CREST. Representing the technical information security industry

Code of Ethics

For suppliers of CREST Accredited Services

v5.0 [Issued] / 10.01.2023

Contents

Purpose

A Code of Ethics is a set of principles designed to influence the judgement of individuals to ensure that they conduct business with honesty and integrity in any given situation. It describes the core values that should guide independent decision-making and provides ethical standards to be followed by Member Companies and their Consultants. Ethical guidance does not grant exemption from professional standards of due skill and care.

All revisions to the Code of Ethics will be notified to principal points of contact in CREST Member Companies and on the CREST website.

Some outline guidance on compliance is provided for information in Annex B.

Definitions

"**Accredited**"	in the context of this Code of Ethics 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.
"**Approved**"	in the context of this Code of Ethics means a Member Company that has been successfully Accredited for a Service and has demonstrated that it has skilled and competent Consultants.
"**Bribery**"	defined as an offer or giving of a financial or other incentive to someone, with the intention of inducing that person or a third party to perform a function or activity improperly, or as a reward for doing so. Further guidance is provided at in Annex B.
"**Consultant**"	in the context of this Code of Ethics, means skilled person who meets the following criteria: i. the Member Company deems them to be appropriately qualified for the assignment they are involved with; and ii. is providing specialist or expert advice and/or information and/or a service to a Client of that CREST Member Company; and iii. where that advice or information relates to the delivery of a Service for which the Member Company has been Accredited by CREST.
"**CREST**"	means CREST (International) and any or all of its global Chapters.
"**Ethics**"	defined as values relating to human conduct with respect to the rightness and wrongness of certain actions and to the goodness and badness of the motives and ends of such actions.
"**CREST Member Company**"	means means a company who has passed the relevant CREST requirements, agreed to the CREST Code of Conduct, including this Code of Ethics, and has paid any fees associated with membership.

"**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
"**Money Laundering**"	defined as the act of concealing the transformation of profits from and corruption into ostensibly legitimate assets. Further guidance is provided at in Annex B.
"**Operating Executive**"	means the employed staff of CREST that comprise the management team.
"**Service**"	in the context of this Code of Ethics includes, but is not limited to: i. Penetration Testing; and/or ii. Intelligence-Led Testing; and/or iii. Incident Response; and/or iv. Threat Intelligence; and/or v. Security Operations Centres; and/or vi. Vulnerability Assessment.
"**Staff**"	means personnel employed directly by the CREST Member Company, including Consultants, and any personnel engaged through a sub-contractor.

Scope

The Code of Ethics is intended for Members Companies and their Consultants who use the CREST name professionally.

This Code of Ethics cannot and is not intended to cover companies who are not Members of CREST nor Consultants that are not delivering services for a Member Company.

This document is written for CREST Members Companies and their Consultants who provide cyber security services to any sector of the business community including Regulators in the UK and overseas. It does not differentiate between the various types of services provided by CREST Member Companies in the execution of the information security services provided to their Clients, nor the different specialisms involved.

This Code of Ethics forms a binding codicil to the CREST Code of Conduct for Member Companies and the CREST Code of Conduct for Consultants Engaged in CREST Accredited Service Delivery. It should be read in conjunction with these Codes of Conduct.

Affirmation

All Member Companies and Consultants agree to abide by the Code of Ethics and be able to demonstrate how it has been applied.

Member Companies and Consultants reaffirm their commitment to the Code of Ethics through the renewal of their membership, including individual CREST certification.

Sanctions

A breach of the Code may not always involve misconduct and lead to sanctions being applied. However, a proven failure to comply with the Code of Ethics may result in penalties which may include, but are not limited to, expulsion from CREST.

The CREST Operating Executive has the right to investigate and to make judgements on formal complaints received about a CREST Member Company's conduct or the conduct of a Consultant. In such instances, the CREST Complaints Handling Process will be initiated.

Disclaimer

CREST accepts no responsibility for the accuracy or validity of assertions or claims made by CREST Member Companies in their CREST Member Company Application Form.

Through Accreditation, CREST prescribes the method and rigor by which Accredited services should be conducted and does not underwrite the result of the services provided by CREST Member Companies or their Consultants.

Code of Ethics - Consultants

The Code of Ethics aims to support individuals to conduct themselves in an ethical manner and balance often conflicting interests and demands. They are designed to guide Consultants to meet the highest standards of professional conduct.

Consultants are expected to exercise their own judgement which should be made in such a way as to be justifiable and defensible and endorse the spirit of CREST's Code of Ethics.

In order to distinguish members from other providers in the cyber security sector, all Consultants agree to abide by the seven principles of business ethics below as a condition of membership.

Honesty

i. To be committed to the highest standards of ethical conduct in all that they do. Members must comply with all applicable legal and regulatory requirements governing business relationships.
ii. Members must subscribe to honesty and integrity engendering trust and conduct their business accordingly, and must comply with all applicable laws and regulations.

Prohibition of bribery, corruption and extortion

i. Members must not offer, promise, give, demand or accept bribes or other unethical inducements, including extortion, in order to obtain, retain or give business or other advantage and take all reasonable measures within its power to ensure that its Staff, including any sub-contractors, follow the same practice.

Competition

i. Members must compete fairly and vigorously in their market sector and not engage in, nor be party to, any agreements, business practices or conduct that, as a matter of law, are anti-competitive or may be construed as participation in trade or associated cartels.
ii. Members must honestly represent themselves and their own abilities as well as the functionality of their products, employees and contractors and must not make disparaging or unjustified references or comparisons to the products and services of other Members or providers including on social media platforms.

Integrity in business behaviour

i. Members are expected to act with integrity at all times and not to act in any way as to cause detriment to CREST or their Client.
ii. Member Company Staff, which includes sub-contractors, who have access to privileged information must not use it to achieve personal gain for themselves or others and no Staff members, including sub-contractors, must engage in personal activities or pursue financial or business interests which might give rise to, or give the appearance of, conflicts of interest with the Company by whom they are employed or sub-contracted or which might compromise their ability to meet the responsibilities of their job.

Professionalism

i. Members will continuously strive to acquire the professional knowledge and skills required to perform their function, recognising that new tools and techniques are evolving rapidly.

Personal Example

i. Members will be role models for employees promoting professional ability, approach to life and work ethic. They will encourage the display of selflessness, honesty and integrity at all times. They will promote respect amongst their Staff and support an environment of leadership and openness in their dealings with clients.
ii. Members will show respect for the personal and professional dignity of employees, colleagues and other people and entities with whom they come into contact.
iii. Members will always assist fellow members when they need help or advice.
iv. Members will accept responsibility for their own work and the work of those under their supervision.
v. Members will respect intellectual property and give credit or other's work. They will never steal or misuse copyrighted, patented material, trade secrets or any other intangible assets.

Application and Compliance

i. Members must respectfully apply laws, regulations, technical rules and accepted professional standards and must not accept instruction in any form that is incompatible with these.
ii. Members are expected to bring any suspected or actual breach of the CREST Code of Conduct promptly to the attention of CREST. Any Member making such information known to CREST through the appropriate channels will not face any adverse or unfavourable treatment for such disclosure.

Code of Ethics - Companies

CREST ensures that its member companies have the appropriate processes and controls in place to perform the services for which they have been appointed. The combination of independently assessed companies with access to skilled and professionally qualified Staff underpinned by effective and meaningful Codes of Conduct provide the buying community with confidence that the services they wish to procure will be provided by a trusted company with access to demonstrably professional technical security Staff.

The Code of Ethics describes the core values that should guide Member Companies' decision-making balanced with understanding the wider impact of their activities.

The following additional corporate ethical principles must be followed as a condition of membership:

Credibility

i. Member Companies will seek to present the highest standards of objectivity in the delivery of their Accredited Services, their advice and their conduct. They must at all times safeguard company information and intellectual property, recognising the poacher/gamekeeper risks to a client of open source research.
ii. They will use accredited, systematic and verifiable processes and act in ways that are at all times accountable, legal and ethical. They will strive continuously to deliver timely, relevant and accurate Services.

Integrity

i. Member Companies must subscribe to honesty and integrity engendering trust. They must conduct their business in accordance with all applicable laws and regulations and ensure that their Consultants and Staff including, for the avoidance of doubt, any sub-contractors, also conduct business accordingly and comply with such laws.
ii. Member Companies will ensure that any form of payment for information is performed with professional individuals and due diligence is carried out to ensure no funding of criminal activity occurs.

Responsibility and Respect

i. Member Companies will work using initiative and diligence, applying common sense within the scope of their authority and will always take responsibility for their actions. They will never promise more than they can deliver and will be honest about the limits of their professional capability. They will always qualify the veracity of their Services with absolute integrity. They will maintain independence of thought, product and organisation and declare immediately any potential conflict of interest to clients.
ii. Member Companies will deliver responsible reports to clients based on objectivity and integrity, not using ambiguous language. They must ensure that the content of reports is justifiable and based on reasonable, defendable assumptions.
iii. Member Companies will at all times apply good practice to safeguarding data and information including, but not limited to, recognising potential risks to ethical principles.
iv. Member Companies will champion equality of opportunity, diversity and inclusion and support human rights, dignity and respect.

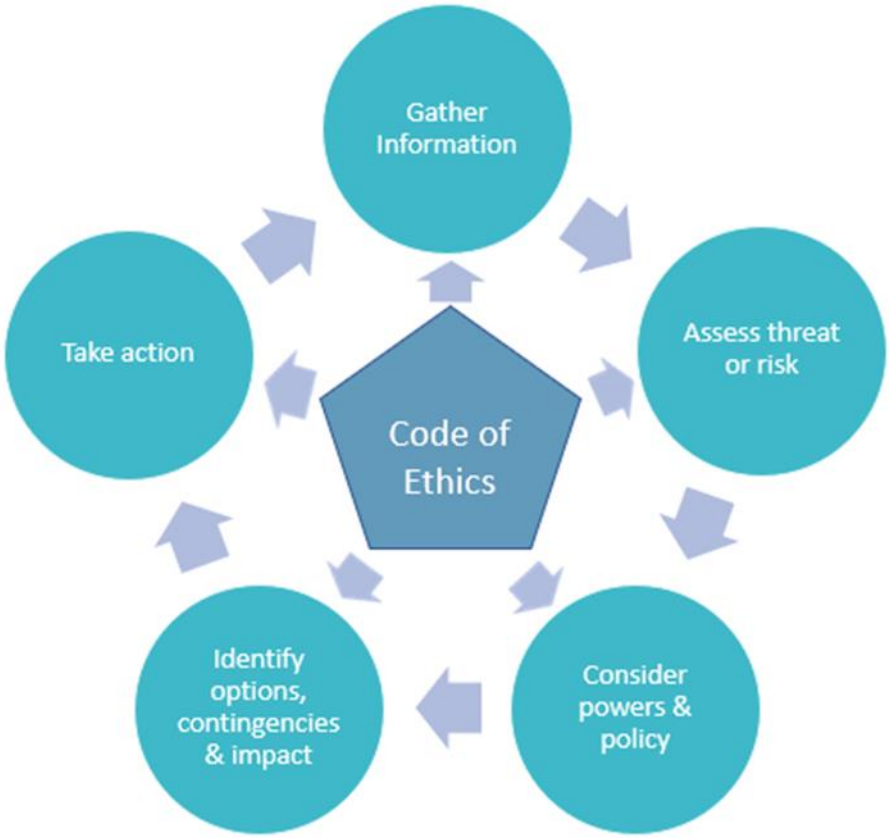
Professionalism

i. Member Companies will uphold and improve the professionalism and standards of the cyber security industry by sharing experiences, opportunities, techniques and tools with the CREST network that they consider of merit or which may represent a potential risk to the industry.

ii. Member Companies undertake to promote and advance public awareness and understanding of cyber security and its benefits.

iii. Member Companies will operate from an evidence-based position and will rebut false or misleading statements concerning the industry or profession and its practices.

Annex A: Decision Model



Annex B: Guidance and Regulations

Guidance: Conflict of Interest, Bribery and Money Laundering

A ***Conflict of Interest*** is typically defined as “a set of circumstances that creates a risk that professional judgement or actions regarding a primary interest will be unduly influenced by a secondary interest”.

It is commonly a situation in which person or organisation is involved in multiple interests, financial or otherwise, one of which could possibly corrupt the motivation or decision-making of that individual or organization.

A conflict of interest policy should include:

- Examples applicable to the business
- How to disclose a potential conflict before it arises
- Protective steps
- Impact to business if conflict arises

Bribery is the illegal act of giving money, goods or other forms of recompense to a recipient in exchange for an alteration of their behaviour (to the benefit/interest of the giver) that the recipient would otherwise not alter.

An anti-bribery policy should be appropriate to the level of risk a business faces and should include:

- the approach to reducing and controlling the risks of bribery
- rules about accepting gifts, hospitality or donations
- guidance on how to conduct business, eg negotiating contracts
- rules on avoiding or stopping conflicts of interest

Money Laundering is the act of concealing the transformation of profits from and corruption into ostensibly "legitimate" assets. Considerable time and effort may put into strategies which enable the safe use of those proceeds without raising unwanted suspicion. Implementing such strategies is generally called money laundering. After money has been suitably laundered or "cleaned", it can be used in the mainstream economy for accumulation of wealth, such as by acquisitions of properties or legitimate businesses, or simply spent. Law enforcement agencies of many jurisdictions have set up sophisticated systems in an effort to detect suspicious transactions or activities, and many have set up international cooperative arrangements to assist each other in these endeavours. In a number of legal and regulatory systems, the term "money laundering" has become conflated with other forms of financial and business crime and is sometimes used more generally to include misuse of the financial system (involving things such as securities, digital currencies, credit cards, and traditional currency), including terrorism financing and evasion of international sanctions. Most anti-money laundering laws openly conflate money laundering (which is concerned with the source of funds) with terrorism financing (which is concerned with destination of funds) when regulating the financial system.

Some countries treat obfuscation of sources of money as also constituting money laundering, whether it is intentional or by merely using financial systems or services that do not identify or track sources or destinations. Other countries define money laundering in such a way as to include money from activity that would have been a crime in that country, even if the activity was legal where the actual conduct occurred.

Anti-money laundering and counter-terrorist financing are now viewed in the context of the wider financial crime agenda, which is increasingly focused on corruption and financial sanctions issues, as well as organised crime. The globalisation of the world economy has emphasised the need for action to be taken collectively at the international level and this has been further emphasised by the continued ease with which funds can be moved around internationally.

Regulation: Bribery, Anti-Corruption and Money Laundering

Official guidance Bribery and Anti-Corruption specifies that, to combat bribery, organisations must adhere to the following six guiding principles:

Proportionate procedures: Measures taken by an organisation to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of its activities. They are also clear, practical, accessible, effectively implemented and enforced.

Top-level commitment: Top-level management of a commercial organisation are committed to preventing bribery and corruption by persons associated with it, and foster a culture within the organisation in which bribery and corruption is never acceptable.

Risk assessment: The organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery and corruption on its behalf by persons associated with it. The assessment is periodic, informed and documented.

Due diligence: The organisation applies due diligence procedures, taking a proportionate and risk-based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified bribery and corruption risks.

Communication (including training): The organisation seeks to ensure that its bribery and corruption prevention policies and procedures are embedded and understood through internal and external communication, including training, that is proportionate to the risks it faces.

Monitoring and review: The organisation monitors and reviews procedures designed to prevent bribery and corruption by persons associated with it, making improvements where necessary.

Compliance

Organisations must comply with their obligations under anti-bribery and anti-corruption regulations. Organisations must be aware that it is a criminal offence to:

- give, promise or offer a bribe, private-to public or public-to-private;
- request, agree to receive or accept a bribe;
- bribe a public official.

Under no circumstances must the giving or receiving be done with a view to anyone obtaining any form of improper advantage.

It does not matter where the offence was committed. If abroad, the law will be applied to all British citizens, UK companies, and anyone normally resident in the UK and most countries have introduced individual criminal liability for bribery related offences.

There is a corporate offence of negligent failure to prevent bribery by persons working on behalf of a business. The offence is one of strict liability, with no need to prove any kind of intention or positive action. It is also one of vicarious liability: a commercial organisation can be guilty of the offence if the bribery is carried out by an employee, an agent, a subsidiary, or another third-party. The location of the third-party is irrelevant to the prosecution. For example, a German business with retail outlets in the UK which pays a bribe in Spain could, theoretically, face prosecution in the UK. However, the commercial organisation has a defence if it can show that, while bribery did take place, it had in place "adequate procedures designed to prevent persons associated with the organisation from undertaking such conduct". The burden of proof in this situation is on the organisation, with the standard of proof being "on the balance of probabilities". Sentences for individuals include 10 years imprisonment and/or unlimited fines.

Providers of CREST services should have in place their own corporate policy on ethics, anti-bribery and corruption. The key elements of such a policy should include:

- Anti-bribery policy
- Communication
- Education, training and guidance
- Responsibility for compliance
- Resources to combat bribery
- Risk assessment
- Due diligence
- Employment procedures
- Gifts, hospitality, donations policies
- Facilitation payments
- Delegated decision-making
- Contractual controls
- Financial controls
- Procurement and commercial controls
- Raising concerns, including whistle-blowing arrangements
- Investigation procedures
- Disciplinary procedures
- Internal audit
- Top management overview and tone

With specific regard to Money Laundering, most countries have legal frameworks in place, institutional regimes and procedure to support international co-operation. An organisation's policies should include measures that support the identification and prevention of embezzlement or misappropriation of property, and abuse of functions.

A copy of an organisation's policy on ethics, anti-bribery and corruption will be reviewed on application to join CREST (International).

All member companies are required to sign up to the CREST Code of Ethics.

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. Throughout b. c. Oct. 2018	Updated throughout to reflect best practice	Elaine Luck	3.0
a. Throughout b. c. March 2022	Updated throughout to reference all Consultants. Additional best practice included from UKCSC workstream activity	Elaine Luck	4.0
a. Consultants b. Honesty (ii) c. 10.01.2023	Clarified	Elaine Luck	5.0
a. Consultants b. Integrity in business behaviour (i) c. 10.01.2023	Amended to include CREST	Elaine Luck	5.0
a. Companies b. Integrity (i) c. 10.01.2023	Clarified	Elaine Luck	5.0
a. b. c.			
a. b. c.			
a. b. c.			

Telephone: +44 (0)20 3058 3122

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

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