FOX IT
part of nccgroup

CLASSIFICATION
FOX.PUBLIC

Corporate Social Responsibility policy Fox-IT

Date 1 October 2019
Version 2.0

FOR A MORE SECURE SOCIETY

Corporate Social Responsibility at Fox-IT

For a more secure society

Technology plays a crucial role in many people's individual lives and in society as a whole, and can often be used both for good and for bad purposes. Seemingly benign products and services, such as network sensors or forensic expertise, could be used for bad purposes.

Fox-IT believes that its ethical responsibilities go beyond what is currently prescribed by laws and regulations. Therefore, Fox-IT has instituted this Corporate Social Responsibility (CSR) policy, and the corresponding rules and procedures as described in the section "Customers". We aim to reduce, as much as reasonably possible, the risk that our products and services could be abused for human rights violations.

At Fox-IT, we contribute to the public debate with our technical expertise. Having said that, we focus on our core expertise: technical knowledge about cyber security. .

To start with:

Because technology is our core expertise, this CSR policy focuses on technology. However, there are many more aspects to contributing to a better world.

- Fox-IT respects human rights as described in the Universal Declaration of Human Rights, and civil rights as championed by Freedom House.
- Fox-IT expects the same from its customers. That is why we think about what services and products we want to deliver to which customers. Export regulations are the baseline but not our only restriction. (See "Customers", below.)
- Fox-IT does not bribe and does not accept bribes in any way.
- The core asset of Fox-IT are the Foxers, so we provide a good working environment and, at a minimum, act in accordance with employment laws and regulations.
- The environment is important. When developing services and products, Fox-IT takes the effect on the environment into account. Furthermore, we also encourage Foxers to implement concrete actions into our (internal) processes that are beneficial for our planet.
- To avoid any doubt, Fox-IT obeys the laws and regulations applicable to Fox-IT, regardless of whether or not these laws and regulations are explicitly mentioned in this CSR policy.

Position statements

Fox-IT's position on a number of topics that are most relevant in the public debate on cyber security will be explained in this document.

Dual-use goods and technologies

Fox-IT produces some so-called dual-use goods and technologies. Dual-use goods and technologies are defined as potentially having both civilian and military applications. Trade in these goods is governed by the Wassenaar arrangement, the European dual-use directive and other laws and regulations. Fox-IT adheres to these rules and regulations and is a proponent of further measures in order to reduce the risk of abuse of these technologies.

Offense and defense

Fox-IT always uses its expertise "for a more secure society." In today's world, society is (generally) forced into the role of (digital) defender; so Fox-IT aims to hinder attackers as much as possible. We name a few consequences of this general principle below.

For the purposes of this section, "offensive technologies and techniques" include zero-day exploits, but also e.g. post-exploitation frameworks and techniques to evade defenders.

- We proudly help our customers defend their systems, both with defensive techniques such as our Managed Detection and Response service and with offensive services such as penetration testing and red teaming. Simulating an attack on our customers requires offensive tools and techniques, but actually hinders adversaries and helps society, by pointing out weaknesses and by helping the defenders experience realistic attacks.
- We aim to publicly disclose any vulnerabilities found during our own research or while doing work for customers, per NCC group's disclosure policy (see https://www.nccgroup.trust/uk/our-research/disclosure-policy/). We believe that publishing vulnerabilities is a key part of getting vendors to improve their products, and of giving defenders the means to upgrade to a fixed version or at least to deploy workarounds/mitigations. The same principle applies to (other) offensive technologies and techniques.

  However, we aim to publish such information in a way that helps defenders more than it helps attackers:
  - We always strive to help defenders by including mitigations and workarounds.
  - We are also wary of publishing offensive technologies in such a way that they are easy to use by less-skilled attackers – since allowing less-skilled attackers to succeed tends to result in many more successful attacks.
  - Fox-IT will not sell, nor publish for free, any toolkit that allows an attacker of any skill level to execute a successful attack (a "hack-in-a-box.").
  - This is a spectrum, and borderline cases are unavoidably subjective.

Entities that have a legal authority to carry out offensive activities against third parties (for example law enforcement, defense departments, intelligence agencies) are among Fox-IT's customers. If such

entities request offensive technologies or services, the board will always request advice from the Ethics Committee and will only approve this on a case-by-case basis.

Part of the public debate on information security focuses on zero day exploits, a form of offensive technology. Fox-IT has never carried out research into unknown vulnerabilities at the request of a law enforcement agency or intelligence service. If such a request is made, the Ethics Committee of Fox-IT will advise. Requests by individual employees not to be involved in such a case will be respected. For more information on zero days, see https://www.fox-it.com/en/about-fox-it/corporate/news/zero-days-secure-society/. When Fox-IT decides to assist intelligence and investigation services this will always be for ethical reasons, i.e. to contribute to a safer society, and never for motives of company profit.

Detecting government operations

With our services in the area of detection and response, our goal is always to provide our clients with facts about (potential) compromises to the confidentiality, integrity or availability of their information or processes. We will pursue this, regardless of whether the source of the compromise is internal or external, criminal or state-affiliated, friend or foe. In other words: we will always provide the facts to our clients, even if that means potentially impacting an operation of a friendly government.

Backdoors

Fox-IT never builds backdoors or undocumented means of access into its products.

Customers

Before *each* new contract, or new deliverable under an existing contract, the Fox-IT employee who is responsible for that delivery/contract must ensure that we follow the procedure below.
"DO", "CHECK", and "DON'T" are explained below.

- Is the *end* customer a government, or an entity under substantial formal or informal government control? Then look up the country's current status in Freedom House's most recent "Freedom in the World" report, and consult the table below.

	Free	Partly Free	Not Free
Intelligence services, secret police, and special forces	CHECK	CHECK	DON'T
Police, (other) armed forces, and other parts of the security apparatus	DO	CHECK	DON'T
Other government or quasi-governmental entity	DO	DO	CHECK

- Otherwise, if there is a reasonable risk of the *end* customer using *this* delivery/contract
  - for (assisting in) mass surveillance, *or*
  - for selling exploits or malware, *or*
  - for (assisting in) violating human or civil rights*, including* cases in which the end customer will be coerced into doing so (e.g. several "Not Free" countries have laws that grossly violate the human/civil rights of minorities and/or criminals),

  then CHECK. Otherwise, DO.

Possible outcomes are:

DO	*If* you believe there is a reasonable risk of the *end* customer using this delivery/contract for one of the goals mentioned above, for any reason, proceed as under "CHECK". *If* you think there is a significant risk of negative publicity, proceed as under "CHECK". *Otherwise*, proceed with Sales and delivery.
CHECK	You *must* ask the Ethics Committee for advice. Afterwards, you or the Ethics Committee *may* go to the board, for a final decision; otherwise, you *must* follow the Ethics Committee's advice.
DON'T	*If* Fox-IT has a prior commitment to this customer, or if you think the world would be better off if Fox-IT helped this customer, proceed as under "CHECK". *Otherwise*, DON'T. (Hint: you should generally focus your efforts on other customers.)

The Ethics Committee

The board has delegated to the Ethics Committee some decisions regarding the application of the CSR policy to deliveries and contracts. The Ethics Committee's advice is binding for all Foxers, but the board can overrule it.

In determining its advice, the Ethics Committee weighs:
- all considerations in the previous section,
- the extent to which the product or service, if used maliciously, can cause harm to human and civil rights (notably privacy),

- the intentions and track record of the customer,
- the customer's justifiable reliance on Fox, if any (in particular, refusing to provide routine maintenance or replacements for previously-delivered products is hardly ever acceptable),
- any other factor the Ethics Committee considers relevant to creating a better world,
- whether there is a significant risk of negative publicity ("Can we justify this in a Tweet?")

The Ethics Committee does *not* consider commercial aspects.

To be more predictable and efficient, the Ethics Committee may make and/or revise, on its own initiative, policies to handle particular classes of questions. These policies are never "self-serve": Foxers *must* ask the Ethics Committee for advice unless the previous section ends in "DO".

The Ethics Committee will provide the board with at least a yearly update regarding changes in the "Freedom in the World" map.

Finally, the Ethics Committee may provide unsolicited advice to the board, either on its own initiative or after receiving reports (ie questions or remarks) from Foxers. Such reports are not anonymous.

Members of the Ethics Committee

The Ethics Committee consists of three employees. The Ethics Committee should collectively have at least:

- legal expertise, and
- technical expertise, and
- affinity with the work of each part of the company, and
- affinity with the impact of technology on human and civil rights.

Members serve until they step down or leave the company. When a member steps down, a new member is proposed by all current members (including by the person leaving), and confirmed by the board if suitable. Potential conflicts of interests will be taken into account.

The board

The board is responsible for Fox-IT's Corporate Social Responsibility policy, as well as for enforcing compliance.
The board commits itself to upholding this policy, and to considering the advice from the Ethics Committee in all relevant decisions.

Foxers

Individual Foxers are expected and encouraged to report (potential) violations of this policy to their line manager and/or directly to the Ethics Committee.