SMART4SOLUTIONS
ETHISCHE CODE

VERSIE 1.5 – 07 JANUARI 2021
[141]

smart4 solutions it's in our nature •

INHOUDSOPGAVE

1 INLEIDING

In deze Ethische code lees je wat de kern is van waaruit SMART4Solutions en haar medewerkers werken. Dit tezamen met de Gedragscode. Deze ethische code geldt ook voor (medewerkers van) externe partijen, die voor of namens SMART4Solutions werkzaamheden verrichten.
Indien je bij een opdrachtgever van SMART4Solutions werkt; geldt logischerwijs ook dat je het beveiligingsbeleid van de opdrachtgever dient te volgen.

2 BINDEND STUK

Na het doorlezen onderteken je deze code voor akkoord; daarmee verklaar je de ethische code en betekenis daarvan voor je werk te kennen en toe te passen. Afwijkingen van deze afspraken dienen als incident[1] geregistreerd of gemeld te worden aan de Security Officer.

Voor interne medewerkers van SMART4Solutions geldt dat jaarlijks de naleving van deze code alsmede je handelen t.o.v. het informatiebeveiligingsbeleid zal worden besproken in je beoordelingsgesprek.

Voor medewerkers van externe partijen die voor of namens SMART4Solutions werkzaamheden verrichten geldt dat de naleving van deze code alsmede je handelen t.o.v. het informatiebeveiligingsbeleid wordt besproken wanneer daar – om welke reden dan ook – aanleiding voor wordt gezien door de Security Officer of directie van SMART4Solutions.

3 ALGEMENE OMGANGSVORMEN EN NORMEN SMART4SOLUTIONS

Als medewerker of contractant van SMART4Solutions;

1. Zal ik nooit het belang van de vertrouwelijkheid voor onze opdrachtgevers uit het oog verliezen, zodra ik daaraan twijfel maak ik er melding van;
2. Behandel ik iedere opdrachtgever, collega en externe relatie met aandacht en respect;
3. Signaleer ik (bijna) fouten en stel ik mijzelf en SMART4Solutions in staat om hiervan te leren door deze te melden en zo bespreekbaar te maken;
4. Ben ik toegankelijk en aanspreekbaar;
5. Neem ik een onderzoekende houding aan en ben ik zelf beschouwend;
6. Ga ik collegiaal, veiligheidsbewust en oplossingsgericht te werk;
7. Kom ik afspraken na (die ik maak) en stel deze zelf aan de orde als dit onverhoopt niet lukt;
8. Weet ik wat in onze samenleving en in het bijzonder de organisaties van de opdrachtgever en SMART4Solutions, grensoverschrijdend (gedrag) is, handel ik daarnaar en ben daarop aanspreekbaar;
9. Mag ik rekenen op een faire behandeling door SMART4Solutions;

[1] *Dit wordt je – als interne medewerkers van SMART4Solutions - uitgelegd bij de awareness training inzake het informatiebeveiligingsbeleid.*

10 Begrijp en onderschrijf ik het belang van informatiebeveiliging, integer handelen en respect voor de privacyaspecten voor SMART4Solutions en opdrachtgevers en handel daarnaar;

4 MELDEN VAN AFWIJKINGEN, (BIJNA-)OVERTREDINGEN EN INCIDENTEN

Iedereen die een geval van fraude, misleiding of onrechtmatig gedrag ontdekt of vermoedt, is verplicht dit onmiddellijk te melden. Overtredingen of incidenten meld je direct bij de Security Officer van SMART4Solutions. De Security Officer zorgt voor de vastlegging, afwikkeling en evaluatie.

Ingeval van incidenten en calamiteiten is de directie verantwoordelijk voor de communicatie met externe partijen, overheid en toezichthouders.

5 MELDEN VAN VERZOEKEN TOT WERKEN IN EEN PRODUCTIEOMGEVING

Het beleid van SMART4Solutions is dat we geen (technische) handelingen verrichten in de productieomgeving van onze opdrachtgevers. Hierop kan een uitzondering worden gemaakt, mits we daartoe als SMART4Solutions een vrijwaringsbewijs hebben.

Je mag nimmer op eigen initiatief (technische) handelingen uitvoeren in een productieomgeving van een opdrachtgever.

Wanneer een opdrachtgever je verzoekt om (technische) handelingen te verrichten in een productieomgeving dan:

- Meld je dit bij de SO en controleer je samen met de SO of hiertoe een vrijwaring bestaat en daarbij ook specifiek voor jou benoemd.
- Bij het ontbreken daarvan meld je de opdrachtgever dat je niet gemachtigd bent om deze handelingen te verrichten en verwijs je de opdrachtgever naar de directie van SMART4Solutions.

6 DOCUMENT EN GEGEVENSBEHEER VIA CLASSIFICATIE VAN GEGEVENS (DATACLASSIFICATIE)

Sommige gegevens zijn vertrouwelijker of gevoeliger dan andere en vereisen daarom andere beschermingsmaatregelen.

We onderkennen de volgende categorie met de eisen binnen SMART4Solutions:

De classificatie van informatie levert dan de volgende classificatieniveaus op:

Type 1	
Classificatie	(Intern) vertrouwelijke gegevens.
Niveau/impact	Ongewenste toegang of verlies heeft kortdurende maar significante impact op operationele of tactische doelstellingen.
Omvat	Naar personen en/of organisaties herleidbare gegevens. Dit o.a. ook omvattend (niet limitatief): interne bedrijfsvoeringgegevens en (tussen)producten design van applicaties.
Hoe te verwerken	Zorgvuldig met de juiste informatiebeveiligingsdoelstellingen in lijn met integriteit, vertrouwelijkheid en beschikbaarheid.
Door wie	Medewerkers na ondertekening geheimhoudingsverklaring en ethische code.
Opslag en transport van de data	Alleen met passende bedrijfsmiddelen (niet via eigen apps en mail).
Principe logische beveiliging	Volgens het eigen informatiebeveiligingsbeleid.

Bron: document "060 – Document en gegevensbeheer klasses"

Documenten worden door ons altijd als categorie I intern vertrouwelijk beschouwd tenzij anders aangegeven (labelen, naamgeving document).

7 WIJZINGEN OPMERKEN, BESPREKEN EN VASTLEGGEN (CHANGEMANAGEMENT)

Als je wijzigingen (moet en) gaat aanbrengen in systemen of applicaties met gegevens van een opdrachtgever, ga je na of er mogelijk informatiebeveiligings- of privacyaspecten aan vast zitten. Vastlegging en afstemming met de Security Officer is dan verplicht.

8 VEILIG GEBRUIK VAN BEDRIJFSMIDDELEN

- Gebruik van door SMART4Solutions verstrekte bedrijfsmiddelen voor privégebruik staan we niet voor; maar verbieden we niet. Het is immers risico verhogend toch?
- Gebruik alleen toegestane tools[2] om klantdata in te verwerken.
- Geen USB-sticks of andere verwijderbare media (SD-cards, etc.) voor opslag en transport van kritische informatie (tenzij in overleg met- en middel goedgekeurd door Security Officer).
- Beveiliging van laptop, tablet of smartphone waar mail of andere gegevens van SMART4Solutions op kunnen staan dient middels een wachtwoord, vingerafdruk of pincode te zijn ingesteld. Dit is verplicht en zal worden gecontroleerd.
- Op je laptop staan makkelijk intern vertrouwelijke gegevens van SMART4Solutions. Wees je daarvan dan bewust en behandel deze ook zo. Ofwel; je mag deze ook NIET uitlenen, kinderen of je partner mogen deze NIET gebruiken en je sluit de apparaten zoveel mogelijk af en bergt ze zorgvuldig op.
- Essentieel is dat je GEEN intern vertrouwelijke gegevens op jouw device hebt staan. We werken met elkaar alleen in de cloud waar je de gegevens opslaat in G-Suite.
- Voorkom malware en virussen: installeer geen onnodige niet werk gerelateerde software op de machines: check altijd met de Security Officer als je iets nieuws wilt installeren. Ter voorkoming van malware en virussen installeer je daartoe voorgeschreven tools (Windows Bitlocker en Defender). Mocht je dit niet duidelijk zijn of tot vragen leiden bij je; contact dan de Security Officer.
- Behandel de spullen van SMART4Solutions – indien verstrekt - als een goed huisvader/-moeder en meldt diefstal en vermissing direct aan de Security Officer.
- Schoon zoveel mogelijk tijdelijke bestanden en directory's op, alsmede de directory van je downloads.
- Sluit je laptop altijd helemaal af als je klaar ben met werken en je gaat verplaatsen (niet in de slaapstand maar echt uit).
- Je neemt een laptop/tablet altijd mee naar huis en bergt deze op een veilige plek op. Je mag je laptop/tablet nooit achterlaten op je zakelijke werkplek anders dan dat je deze veilig kunt opbergen in een daartoe bestemde veilige/beveiligde ruimte op kantoor (van de opdrachtgever).

[2] *Op dit moment verwerkt SMART4Solutions nog geen klantdata. Wanneer dit – in de toekomst - wel geschiedt dien je bij de Security Officer op te vragen welke tools (alsdan) je dan mag/kan gebruiken. Eigen keuzen zijn NIET toegestaan.*

9 GEBRUIK VAN E-MAIL EN INTERNET

- Internet en SMART4Solutions email voor niet-zakelijk verkeer is beperkt toegestaan, voor zover dit niet storend is voor de goede voortgang en kwantiteit van de dagelijkse werkzaamheden, dit ter beoordeling aan de directie.
- Bezoek geen websites waar mogelijk discriminerende, seksuele of criminele inhoud te vinden is.

10 MOBIELE APPARATUUR EN WERKEN OP AFSTAND (TELEWERKEN)

Voorzichtigheid is geboden bij het gebruik van mobiele apparatuur in openbare ruimten, vergaderruimten en andere onbeschermde locaties. Je gebruikt daarbij altijd geheime authenticatie-informatie. Je kunt je ook buiten kantooromgeving toegang verschaffen tot voornoemde omgeving en de applicaties die wij gebruiken. Zij bevinden zich immers op het internet.

11 UITINGEN OP SOCIAL MEDIA

Social media is niet meer weg te denken in onze huidige maatschappij. Zo zul jij mogelijk ook één of meerdere sociale apps gebruiken, waaronder één of meerdere voor privé gebruik.

SMART4Solutions heeft kernwaarden zijnde:

1.5 KERNWAARDEN

Het DNA van onze organisatie omvat de volgende kernwaarden welke de handelingen en het gedrag van onze medewerkers bepalen:

Toegewijd	We doen wat we beloven.
Ambitieus	We houden van resultaatgericht aanpakken.
Leergierig	We verlangen naar groei in kennis en kunde.
Nuchter	We zijn 'down to earth'.
Lef	We durven scherp te blijven naar onszelf en onze omgeving.
Fun	Een plezierige samenwerking leidt tot succes.

Het is te betitelen als een belofte van professioneel gedrag naar onszelf, collega's en opdrachtgevers.

Hou daar rekening mee als je privé uitingen doet via social media. Ofwel je weet wat maatschappelijk en binnen onze organisatie als verantwoord gedrag wordt gezien/geaccepteerd en je laat zien dat je je daaraan houdt. Je bent ook immers altijd ook een collega binnen SMART4Solutions.

12 GEBRUIK VAN SOFTWARE

- We respecteren intellectuele eigendomsrechten en gebruiken geen illegale software of andere middelen zonder toestemming van de eigenaar.
- Ingeval van twijfel over de rechten of legaliteit van software: overleg met de Security Officer.

13 TOEGANGSBEVEILIGING MIDDELEN (LAPTOPS, TELEFOONS, USB-STICKS E.D.)

- Gebruik van usb sticks, cloudopslag of andere middelen voor zover niet in eigendom of verstrekt door SMART4Solutions is niet toegestaan.
- Mocht gebruik van deze middelen gewenst zijn voor de uitvoering van je werkzaamheden dan in overleg met/na goedkeuring door de Security Officer (deze registreert het middel en zorgt voor veilige opslag en de verwijdering van (gegevens op) het middel).

14 WACHTWOORDEN (GEBRUIK VEILIGE)

- Omtrent het gebruik van wachtwoorden is door SMART4Solutions een wachtwoordbeleid uitgewerkt. De directie gaat ervan uit dat je deze tot je genomen hebt en je je er aan conformeert. Met ondertekening van deze ethische code ga je ook akkoord met het wachtwoordbeleid.

15 TOEGANGSBEHEER (KANTOORTOEGANG)

- Sommige medewerkers ontvangen een persoonlijke sleutel die strikt persoonlijke toegang verschaft (voorkom indringers, begeleidt meelopende bezoekers naar de gastheer of -vrouw).
- Toegang is alleen toegestaan tijdens kantooruren of daarbuiten indien noodzakelijk voor werkzaamheden.
- Meldt verlies of diefstal van de sleutel direct bij de Security Officer én Directie.
- Je maakt geen kopieën van de sleutel.
- Je levert de sleutel – per omgaande - in bij uitdiensttreding of zoveel eerder als je daartoe een verzoek van de directie en/of Security Officer krijgt.
- Als sleutelhouder van je verantwoordelijk voor alle schade die ontstaat of ontstaan is door misbruik van de sleutel.

16 TOEGANG VOOR BEZOEKERS VAN SMART4SOLUTIONS

- Bezoekers worden altijd ontvangen en naar de uitgang begeleid door de gastheer of -vrouw (jij of jouw collega die de bezoeker ontvangt).
- Bezoekers worden niet achtergelaten in ruimtes waar gegevens toegankelijk zijn (open kasten, niet afgesloten computers of verwijderbare media).

17 VEILIGE WERKPLEK (CLEAN DESK EN CLEAR SCREEN)

- Bij het verlaten van de werkplek wordt de computer gelocked (clear screen) of geschiedt dit automatisch binnen enkele minuten.
- Aan het einde van de werkdag worden gegevensdragers (papier en digitaal) opgeborgen (clean desk). Papier wat je niet meer gebruikt wordt door je verscheurd en weggegooid in de daarvoor bestemde prullenbakken.

18 PRIVACY RESPECTEREN

Dit gaat over het al dan niet werken met persoonsgegevens:

- We delen geen informatie over of van SMART4Solutions en haar opdrachtgevers met derden.
- We verwerken geen persoonlijke (gezondheids-) gegevens zonder reden of opdracht (door de opdrachtgever of directie).
- Bij het testen worden nooit gegevens van bestaande mensen gebruikt (tenzij geanonimiseerd). Wanneer we met testdata van opdrachtgevers werken en bemerken dat de testdata bestaande mensen betreft, melden we dit. Het is aan de opdrachtgever om hiernaar te handelen.
- We bespreken in openbare ruimtes[3] geen opdrachtgevers of personen (ook niet in een telefoongesprek) .
- We printen geen documenten met vertrouwelijke gegevens tenzij absoluut noodzakelijk.

19 VEILIGHEID EN REGISTRATIE DOOR SMART4SOLUTIONS

- Zoveel- én daar waar mogelijk loggen we toegang tot kritische systemen voor beveiligingsdoeleinden. Om aan te kunnen tonen wie wanneer welke toegang heeft gehad. Dit doen we alleen ter controle en ondertekenaar kan op verzoek inzage krijgen in de loggingbestanden.

[3] *Ruimten die niet werkplek gebonden zijn.*

20 DISCIPLINAIRE GEVOLGEN (BIJ NIET NALEVING VAN REGELS)

- Afwijkingen en incidenten geef je zo snel mogelijk door aan securityofficer@smart4solutions.nl. Het afwijken van bovenstaande afspraken kan tot sancties leiden. Dit ter beoordeling aan de directie.

21 GOOGLE DRIVE EN FILESTREAM

- Alle documenten worden opgeslagen in de Cloud omgeving van SMART4Solutions: Google Drive.
- Het is niet toegestaan om lokale kopieën te maken van deze Google Drive bestanden.
- Bij gebruik van Google Filestream dient deze altijd op ONLINE modus te staan.
- Indien bestanden toch OFFLINE beschikbaar moeten zijn, om welke reden dan ook, dan dient hier toestemming voor worden gevraag bij de Securityofficer.

22 ONDERTEKENING VOOR AKKOORD

"Ik heb de ethische code gelezen en begrijp de impact op mijn werkzaamheden.
Ik neem deze regels in acht bij de uitvoering van mijn werkzaamheden.

Het wachtwoordbeleid heb ik ook gelezen en
neem ik in acht bij de uitvoering van mijn werkzaamheden.

In gevallen waarin ik deze ethische code niet kan naleven, of twijfel over naleving,
maak ik daarvan melding aan mijn leidinggevende, directie of de Security Officer.

Ik geef de directie en/of Security Officer toestemming om te controleren
of ik de spelregels in deze documenten op de juiste wijze in acht neem.
Ik heb daartoe ook de checklist "144 – Checklist device" tot mij genomen."

Aldus opgemaakt te …… , op …… - …….. - …….

Naam: ……

Functie: ……

Handtekening:

……

VERSIEBEHEER

Eigenaar		Luciano Currie		
Vertrouwelijkheid		I - Intern vertrouwelijk		
Geldig tot (volgende review)		31 December 2021		
Versie	Status	Aangepast	d.d.	Door
0.1	Concept versie	NVT	20 november 2018	WS
1.0	Definitieve versie	Bespreking intern	15 december 2018	WS
1.01	Definitieve versie	Toevoeging checklist device	27 december 2018	WS/RvL
1.02	Definitieve versie	N.a.v. opmerkingen SM	8 januari 2019	WS
1.1	Definitieve versie	N.a.v. overleg directie	9 januari 2019	WS
1.2	Definitieve versie	N.a.v. input vanuit de externe audit	14 februari 2019	WS
1.3	Definitieve versie	Meldingsplicht technische handelingen in een productieomgeving opgenomen	11 juli 2019	WS
1.4	Definitieve versie	Hoofdstuk toegevoegd “Google Drive en Filestream”	24 december 2019	RvL
1.5	Definitieve versie	Review zonder verdere aanpassingen	07 januari 2021	LC