

CIISec Code of Conduct & Ethics

Introduction

A profession is distinguished by certain characteristics, including:

- mastery of a particular intellectual skill, acquired by training, education and experience;
- adherence by its members to a common set of values and code of conduct; and
- acceptance of a duty to society as a whole.

Objectives

This code of ethics recognises that the objectives of the information security profession are that its members should work to the highest standards of professionalism and that their work should fully satisfy the needs of all stakeholders and those of society as a whole. These objectives require that three basic needs are satisfied, namely:

- **Trust** - for employers, clients, regulators, other interested parties and for society as a whole there is a need for trust in information and information systems and in the practitioners working in those fields
- **Quality** - there is a need for assurance that all services obtained from an information security professional are carried out to the highest levels of performance
- **Standards** - users of the services of information security professionals should be confident that a framework of professional ethics and technical standards exists, which governs the provision of those services.

Values

In order to achieve the objectives of the information security profession, CIISec has identified four core values that all members shall be required to observe:

- Honesty
- Diligence
- Objectivity
- Integrity

Code of Conduct

This code of conduct is intended to guide members in their professional and personal conduct.

Members of CIISec shall:

- Act at all times in accordance with CIISec's values;
- Maintain competency and currency in their respective fields;
- Promote best practice in information security;
- Act only within their level of competence;
- Promote and carry out professional services in accordance with the relevant technical and professional standards;
- Act within the law;
- Act in a manner consistent with the good reputation of CIISec and the profession;
- Respect the confidentiality of information acquired during the course of their duties and should not use or disclose any such information without proper and specific authority or unless there is a legal or professional requirement to do so;
- Recognise the potential for any conflict of interests and, where appropriate, take steps to resolve or avoid any such conflict;
- Support the professional education and development of other members of the profession and other individuals involved in information security.

Changes to the Code of Ethics

Any changes to the Code of Ethics and the associated disciplinary process must be agreed by the Board of CIISec. The Disciplinary Committee can make recommendations to the Board in this regard.

Disciplinary Process

In becoming a member of CIISec a member accepts the Chartered Institute's code of ethics and agrees to be bound by the associated disciplinary process.

A Disciplinary Committee will oversee the disciplinary process. The Disciplinary Committee will be appointed by the Board of CIISec and may contain independent non-members. The Disciplinary Committee will be concerned with any complaints or issues relating to CIISec's Code of Ethics.

Complaints, which must be submitted in writing, can be submitted to the Disciplinary Committee by other members or by those associated with the defendant's work or by a member of the public. Complaints will be registered in a complaint register and will be tracked regarding progress.

In most cases, a sub-committee or work group will be appointed to investigate each complaint. Those appointed to the investigation sub-committee will include subject experts in the matter being investigated and may include independent non-members.

The investigation sub-committee will investigate the complaint. The defendant will be notified by the sub-committee and will be entitled to present appropriate information to the subcommittee and, if required, can be accompanied or represented in any meetings with the subcommittee. Following the investigation, the sub-committee will submit a report and recommendation to the Disciplinary Committee.

In the event of a complaint, the register of members would indicate that a complaint had been received and was under investigation.

Any complaint must relate to actions or activity that have occurred within the last 12 months. It is expected that most complaints would be dealt with within 6 months and a maximum of 12 months.

The sanctions, which the Disciplinary Committee can impose, are:

- Reprimand;
- Severe reprimand;
- Suspension; and
- Expulsion.

As an alternative or in addition to any of the above sanctions a fine may be levied up to a maximum figure as agreed by the Board.

Whenever a sanction is imposed by the Disciplinary Committee, the length of the sanction and, if appropriate, the reinstatement process will also be specified.

The Disciplinary Committee will review the report and recommendations from the investigation sub-committee and will make their own judgement. The judgement will take into account the defendants track record and behaviour prior to the complaint. If the judgement is for any form of sanction, then this will be entered on the register of members.

Both the defendant and the complainant can appeal the initial decision made by the Disciplinary Committee. For each appeal the Disciplinary Committee will appoint an appeal sub-committee.

Cotswold House, Haddonsacre
Station Road
Offenham
WR11 8JJ

Contact
Email: enquiries@ciisec.org
Phone: 0203 384 0399
Company Number RC000901



All the members of the appeal sub-committee will not have had any involvement in the investigation or the review by the Disciplinary Committee. The appeal sub-committee will submit a report and recommendations to the Disciplinary Committee and a final decision will be made. The members register will be updated accordingly.

The results of any complaint will be made available to members of CIISec, those initiating the complaint or to a member of the public, upon request, while any penalty is in force.