GUIDING ETHICAL PRINCIPLES FOR CYBER SECURITY PROFESSIONALS

Version: July 2021

INTRODUCTION

These Principles aim to support those in the cyber security sector to conduct themselves in an ethical manner and balance competing interests and demands in their professional practice. These Guiding Principles are aimed at practitioners within Member organisations, but may include practitioners within non-member organisations.

Member organisations may have their own requirements for individual members. This Guidance is not intended as a replacement, but rather to ensure their requirements include all of the Guiding Principles below. The expectations of the Principles include:

Competition

- not making unjustified references or comparisons to other providers and not engaging in, nor being party to, any agreements, business practices or conduct that are anti-competitive
- not misrepresenting the functionality of their products nor the abilities of their representatives and persons under their control and/or supervision

Case Studies that apply to this principle: 17, 18.

Honesty

- honesty in the conduct of activities and services
- neither making nor endorsing false or unjustified statements

Case Studies that apply to this principle: 19.

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

ukcybersecuritycouncil.org.uk

Registered as a Charity in England & Wales (number 1195030)

Inclusion

- showing respect for the personal and professional dignity of others and acting in a non-discriminatory manner at all times

Case Studies that apply to this principle: 18.

Integrity

- acting with integrity at all times and not acting in any way as to cause malicious detriment to others
- addressing conflicts of interest where known, and where unintended conflicts arise, taking action to report where unintended conflicts arise

Case Studies that apply to this principle: 20, 21, 22, 23, 24, 25.

Lawful behaviour

- demonstrating ethical behaviour and compliance with applicable legislation and regulations, including in other jurisdictions; and taking reasonable measures within their power to ensure that both they and staff working under their control or supervision, including any subcontractors, follow ethical principles
- striving to do more than just comply with legislation and codes

Case Studies that apply to this principle: 26, 27.

Professionalism and role model

- acting professionally at all times
- assisting others when they need help, guidance or advice

Case Studies that apply to this principle: 6.

Responsible reporting

- practicing responsible reporting when cyber security risks are identified, or if unlawful activity is witnessed or suspected

Case Studies that apply to this principle: 28, 29, 30, 31, 32, 33, 34, 35, 36, 37.

Skills, knowledge and competence

- acquiring and maintaining the professional knowledge and the skills required to perform their function as the cyber security sector evolves, seeking support and guidance as and when needed

Case Studies that apply to this principle: 38.

Individuals are expected to exercise their own judgement, which should be made in such a way as to be justifiable and defensible and meet the spirit of the Council's ethical guidance. If individuals are in any doubt, they should seek advice from their professional body or from the Council itself.

[ends]