CREST. Building trust in the digital world, together

Code of Conduct

CREST Certification Holders

v26 [Issued | 08.06.2026]

Contents

1. Executive Summary

1.1. Introduction

A Code of Conduct sets out the principles, values, standards and rules of behaviour that guide decisions, actions, procedures and systems in a way that contributes to the welfare of Clients and respects the rights of all constituents affected by such operations.

Those involved in providing technical information security advice and Services hold the role of trusted advisers and there are duties arising from this role and obligations owed to others. This activity is outcomes-focused and concentrates on providing positive outcomes which when achieved will benefit and protect Clients.

No Code can foresee or address every issue or ethical dilemma which may arise. Individuals holding a CREST Qualification must uphold the intention of a Code as well as the letter.

1.2. The CREST Code of Conduct for Consultants

This Code of Conduct for holders of CREST Certifications (hereafter referred to as "**Consultants**") contains the basic principles that underpin good business practice and ethics which are all-pervasive. It sets out CREST's conduct requirements to enable Consultants to consider how their actions can achieve the right outcomes for their Clients, and is underpinned by an effective Client complaint handling process.

This Code must be observed in parallel with the CREST Code of Ethics which represents the guiding principles for business judgements.

Consultants are expected to exercise their own professional discretion, ensuring that their decisions can be reasonably justified and meet the requirements of the CREST Codes of Conduct. They should seek advice from CREST if in doubt.

For Consultants that either work for, or are sub-contracted to, a CREST Member Company and are engaged in any element of delivering a Service for which the Member Company has been Accredited by CREST, it must also be observed in conjunction with CREST's Code of Conduct for Member Companies. It means that when providing Services on behalf of a CREST Member Company, they will be held accountable for their actions and as a result it is incumbent upon a Consultant to familiarise themselves and comply with the policies, processes and procedures of that CREST Member Company.

The CREST Codes of Conduct include requirements covering the following headline areas:

- Promotion of Good Practices
- Professional Representation
- CREST Assignments
- Regulations
- Competencies
- Client Interests
- Sanctions
- Ethics
- Responsible Reporting

There are also additional requirements relating to some of the Schemes that CREST manage and it is important that Consultants understand these specific additional obligations when delivering Services under those frameworks.

This Code of Conduct describes the responsibilities of Consultants who should recognise that the Codes are used to support any investigations undertaken by CREST and CREST has the right, where appropriate, to oblige Member Companies to make changes to the company's policies and procedures.

2. Definitions

(i) **"Accredited"** in the context of this Code of Conduct means a Member Company that has successfully completed a CREST audit of its quality processes, data handling procedures, technical methodologies and any other assessment criteria required by CREST for delivery of a Service Accredited by CREST.

(ii) "**Certification**" means the action or process of conferring a CREST Qualification to an individual that represents a level of achievement in a CREST Examination. "**CREST Qualification**" and "**Certified**" shall be similarly construed where context demands.

(iii) "**Client**" in the context of this Code of Conduct, means either an organisation receiving Services from a CREST Member Company utilising Consultants where CREST has been referenced in tender or contractual documentation, or an organisation utilising a Consultant.

(iv) "**Consultant**", in the context of this Code of Conduct, means an individual holding a current CREST Certification. For the avoidance of doubt, this includes all Consultants recognised under an equivalency scheme such as, but not limited to, Offensive Security.

(v) "**CREST Assignment**" means an assignment carried out by a CREST Member Company utilising Consultants. Note that if CREST is referenced in tender documentation but not in contractual documents, the contractual documents must identify this change and clarify the position.

(vi) "**CREST Examination**" means any formal collection of questions, prompts, or other items collected and offered with the intent of evaluating a Candidate's ability, aptitude, knowledge, proficiency, performance, competency, or skill. Examinations will be deemed to be inclusive of all components of an evaluation instrument, whether written questions, hands-on tasks, or any other conceivable exercise including scoring criteria.

(vii) **"CREST International"** means CREST (International), with Company Registration number 09805375, and any or all of its global businesses. **"CREST"** shall be similarly construed.

(viii) "**Employer**" means the company employing or engaging the Consultant.

(ix) "**Member Company**" or "**CREST Member Company**" means a company who has passed the relevant CREST Accreditation requirements, agreed to the CREST Code of Conduct for Member Companies, and has paid any fees associated with membership.

(x) "**Member Application Form**" means the latest completed CREST Member Application Form and associated reference material reviewed and agreed by CREST. Any reports to the Member Company of minor compliance issues will also be considered as being part of the application.

(xi) A "**Region**" means a group of countries in a relevant geographical area as determined by CREST from time to time.

(xii) **"Regional Council"** means a body created to oversee multiple countries in a Region (or a single country as appropriate) and as determined by CREST from time to time, and comprising representatives elected by the Member Companies entitled to vote in a Region.

(xiii) "**Scheme**" means bespoke accreditation programme that requires trusted and Accredited companies utilising skilled and competent individuals with specific skills.

(xiv) "**Service**" in the context of this Code of Conduct includes, but is not limited to:

(a) Penetration Testing; and/or

(b) Incident Response; and/or

(c) Threat Intelligence; and/or

(d) Security Architecture; and/or

(e) Security Operations Centres; and/or

(f) Threat-Led Penetration Testing; and/or

(g) Vulnerability Assessment

(xv) "**Testing**" means the performance of any actions, howsoever occasioned, on a Client computer system or network.

For the purposes of this Code of Conduct, these verbal forms have the following indications:

(a) "shall", "must" and "will" indicate a mandatory requirement

(b) "should" indicates a recommendation

(c) "may" and "can" indicate a permission

(d) "demonstrate" indicates where evidence will be required

3. Scope

3.1. In Scope

(i) This CREST Code of Conduct is intended for all Consultants and will take effect on achieving and/or re-certifying a CREST Qualification. For the avoidance of doubt, this includes those working independently or for a non-CREST Member Company

(ii) Consultants employed by or sub-contracted to a CREST Member Company must familiarise themselves with CREST's Code of Conduct for Member Companies. Codes Of Conduct - CREST

(iii) The components of a Service for a Client include, but depending upon the Service to be delivered may not necessarily limited to:

- Scoping the Service to be delivered; and/or
- Evidence or Intelligence collection; and/or
- Evidence or Intelligence analysis; and/or
- Delivery (of Service or report); and/or
- Sign-off; and/or
- Feedback or Review.

3.2. Out of Scope

(i) This Code of Conduct cannot and is not intended to cover:

(a) Consultants that do not hold a current CREST Certification; and/or

(b) Any assignments undertaken by Consultants that are not conducted as a CREST Assignment; and/or

(c) Any assignments undertaken by Consultants that are not covered by the CREST Accreditation held by a Member Company.

(ii) For the sake of clarity, a CREST Assignment can only be referenced by CREST Member Companies. CREST Member Companies must refer to the CREST Branding Guidelines regarding usage.

(iii) For the avoidance of doubt, this Code of Conduct will come into effect at the point that a CREST Certification is awarded to a Consultant, which includes re-certifications.

(iv) This document will not differentiate between the various types of Services provided by Members Companies in the execution of the information security Services provided to their Clients nor the different specialisms involved in those Services.

3.3. Affirmation

(i) All Consultants that hold a CREST Qualification agree to follow the principles contained in the Code of Ethics and to abide by this Code of Conduct for Consultants, and will be held accountable for any violation.

(ii) Consultants will be required to reaffirm their commitment to this Code of Conduct through the re-certification of their CREST Qualification or by being awarded certification in another discipline Certified by CREST.

3.4. Disclaimer

(i) CREST accepts no responsibility for the accuracy or validity of assertions or claims made by Consultants or CREST Member Companies.

(ii) For the avoidance of doubt, through the Accreditation process CREST prescribes the method and rigor by which Accredited Services should be conducted but does not underwrite the result of the Services provided by CREST Member Companies or Consultants.

(iii) In the course of any investigation into a complaint against the Consultant, CREST reserves the right to disclose a Consultant's Qualification and Certification information to the complainant if it deems such action necessary and appropriate.

Any reference to another organisation's website does not constitute a recommendation or endorsement of that organisation, website or its content by CREST.

3.5. Jurisdiction

The construction, validity and performance of this Code of Conduct shall be governed in all respects in accordance with English law and the Parties submit to the non-exclusive jurisdiction of the English Courts.

4. The Requirements

4.1. Promotion of Good Practices

All Consultants must promote good practices. These include, but are not limited to, the following:

(i) Maintaining their technical information security knowledge at the highest level and keeping up to date with new techniques, and the tools and exploits to carry out information security services to improve the quality of cyber security.

(ii) Ensuring that their Employer or organisation to which they are contracted carries appropriate insurances for the work they are undertaking.

(iii) Promoting the effective use of these methods and tools for other security testers.

(iv) If they are working for or are sub-contracted to a CREST Member Company, ensuring that they are fully conversant with all the policies, procedures and methodologies of that Member Company as referenced in that company's CREST Member Application Form.

(v) Ensuring that they are fully conversant with the complaints resolution procedure and are aware of the CREST measures for resolving complaints. Governance - CREST.

(vi) Evaluating new security tools, techniques and products, assessing their potential benefits and weaknesses and understanding fully the impact on the environment that they are to be used on.

(vii) Bringing to the attention of CREST any information pertinent to the community such as a tool that is found to be malicious, changes to legislation that might impact on the ability to carry out assignments, and contractual difficulties associated with handling assignments in foreign countries.

(viii) Making recommendations to CREST for changes in the methodologies detailed by CREST for consideration and evaluation by CREST.

(ix) Ensuring that those working under their authority or supervision are competent to carry out the tasks assigned to them and take responsibility for both their own actions, omissions and decisions and those of individuals working under their supervision.

(x) If they become aware that their Employer or the organisation to which they are contracted has committed an unlawful act, making every effort to dissuade that entity from continuation. If a Consultant is uncomfortable about performing such action, they can report the matter to CREST.

4.2. Professional Representation

All Consultants will represent CREST to the public in a professional manner preserving CREST's reputation at all times. They agree to adhere to the following:

(i) To undertake to use the CREST logo and branding in CVs and other correspondence in accordance with the CREST Branding Guidelines that have been provided to them when their CREST Qualification was conferred. For the avoidance of doubt, they may only use the CREST name in relation to their own name (CVs etc.) and **ONLY** if they hold a valid CREST Certification. For the avoidance of doubt, they may **not** imply nor state any Company Membership.

(ii) To ensure that the CREST logo is used on tender documents, contracts and reports if the CREST Member Company for whom they are working or sub-contracted to is undertaking an assignment using the CREST name.

(iii) To accurately describe the CREST Qualification they hold.

(iv) Not to advertise, publish, nor authorise the same for publication, any article in any medium that is derogatory or disparaging to CREST or to the dignity of the industry or another individual, nor shall they authorise the same to be written or published by others. They will not act in any way to bring CREST into disrepute, all of the aforementioned as determined by CREST in its sole discretion.

(v) When called upon to give an opinion in their professional capacity, to the best of their ability, to give that opinion in an objective manner based upon their best available knowledge and information and shall clearly state any limitations or qualifications to that opinion.

(vi) Not to misrepresent or withhold information relating to the performance of products, tools, systems or Services (unless bound by confidentiality), nor to take advantage of the lack of pertinent knowledge or inexperience of others in order to mislead or misrepresent.

(vii) Where they change Employer, they will be entitled to use the experience gained in their previous employment but not confidential information of any description that was acquired or received by them in the course of that previous employment.

(viii) To discharge their activities with complete fidelity and to safeguard and ensure the confidentiality of data and research from previous assignments, and undertake not to make use of such data or research in other assignments.

(ix) Where a Consultant is also a member of another trade or professional body, the clauses in any other applicable Code of Conduct cannot be used to diminish or negate the clauses in this CREST Code of Conduct.

4.3. CREST Assignments

When working for, or contracted to, a CREST Member Company, all Consultants must define information security assignments in accordance with the method described in the CREST Application Form of the CREST Member Company they are representing if the CREST name is being used in that CREST Assignment. They must act professionally as an information security professional and use appropriate techniques and tools. They must:

(i) Understand their limitations of information security and associated specialist knowledge. They must seek advice or guidance from appropriately qualified colleagues who have the necessary expertise for any areas that are beyond their abilities or that they are not qualified for. They must not make misleading claims about their expertise.

(ii) Ensure that any information security assignment that they undertake is covered by appropriate contract terms and that all local legislation of the country in which the Assignment is being run and any sectoral requirements have been correctly authorised and are complied with.

(iii) Not exceed the scope that is detailed in the contract for any Assignment.

(iv) Fully understand the corporate objectives that underpin the proposed Assignment, the scope, any issues, the constraints, and any risks that need to be addressed.

(v) Understand the desired business benefits for the Client as a result of the Assignment and how they will be measured.

(vi) Recognise the scope and applicability of any techniques or tools and resist any pressure to:

  (a) use inappropriate methods

  (b) use methods that do not comply with the methodologies described in the CREST Application Form of the CREST Member Company they are representing.

(vii) Fully explain the deliverables of the Assignment.

(viii) Offer constructive written challenge if:

  (a) the Client or Member Company requirement is unrealistic;

  (b) any of the Member Company or Client's expectations are unreasonable;

  (c) any Client or Member Company requests are illegal or unethical

  (d) their professional advice is overruled which would result in danger or loss for the Client. In these cases, the likely consequences must be outlined in writing to the Client.

(ix) Devise an acceptance strategy that will fairly demonstrate that the requirements of the project have been met.

(x) Ensure that if an Assignment is delivered for Services that the Member Company has not been Accredited by CREST to deliver, that any report provided to the Client clearly states that the Services are not covered by the company's CREST Accreditation.

(xi) If working for or contracted to a CREST Member Company, be fully aware of the escalation/ exception procedures to be followed in the event of deviation from the Assignment as documented in the CREST Member Application Form.

(xii) Conduct CREST Assignments in accordance with the methodology defined in the CREST Member Company's Application Form.

4.4. Regulations

All Consultants must maintain a thorough understanding of relevant regulations and guidelines. In particular, they must:

(i) Follow the standards and regulations relevant to the information security assignment as related to its geographical location, nationality, technology, security tool development and methodologies.

(ii) Use tools and techniques in an effective and intelligent manner to achieve well-engineered results.

(iii) Keep up to date with new standards and regulations and promote their adoption as appropriate.

(iv) Ensure that they are up to date with the substance and content of the legal and regulatory frameworks of the country in which they are working including, but not limited to: data protection; computer misuse; health and safety; copyright; and geographical and industry specific legal and regulatory frameworks.

(v) Act at all times in a manner that gives full effect to their obligations under such legal and regulatory frameworks and encourage their colleagues to do likewise.

(vi) Seek professional advice at an early stage if they have any doubts as to the appropriate application of the law or regulations.

(vii) Follow and comply with the policies, procedures, standards, guidelines and measures as defined in this Code of Conduct and, if working for or sub-contracted to a CREST Member Company, follow and comply with the policies, procedures, standards, and guidelines defined in the CREST Member Company Application Form for the Accredited Service they are delivering for the CREST Member Company they are representing.

(viii) When engaged in Assignments abroad, they must comply with local legislation and regulation. Consultants should adhere to local ethical guidance and good practice, and follow the guidance of CREST if in doubt.

4.5. Competencies

All Consultants must maintain their technical competencies. They must:

(i) Keep up to date with technological advances through training, technical publications and specialist groups within professional bodies and recognise that information gained solely from the internet may not be validated.

(ii) Undertake to inform CREST immediately of matters affecting their capability to continue to fulfil the requirements of any relevant information security certifications they hold, including CREST Certifications.

4.6. Client Interests

All Consultants must respect the interest of the Client. They must:

(i) Not disclose to any third party, formally or informally, any information about the Client or its competitors without the specific approval of the Client and/or unless obliged to do so by law.

(ii) Declare any personal gains, financial or otherwise, that they may make from any proposed work and not falsify or conceal information for their own benefit.

(iii) Only accept those Assignments for which they are qualified and competent to undertake, and recognise that they have a responsibility to inform the Client if there is a question about the technical value of a particular Assignment, or another aspect of the Assignment.

(iv) Safeguard the confidentiality of all information concerning the Clients.

(v) Ensure that they utilise professional judgement and act with professional objectivity and independence at all times. In this respect, "independence" is taken to mean "independence of relationships which might be taken to impair objectivity".

(vi) Disclose any interests in products which they may recommend to the Client.

(vii) Avoid any situation that may give rise to a conflict of interest between themselves and the Client.

(viii) Not handle Client finances or place orders in the Client's name without prior written permission from the Client.

4.7. Sanctions

If CREST receives evidence of a breach of this Code of Conduct by a Consultant, or if evidence is found that they have accessed illegitimately sourced or unauthorised documentation to prepare for a CREST Examination, sanctions may be applied which include (but are not limited to):

(i) Immediate revocation of all CREST Qualifications held by the Consultant in question;

(ii) Bar on attempting CREST Examinations. CREST reserves the right to set a period of time for such a bar or to invoke such a bar indefinitely;

(iii) Legal action, for a breach of the Non-Disclosure Agreement;

(iv) Legal action, for theft of intellectual property;

(v) Informing appropriate third parties if the decision is suspension, revocation of a CREST Certification or removal from the CREST register.

4.8. Ethics

(i) Consultants agree to abide by the CREST Code of Ethics. Code of Ethics - CREST

(ii) Consultant must show respect for the personal and professional dignity of others and act in a non-discriminatory and inclusive manner at all times and shall not conduct themselves in either a physical or verbal manner that is intimidating, harassing, abusive, derogatory or demeaning.

4.9. Responsible Reporting

All Consultants should practice Responsible Disclosure if they identify serious vulnerabilities on a system during routine, legitimate Testing or whilst engaged in any analysis or evaluation of a business in order to prevent or limit potential damage to the maximum possible extent. They should:

(i) Expeditiously and securely report serious vulnerabilities found to the vendor or system owner, which may be the Client, in a responsible manner. They must balance the need for the public to be informed of security vulnerabilities against the need for the vendor or system owner to be given time to respond effectively;

(ii) Ensure reporting includes sufficient information to allow the vendor or system owner to verify and evaluate the risk;

(iii) Make best efforts to prevent further exploitation that could adversely affect product or system availability, data integrity and confidentiality breaches;

(iv) Show respect and support to all parties involved;

(v) Ensure open and positive communication channels and show mutual respect and transparency;

(vi) Make best efforts to ensure a co-ordinated approach to disclosure;

(vii) Advise Government or Regulatory Bodies appropriately;

(viii) Not demand or expect credit for disclosure;

(ix) Not seek or expect to profit (disproportionately) from such disclosure;

(x) Seek advice from CREST as necessary.

5. Signatures

Your signature below indicates that you have:

(i) Read this Code of Conduct (version 26); and

(ii) Accept the terms of this Code of Conduct; and

(iii) Agree that your data may be shared with the CREST (International) Council, other CREST Regional Councils, and appropriate third parties if necessary.

CREST		**CONSULTANT**	
Signature:		Signature:	
Print Name:		Print Name:	
Position:		Position:	
Date:	*As per Consultant's signature*	Date:	

Amendment List

This document has been amended in the areas described below:

a. Section reference b. Clause Reference c. Date Issued	Description of Changes	Authorised by	Version No. issued
a. 6 b. 6.2 c. 28.09.2022	OVS icons added	Elaine A Luck	21
a. 6 b. 6.6 (6.6.4 new) c. 28.10.2022	Clarification of use of logo by CREST Qualified Individuals	Elaine A Luck	22
a. 3 b. 3.2.2 (v) c. 12.01.2023	New clause	Elaine A Luck	23
a. 3 b. 3.3.1(ii) & (iii) c.12.01.2023	Assignment terms clarified	Elaine A Luck	23
a. 3 b. 3.8.2 c. 12.01.2023	Amended to cover ethical principles	Elaine A Luck	23
a. 6 b. 6.2 c. 15.12.2023	Errors in STAR and STAR-FS logos corrected	Elaine A Luck	24
a. Throughout b. c. 15.12 2023	Reference to Chapters replaced by Local Council. Appropriate definitions added.	Elaine A Luck	24
a. 3 b. 3.7.1 c. 09.02.2024	Clarification that access to unauthorised exam preparation material may result in sanctions (inc. definition of CREST Examination)	Elaine A Luck	25
a. Throughout b. c. 13.05.2026	Section 5 – Complaints Handling Process removed Branding guidelines removed Definitions (e.g. Consultant) clarified and references adjusted throughout Reference to Local Councils replaced by Regional Councils	Elaine A Luck	26
a. b. c.		Elaine A Luck	
a. b. c.		Elaine A Luck	
a. b. c.		Elaine A Luck	

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

Press / Public Relations: media@crest-approved.org