violations are private matters between the Association and the members involved. No details of the decision will be communicated to any third party by any member involved in the decision. Any member violating this restriction will be charged for violating the Association Code of Ethics.

A summary of all ethics complaints will be prepared without specific names for the Director of Operations to present at the next ISSA International Board Meeting. A finding of guilt will be communicated to the ISSA International Board in detail along with recommended action.

12.8.9 Appeal

The charged member, if found guilty, may file an appeal to the International Board within 60 days of the notice of decision. Failure to appeal will indicate consent to the decision. Such appeal may question only whether the proper procedures were followed, and if the penalty was suitable to the offense.

The International Board will review the materials provided by the Committee, and will determine if the proper guidelines and procedures have been followed. The Board will notify the parties involved.

12.8.10 Recording the Decision

The management company will be charged with recording the decision, and with performing any steps required to implement the decision.

12.8.11 Review of Membership Applications

New and renewing membership applications will be reviewed against the filed records by the management company to ensure that those previously convicted of offenses are not readmitted.

12.8.12 Periodic Review

The Committee will periodically review the ethics review guidelines and the decisions handed down to ensure that the process is appropriate and fair.

Appendix A

ISSA Ethics Complaint Form

Date Filed: _____

SUBMITTED BY:
Name: _____
Company: _____
External Address: _____
_____
Email Address: _____
Phone: _____

ACCUSED:
Name: _____
Company: _____
External Address: _____
_____
Email Address: _____
Phone: _____

Detailed Description of Alleged Violation (Use as much space as needed):

_____

_____

_____

_____

_____

Sources of Information (and corresponding contact information):

_____

_____

_____

_____

_____

Section of ISSA Code of Ethics Violated:

_____

Please attach all supporting evidence and email to:
Ethics@ISSA.org

Appendix B – Sample Notification Letter

[DATE]

Dear XX:

The Information Systems Security Association, Inc. (ISSA) and its Ethics Committee are committed to enforcing the ISSA Code of Ethics and Review procedures as contained in the ISSA Operations Manual. As a member of the Association, you agreed to abide by the Association Code of Ethics when you joined. The Code of Ethics is enclosed here and online in the Association file library for your review. It states the following:

> *The primary goal of the Information Systems Security Association, Inc. (ISSA) is to promote practices that will ensure the confidentiality, integrity; and availability of organizational information resources. To achieve this goal, members of the Association must reflect the highest standards of ethical conduct. Therefore, ISSA has established the following Code of Ethics and requires its observance as a prerequisite for continued membership and affiliation with the Association.*
>
> *As an applicant for membership and as a member of ISSA, I have in the past and will in the future:*
> - *Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;*
> - *Promote generally accepted information security current best practices and standards;*
> - *Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;*
> - *Discharge professional responsibilities with diligence and honesty;*
> - *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; and*
> - *Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.*

The ISSA Ethics Committee has received a written complaint concerning activities on your part that are alleged to have violated the Association Code of Ethics. Additional information concerning this alleged violation has also been obtained and placed in a file located at ISSA headquarters. Attached is a copy of that complaint and information contained in the file.

The ISSA Ethics Review Board will convene to consider the complaint, its allegations and pertinent information concerning this potential violation of the ISSA Code of Ethics by teleconference on (date). The Ethics Review Board will consist of six persons who will serve as a fact-finding and decision-making body to determine if there is evidence of a violation of the ISSA Code of Ethics and to determine if action should be taken by the Association. A finding of violation of the ISSA Code of Ethics violation must be agreed upon by a 2/3-majority vote of the Review Board. All actions will be reported to the ISSA International Board for action. You will be informed of the decision of the Review Board.

An appeal of the Ethics Review Board finding and recommendation, allowing for procedural corrections only, for the record and not a rehearing, may be made in writing within 60

days of the date of a report from the Review Board being mailed to you. At the end of that 60-day period the International Board will review the report and any appeal which may be filed.

If you or a representative would like to present evidence and/or attend the Ethics Review Board hearing by teleconference or otherwise as may be scheduled by the Ethics Review Board, you must send written notice of this fact and identification of who will attend or participate to Ethics@ISSA.org no later than 5 p.m. ET, (date). If by representative, please identify this representative by name, title and contact information (either home or business address and e-mail address). You will be assigned a scheduled hearing time on (date) based on current scheduling availability. If you or a representative will not be attending or participating in person and would like to submit written evidence or a written statement only, it must be submitted and received by 5 p.m. ET, (date).

Attached please also find a listing of Ethics Committee members and others who may be called upon to participate in the Ethics Review Board hearing. The members of the Ethics Review Board will be selected from this list of persons. They will be reviewing the complaint and all information in the file. If there are members of the Ethics Committee or others who may participate in the Ethics Review Board work listed here who you feel may be unable to fairly and objectively review and take action with respect to this matter, please forward in writing an identification of such individual(s) and a complete written explanation as to why the individual(s) is or are in your opinion unsuited to review this matter. Such objections should be received by no later than 5 p.m. ET, (date).

If (a) you choose not to appear or to present evidence contrary to the complaint and information contained in the file, or (b) you choose not to appeal a decision and recommendation of the Ethics Review Board, it will be understood that you agree with and waive any and all objections to these proceedings and any action that may be taken.

Sincerely,
[Information Systems Security Association]

(Name) _____
(Title) _____

12.9 Disclosure of Relationships Process

Intent: ISSA members hold our professional and the association's reputations as a priceless asset, and any appearance of impropriety or conflict of interest could irreparably tarnish the value. Also, ISSA desires to set and uphold ethical standards of behavior across the industry and ensure that our internal practices are above reproach.

Policy: All members of the ISSA International Board and the ISSA Ethics Committee are required to complete a form annually and submit it to the ISSA Ethics Committee by sending softcopy to: Ethics@ISSA.org.

Previously Approved, Resubmitted as Inclusion:

This process serves to assist in determining actual or potential conflicts of interest and allows for appropriate protections to be implemented. Each covered individual will objectively list and share information regarding relationships where financial, professional and personal interests exist.

The form is to be completed annually, realizing information of potential relationships in the previous two years. It is also required that should there be a change in the relationships, that a new form be filed within thirty (30) days of the change of relationship. Feedback in the form of suggested activities to obviate conflicts of interest will be delivered to each submitter within four (4) weeks.

These submissions will be treated with the utmost confidentiality. Review will be by a five (5) person subcommittee of Ethics Committee Members, three members constituting a quorum. The names of the Committee Members shall be provided to the ISSA Board of Directors. Review will be further limited to only necessary ISSA Board Members and counsel on a need-to-know basis. The Ethics Committee will provide a summary to the ISSA Board detailing all conflicts or potential conflicts.

While it is anticipated that almost all, if not all relationships can be disclosed on the form, it is acknowledged that there may be a situation in which the member required to disclose has a relationship with another entity or individual in which that entity or individual requires nondisclosure of it or their identity. The subcommittee will discuss the parameters of the disclosure with the member required to disclose. If the member still requires nondisclosure, they will be required to sign an affidavit with general identifying information such as the city or state of the entity and general nature and length of time of their involvement. The member required to disclose shall include in that signed affidavit that there is no conflict of interest. It is anticipated that if a conflict shall become apparent even after the signed affidavit, the Ethics Committee would then recommend appropriate action.

All ISSA members running for election to any position on the ISSA International Board of Directors shall be informed of the requirement to disclose relationships.

DISCLOSURE OF RELATIONSHIPS

A. DEFINITIONS

1. "You" means yourself, your immediate family, a significant other or a trust of which any of these individuals are members, trustees or beneficiaries.

2. "Ownership" means any percentage (%) of ownership in a closely or privately held sole proprietorship, corporation, limited liability corporation, limited liability partnership, partnership or similar entity. Ownership shall also include any non-profit organization or foundation. Furthermore, ownership is having at least a $50,000 stock position in a publicly traded company.

3. ISSA" means the international organization or its chapters and other sub-entities.

4. "Business Relationship means a financial or economic involvement. Business relationship also means involvement with a non-profit organization, a foundation or for which professional services are provided, whether there is a financial or economic component

5. "Indebted" means any individual or closely or privately held entity as described in Paragraph 2 above to which you (as described in Paragraph 1 above) owe money. Indebted also means any publicly traded corporation to which you owe at least $50,000.

6. "Employment" means all entities from which the person filling out this form and his/her spouse or significant other has received earned income during the last two years.

B. DISCLOSURES

1. List all places of employment you or your spouse/significant other have been employed by in the last two (2) years.

_____

_____

_____

_____

2. List all entities in which you either have an ownership or which you are indebted to or employed by that have an ISSA business relationship of which you are aware. Please provide applicable information within the two years

preceding the submission of this form.

3. List all entities in which a customer, vendor, employee, contractor or other entity has a business relationship with an entity in which you are employed or have an ownership interest that have an ISSA business relationship of which you are aware. Please provide applicable information within the two years preceding the submission of this form.

4. List all individuals on the ISSA Board of Directors, all ISSA Committees, Chapter Officers, or contract management companies with which *you* have a *business relationship*. Please provide applicable information within the two years preceding the submission of this form.

I CERTIFY THAT THE INFORMATION CONTAINED IN THIS STATEMENT IS TRUE, COMPLETE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF. I AGREE TO SUPPLEMENT THIS DISCLOSURE FORM WITHIN THIRTY (30) DAYS OF ANY SUBSTANTIAL CHANGE. IF ANY PART HAS BEEN LEFT BLANK, I HAVE DONE SO INTENTIONALLY BECAUSE THERE IS NOTHING TO REPORT.

DATE **SIGNATURE**

ISSA TITLE: