CODE OF ETHICS
FOR MEMBER ORGANISATIONS

Version: July 2021

1 PURPOSE

1.1 This Code of Ethics (hereafter referred to as "the Code") sets out the benefit of ethical values to organisational behaviour. It is intended to assure the public and society in general that high standards of professional behaviour will be exhibited. The Code applies to any and all aspects of security professional practice, from boardroom strategies and how organisations treat their employees and suppliers, to techniques and practices employed by practitioners.

1.2 The Code sets out the expectations that the United Kingdom Cyber Security Council (also referred to as "the Council") has for how organisations should behave in any relevant situation and describes the core values that should guide decision-making, while understanding the wider impact of their work.

1.3 All UK Cyber Security Council Member Organisations are required to adhere to the Code which is intended to support them to follow ethical behaviour and they are encouraged to champion the same for their own members and staff via the Guiding Principles for Individuals.

1.4 Member Organisations are expected to bring any breach of the Code to the attention of the Council in a timely and proportionate manner. The determination of breaches rests with the Council whose decision will be final. Any Member Organisation making such information known to the Council through the appropriate channels will not face any adverse or unfavourable treatment by the Council for such disclosure. The process for reporting a breach is defined in the Complaints policy.

1.5 If there is an overlap with locally defined organisational ethics, the highest standard of behaviour will take precedence and the clauses in any other applicable Code of Ethics cannot be used to diminish or negate the clauses in this UK Cyber Security Council Code of Ethics.

UK Cyber Security Council
C/O Providence House
141-145 Princes Street
Ipswich
IP1 1QJ
ukcybersecuritycouncil.org.uk

2 DEFINITIONS

For the purposes of this Code of Ethics, these terms have the following meanings:

- "must" and "will" and "obligation to" indicate a mandatory requirement
- "should" indicates a recommendation
- "may" and "can" indicate a permission
- "demonstrate" indicates where evidence will be required
- "conflict of interest": a set of circumstances that create a risk that professional judgement or actions regarding a primary interest will be unduly influenced by a secondary interest
- "Ethics Committee": a body of independent, impartial and multi-disciplinary individuals empowered to review the content of the UK Cyber Security Council Codes of Ethics and to consider cases where the consistent application of the duly established code may not have been upheld; a Committee with the authority in such cases to apply documented sanctions where they are deemed appropriate.
- "Member": in the context of this Code of Ethics, means an organisation that has passed all the relevant requirements to become a Member Organisation of the Council
- "supply chain": means the individuals, organisations, resources, activities and technology involved in the creation, sales and distribution of a product to the final buyer. This network includes different activities, people, entities, information, and resources.

3 SCOPE

3.1 The Code is intended for all Member Organisations of the Council.

3.2 Member Organisations must, where applicable, encourage their own members and supply chains to engage with the Code.

3.3 This document is written for Member Organisations practicing in the UK and worldwide. It does not differentiate between the various types of services provided by them.

3.4 Guiding Ethical Principles for Individuals are provided separately.

4 AFFIRMATION

4.1 All Member Organisations agree to abide by the Code and be able to demonstrate how it has been applied.

4.2 Member Organisations reaffirm their commitment to the Code through the renewal of their Membership.

5 SANCTIONS

5.1 The Council's Ethics Committee investigate, make judgements and make recommendations on alleged breaches of the Code.

5.2 A breach of this Code may result in sanctions being applied.

6 DISCLAIMER

6.1 The UK Cyber Security Council accepts no responsibility for the accuracy or validity of assertions or claims made by Member Organisations in the conduct of their business or practice.

6.2 The UK Cyber Security Council does not underwrite the services provided by its Member Organisations.

7 THE CODE

In alphabetical order:

7.1 Credibility

Member Organisations will seek to:

i) maintain the highest standards of objectivity in their service delivery

ii) present the highest standards of advice and conduct

iii) act in ways that are at all times accountable and ethical

Case studies that apply to this principle: 1, 2, 3.

7.2 Integrity

Member Organisations must:

i) be honest and act with integrity in the conduct of their activities and services

ii) demonstrate compliance with legislation and regulations

Case studies that apply to this principle: 4, 5, 6, 7, 8.

7.3 Professionalism

Member Organisations will:

i) uphold and improve the professionalism and reputation of the cyber security sector, and be able to evince this by sharing experiences, opportunities, techniques and tools that they consider of merit or which may represent a potential cyber security risk

ii) undertake to promote and advance public awareness and understanding of cyber security and its benefits

iii) operate from an evidence-based position

iv) rebut false or misleading statements concerning the industry or profession and its practices

Case studies that apply to this principle: 9, 10, 11, 12.

7.4 Responsibility and Respect

Member Organisations will:

i) accept appropriate responsibility for what is within their power, control or management

ii) apply, at all times, good practice in respect of safeguarding data and information, including but not limited to recognition of potential risks to an ethical principle

iii) declare immediately any potential conflict of interest

iv) ensure any deliverable is objective, justifiable and defendable

v) champion equality of opportunity, diversity and inclusion and support human rights, dignity and respect

Case studies that apply to this principle: 13, 14, 15, 16.

8 CONTACT US

Please contact us via email at enquiries@ukcybersecuritycouncil.org.uk.

[ends]