



FOX IT
part of nccgroup

CLASSIFICATION
FOX.PUBLIC

MVO-beleid Fox-IT

Datum	1 October 2019
Versie	2.0

**FOR A
MORE
SECURE
SOCIETY**

Maatschappelijk Verantwoord Ondernemen bij Fox-IT¹

For a more secure society

Technologie is volledig verweven met het dagelijks leven van individuele burgers en de samenleving als geheel, en kan worden ingezet met zowel goede als slechte bedoelingen. Producten en diensten die een onschuldige indruk maken, zoals netwerksensoren of forensische expertise, kunnen ook gebruikt worden voor slechte doeleinden.

Fox-IT neemt zijn ethische verantwoordelijkheid uiterst serieus en gaat daarin verder dan de huidige wet- en regelgeving. Daarom hebben wij dit beleidsdocument voor Maatschappelijk Verantwoord Ondernemen (MVO) opgesteld, en de bijbehorende regels en procedures geformuleerd onder het kopje 'Klanten'. Ons doel is om het risico dat onze producten en diensten worden misbruikt om mensenrechten en/of burgerrechten te schenden tot een absoluut minimum te beperken.

Bij Fox-IT dragen we met onze technologische kennis bij aan het publieke debat. We richten ons echter vooral op onze kernexpertise: technische kennis over cyberveiligheid.

Om te beginnen:

Omdat technologie onze kernactiviteit is, gaat dit MVO-beleidsdocument vooral daarover. Maar bijdragen aan een betere wereld kan op veel meer manieren.

- Fox-IT respecteert de mensenrechten die zijn beschreven in de Universele Verklaring van de Rechten van de Mens en de burgerrechten waar Freedom House zich voor inzet.
- Fox-IT verwacht hetzelfde van zijn opdrachtgevers. Daarom denken we goed na over welke diensten en producten we aanbieden en aan welke opdrachtgevers we die aanbieden. Exportregels vormen de basis, maar we maken ook andere afwegingen. (Zie 'Klanten'.)
- Fox-IT koopt niemand om en laat zich niet omkopen.
- Foxers zijn het allerbelangrijkste asset van Fox-IT, dus we zorgen voor goede werkomstandigheden en we voldoen altijd minimaal aan alle arbeidswet- en regelgeving.
- Wij geven om het milieu. Bij het ontwikkelen van nieuwe diensten en producten houdt Fox-IT rekening met eventuele invloed op het milieu. Bovendien moedigen we Foxers aan om zelf concrete stappen te nemen, zodat onze interne processen het behoud van onze planeet niet in de weg staan.
- Voor alle duidelijkheid: Fox-IT houdt zich aan alle wetten en regelgeving die van toepassing zijn, of die nu expliciet genoemd worden in dit MVO-beleidsdocument of niet.

¹ Deze Nederlandse versie is een vertaling. Mochten er verschillen bestaan, dan is de Engelse versie van dit beleid leidend.

Standpunten

In dit document leggen we uit hoe we bij Fox-IT denken over een aantal belangrijke kwesties die een rol spelen in het publieke debat over cyberveiligheid.

Dual-use producten en diensten

Fox-IT ontwikkelt ook dual-use-technologie. Dat zijn producten en diensten die potentieel geschikt zijn voor zowel militaire als algemene toepassingen. Handel in dergelijke technologie is aan banden gelegd door middel van het Wassenaar Arrangement, het Europese dual-use-besluit, en in een aantal andere wetten en regels. Fox-IT houdt zich aan alle regelgeving en is een voorstander van verdere maatregelen om misbruik van dit soort technologie zo veel mogelijk te voorkomen.

Aanval en verdediging

Fox-IT gebruikt zijn expertise “for a more secure society”. Tegenwoordig worden we als samenleving vaak in de rol van (digitale) verdediger geduwd. Om die reden probeert Fox-IT aanvallen zo veel mogelijk te bemoeilijken. Wat dat in de praktijk betekent beschrijven we hierna.

Onder ‘aanvallende technologie en techniek’ verstaan wij niet alleen zero-day-exploits, maar bijvoorbeeld ook post-exploitation tools en methodes om cyberbeveiliging mee te omzeilen.

- Wij zijn trots op het feit dat wij onze klanten helpen bij het beschermen van hun informatie en systemen, met onze defensieve Managed Detection & Response-dienst en met offensieve diensten zoals penetratietesten en red teaming. Bij gesimuleerde aanvallen maken we ook gebruik van technologie om door de beveiliging heen te breken, maar dit helpt de maatschappij juist en maakt het lastiger voor kwaadwillenden. Dit is omdat eventuele kwetsbaarheden dan tijdig aan het licht worden gebracht en omdat opdrachtgevers dan zelf ervaren hoe een aanval in zijn werk gaat.
- Kwetsbaarheden die we tijdens eigen onderzoek of tijdens werk voor klanten tegenkomen, maken wij zoveel mogelijk openbaar, volgens het transparantiebeleid van NCC Group. (Zie <https://www.nccgroup.trust/uk/our-research/disclosure-policy/>). Wij geloven dat openheid over eventuele kwetsbaarheden een belangrijke rol speelt bij het zorgen dat ontwikkelaars hun producten verbeteren; bovendien krijgen gebruikers zo de kans om een upgrade te installeren of de mogelijkheden en/of gevolgen van een aanval in ieder geval te beperken. Dit principe geldt ook voor (andere) aanvallende technologieën en instrumenten.

We streven ernaar om gevoelige informatie zo te presenteren dat verdedigers er meer aan hebben dan aanvallers:

- We ondersteunen verdedigers met workarounds en manieren om de effecten van een aanval af te zwakken.
- We letten op met het verpakken van aanvalstechnieken op een manier die voor een aanvalster met minimale kennis bruikbaar is. Want hoe meer mensen een cyberaanval kunnen uitvoeren, hoe meer pogingen én successen er zullen zijn.
- Wanneer een bepaalde toolkit het te gemakkelijk maakt om een cyberaanval uit te voeren (een “hack-in-a-box”), zal Fox-IT die niet verkopen of beschikbaar stellen.
- Dit blijft een spectrum, en over grensgevallen valt helaas altijd te discussiëren.

Onder Fox-IT's opdrachtgevers zijn ook partijen die wettelijk gerechtigd zijn om aanvallen op derden uit te voeren (de politie, het leger en nationale inlichtingendiensten bijvoorbeeld). Als die opdrachtgevers vragen om producten of diensten die cyberaanvallen mogelijk maken, zal de directie van Fox-IT de ethische commissie van te voren om advies vragen, en slechts per geval toestemming verlenen.

Een belangrijk onderwerp in het publieke debat over cyberveiligheid zijn zero-day-exploits. Fox-IT heeft nog nooit onderzoek gedaan naar onbekende kwetsbaarheden op verzoek van de politie of een inlichtingendienst. Mochten wij een dergelijk verzoek krijgen, dan zal de ethische commissie zich daar eerst over buigen. Een verzoek van individuele medewerkers om niet bij zo'n opdracht betrokken te zijn, worden altijd gerespecteerd. Voor meer informatie over zero days zie <https://www.fox-it.com/nl/over-fox-it/corporate-nieuws/news/zero-days-for-a-more-secure-society/>. Indien Fox-IT besluit om mee te werken aan een dergelijk verzoek zal dit altijd om ethische redenen zijn, om bij te dragen aan een veiligere samenleving, en nooit om financieel-zakelijke redenen.

Detection and response van overheidsoperaties

Wat *detection and response* betreft is onze dienstverlening erop gericht om opdrachtgevers de feiten te geven over (mogelijke) problemen met de vertrouwelijkheid, integriteit of beschikbaarheid van hun informatie of processen. Dat doel zullen we altijd nastreven, of de oorzaak van die problemen nu binnen de organisatie ligt of daarbuiten, bij criminelen of statelijke actoren, bij vriend of vijand. Met andere woorden: we leveren de informatie altijd, ook als dat misschien invloed heeft op de activiteiten van een bevriende natie.

Achterdeur

Fox-IT voorziet zijn producten nooit van achterdeurtjes of andere niet-gedocumenteerde manieren binnen te komen.

Klanten

Voor elke nieuwe opdracht, of nieuw op te leveren product of dienst binnen een bestaande overeenkomst, dient de Fox-IT medewerker die hiervoor verantwoordelijk is de hieronder beschreven procedure te volgen. "DO", "CHECK" en "DON'T" worden verderop uitgewerkt.

- Is de eindopdrachtgever een overheid of een organisatie onder substantiële formele of informele invloed van een overheid? Zoek in dat geval op wat de status van dat land is in het meest recente 'Freedom in the World'-rapport van het Freedom House en werk volgens de tabel hieronder.

	Vrij	Deels vrij	Niet vrij
Inlichtingendiensten, geheime politie, en speciale eenheden	CHECK	CHECK	DON'T
Politie, (andere) gewapende eenheden, andere onderdelen van defensie	DO	CHECK	DON'T
Andere (quasi-)overheidsinstanties	DO	DO	CHECK

- Is er een aanmerkelijk risico dat de eindgebruiker *deze* opdracht of *dit* opgeleverde product zal gebruiken voor:
 - (ondersteuning bij) massa-surveillance, *of*
 - de verkoop van exploits en/of malware, *of*
 - (ondersteuning bij) schendingen van mensenrechten en/of burgerrechten, inclusief situaties waarin de eindgebruiker tot dat soort schendingen wordt gedwongen (landen die als 'Not Free' zijn beoordeeld, hebben vaak wetten die de rechten van minderheden en/of criminelen met voeten treden.)
 Zorg eerst voor een CHECK, anders DO.

De procedure gaat als volgt:

DO	Is er een aanmerkelijk risico dat de eindgebruiker dit product/deze opdracht voor één van de hierboven genoemde doelen zal gebruiken, om welke reden dan ook? Ga dan verder bij CHECK. Is er een aanmerkelijk risico op negatieve publiciteit? Ga dan verder bij CHECK. In alle andere gevallen: ga verder met verkoop en oplevering.
CHECK	Je <i>moet</i> de ethische commissie om advies vragen. Jij of de ethische commissie kan een definitieve beslissing vragen aan de directie van Fox-IT; in alle andere gevallen ben je verplicht het advies van de ethische commissie te volgen.
DON'T	Heeft Fox-IT een bestaande (morele) verplichting jegens deze klant, of denk je dat de wereld er beter van wordt als Fox-IT deze klant van dienst is? Ga dan verder bij CHECK. In alle andere gevallen: DON'T. (Tip: waarschijnlijk kun je je energie beter aan andere opdrachtgevers besteden.)

De ethische commissie

De directie van Fox-IT heeft beslissingen over de uitvoering van het MVO-beleid op het gebied van producten en overeenkomsten van opdracht deels overgedragen aan de ethische commissie. Het advies van de ethische commissie is bindend voor alle Foxers, maar de directie van Fox-IT kan alsnog een ander besluit nemen.

Bij adviezen weegt de ethische commissie het volgende af:

- alles wat hierboven beschreven staat;

- de mate waarin een product of dienst schadelijk kan zijn voor mensenrechten en/of burgerrechten (met name privacy) bij misbruik;
- de intenties en voorgeschiedenis van de opdrachtgever;
- de mate waarin de opdrachtgever (terecht) afhankelijk is van Fox-IT (het is vrijwel nooit te verantwoorden om te weigeren routinematig onderhoud of vervanging van eerder geleverde te leveren);
- alle andere factoren die de ethische commissie belangrijk acht voor een betere wereld;
- de kans op negatieve publiciteit ('Is dit in een tweet uit te leggen?')

De ethische commissie houdt geen rekening met commerciële belangen.

Om efficiënter te kunnen werken, mag de ethische commissie op eigen initiatief beleid maken of aanpassen om een bepaald type vragen te kunnen beantwoorden. Dit wordt echter nooit een vorm van zelfbediening. Foxers zijn in alle gevallen verplicht om langs de ethische commissie te gaan als de standaardprocedure niet leidt tot DO.

De ethische commissie zal de directie minstens een keer per jaar voorzien van een update n.a.v. de actuele kaart van 'Freedom in the World'.

Ten slotte kan de ethische commissie de directie van Fox-IT voorzien van ongevraagd advies, op eigen initiatief of op basis van rapporten (met vragen en opmerkingen) van Foxers. Die rapporten zijn niet anoniem.

Leden van de ethische commissie

De ethische commissie bestaat uit drie medewerkers. Als collectief heeft de ethische commissie in ieder geval het volgende in huis:

- juridische expertise, en
- technische expertise, en
- affiniteit met het werk van de verschillende bedrijfsonderdelen, en
- affiniteit met de invloed van technologie op mensenrechten en burgerrechten.

Leden van de ethische commissie blijven aan tot ze hun lidmaatschap opzeggen óf uit dienst gaan bij Fox-IT. Wanneer een lid uit de commissie vertrekt, wordt een nieuw lid door de overige leden (inclusief degene die vertrekt) voorgedragen en – indien geschikt – door de directie van Fox-IT benoemd. Hierbij wordt rekening gehouden met eventuele belangenverstrengeling.

De directie

De directie is verantwoordelijk voor het MVO-beleid van Fox-IT, inclusief voor het zorg dragen dat het uitgevoerd wordt.

De directie verplicht zich om het MVO-beleid na te leven, en om het advies van de ethische commissie in overweging te nemen bij alle relevante beslissingen.

Foxers

Van Foxers wordt verwacht dat zij eventuele (mogelijke) overtredingen melden bij hun leidinggevende en/of rechtstreeks bij de ethische commissie.