

Code of Practice - Security Consultancy

Contents

Page

Foreword	1
1. Terms and definitions	3
2. The consultancy	4
3. Personnel	5
4. Competence and training	7
5. Consultancy services	7

Foreword

As a Code of Practice, this takes the form of guidance and recommendations. It should not be quoted as if it was a specification and particular care should be taken to ensure that claims of compliance are not misleading.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

1. Terms and Definitions

For the purpose of this Code of Practice, the following terms and definitions apply.

1.1 customers

Individual, public or corporate body retaining the services of a consultancy

1.2 consultancy

Individual or organisation that is the prime provider of security consultancy services. This applies to a security consultant acting in a self-employed capacity, a sole trader, a partnership or an incorporated company.

1.3 security consultant

Individual giving advice about:

- a) Security precautions or processes in relation to any risk to property, the person or other tangible/intangible assets;
- b) The use of any services involving the activities of security operatives

1.4 security operative

individual or company that performs activities relating to the provision of security services

1.5 suppliers

Individual or company (and the persons employed, including all levels of subcontractor, by that individual or company) that provides the consultancy with information, equipment and /or labour which is used in providing the service to the customer

1.6 technical experts

Individual who provides specific knowledge or expertise for the fulfilment of the contract

2 The Consultancy

2.1 Professional integrity

The security consultant/consultancy

- a) Will provide its services solely in the interests of the customer and will inform clients and prospective clients of any special relationship or circumstances that could be considered a conflict of interest.
- b) Will view and handle as confidential all information concerning the affairs of the client.
- c) will not take personal, financial, or any other advantage of inside information gained by virtue of the consulting relationship
- d) Will only accept assignments for and render expert opinions on matters they are eminently qualified in and for.
- e) Will not accept an assignment for a client while another consultant is serving that client unless assured that any conflict is recognized by and has the consent of the client.
- f) will not review the work of another consultant who is still engaged with the client, without such consultant's knowledge
- g) will not be known as investigators and will not advertise themselves as such
- h) Will not engage in any of the following activities: divorce, domestic investigations, surveillance, skip tracing, repossession of property, or stand alone civil or criminal record checks.
- i) Will not provide undercover or bodyguard personnel. Nothing contained herein prohibits any consultant/consultancy from complying with any law or regulation, by any governmental or regulatory body, which requires that security consultants be licensed as Investigators or any other related license. Security Consultants or consultancies may "investigate" within broad parameters of the definition of the word, in order to determine the needs of their client.
- j) Will investigate only for the purpose of developing information to complete their surveys, design, or testimony, contracting out traditional investigative work to private investigators or similar practitioners. It is understood that a greater level of investigation may be required of those who specialize in fields of financial fraud, art theft, corporate internal theft and fraud, securities fraud, terrorism-extortion, or similar environments, requiring specialized knowledge and experience outside the scope of the routine private investigator.

2.2 Finances

When the consultancy is trading as a sole trader or a partnership, it should prepare annual accounts in accordance with generally accepted accounting standards.

2.3 Insurance

The consultancy should possess public liability and professional indemnity insurance at a level of cover commensurate with the business undertaken, specific contractual requirements and the number of persons employed.

2.4 Premises

The consultancy should have an administrative office(s) where records and business documents, certificates, correspondence, files and other documents necessary for conducting business transactions should be kept in a secure manner.

2.5 Documents and data

Separate records (hardcopy or electronic) should be maintained for each customer, employee and supplier. Records should be kept for a minimum of 12 months from cessation of contract or for the required statutory minimum retention period.

3 Personnel

3.1 Selection and screening

Security screening in accordance with I.S. 999: 2004 should be applied to all individuals in relevant employment including full-time and part-time, temporary and permanent employees, and to all levels of seniority, including directors. Full security screening should be carried out in the case of individuals regardless of their previous employment, even if that was in a previous security environment and shall not be for less than 10 years or from school leaving. All relevant experience and qualifications should be verified.

All employees and/or suppliers and/ or technical experts who have access to information and/or property of the customer and/or the consultancy should be bound by an agreement to keep confidential such information indefinitely unless authorised otherwise in writing or by court order.

3.2 Identification

Persons who have been screened in accordance with **3.1** should be issued with an identity card incorporating as a minimum, the following information;

- a) consultancy name, address and telephone number
- b) name, job title and signature of the holder
- c) the expiry date of the card, not more than two years from date of issue
- d) a current photograph of the holder

3.3 Code of conduct

The consultancy should advise its employees of the obligations under their terms and conditions of employment, in respect of the following;

- a) completing required tasks promptly and diligently, unless there is due and sufficient cause not to
- b) making or signing false statements, of any description
- c) destroying, altering or erasing documents, records or electronic data without permission
- d) divulging matters confidential to the consultancy or customer, past or present,
- e) Without permission.
- f) being unfit for the task through alcohol or restricted drugs
- g) being convicted of a criminal offence(s)
- h) Actions taken by them are such as not to bring discredit on the consultancy, the customer or fellow employees.

Identity cards should be formally withdrawn from persons renewing their cards or leaving the consultancy.

4 Competence and Training

4.1 General

The consultancy should have a clearly defined and documented training policy for its employees. This policy should include a pre-commencement awareness programme, induction training, covering company and employee roles and responsibilities.

4.2 Competence

Security consultants will normally be experts in a specific field or fields as a result of previous experience, however they should be able to verify they have the requisite experience and knowledge through any of the following;

- a) 3 years of documented security consulting experience, verification should be in the form of validated references and a diploma/degree in security management from a recognised institution or the designation of Certified Protection Professional.
- b) An earned baccalaureate or higher degree from an accredited university or college that demonstrates a proficiency in their field of expertise.
- c) at least five years of broad security experience in paid positions, demonstrating increasing responsibilities, and a diploma/degree in security management from a recognised institution or the designation of Certified Protection Professional
- d) There will be a requirement on the consultant to provide proof of Continuing Professional Development on a year on year basis.

4.3 Continuing professional development (CPD)

Consultancies should ensure that their security consultants continue to update themselves with new developments within their area of expertise, as they arise. Evidence of CPD should be held by the security consultant.

4.4 Records

All CPD and training undertaken should be accurately recorded and endorsed by the trainer or other authorised person.

Training records should be reviewed annually by the consultancy to ensure appropriate training has been provided.

5 Consultancy Service

5.1 Ownership

Ownership of the consultancy should be clearly established and the potential customers should be provided with information of name, address and principals of the consultancy.

If requested, the consultancy should supply the following additional information;

- a) terms and conditions of trading
- b) the type and extent of insurance cover
- c) reference sources of work carried out by the consultancy

5.2 Scope of work

Prior to commencement of any security consultancy service, the consultancy should agree with the customer the scope and extent of the work required. This should be clearly defined and presented to the customer in documented form.

The work should only be undertaken if, after consultation with the customer, it is in the opinion of the consultancy that:

- a) there is sufficient and appropriate information about the scope of work
- b) the consultancy is competent to undertake the work

5.3 Proposal

A clear written proposal should be provided by the consultancy. If accepted by the customer, it should form part of the contract. The proposal document should include:

- a) the terms and conditions under which the work would be carried out
- b) the total costing of the service, and payment terms
- c) the contract period
- d) reference to the scope of work
- e) the obligations of the customer to identify and consult with the consultancy on any specific health and safety requirements that apply, or are likely to apply, during the period of the contract.
- f) Any issues regarding intellectual property rights
- g) A statement including as a minimum the full name and previous experience and qualifications of the security consultant(s) who may be involved in the proposed consultancy service and their relationship with the consultancy

5.4 Contracts

The customer should be asked to agree either:

- a) to provide formal confirmation that they have read, understood and accepted the proposal and terms and conditions; or
- b) a contract document referring to the proposal and terms and conditions

The contract should be agreed and exchanged before work commences

-----o0o-----