STRUKTON ICT-GEDRAGSPROTOCOL
betreffende het gebruik van ICT-middelen en -voorzieningen

Algemeen

Strukton stelt haar medewerkers ICT-middelen en –voorzieningen zoals computers met software daarop, internettoegang en e-mail ter beschikking voor het uitoefenen van de functie. Om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en de informatievoorziening te beschermen, is er een informatiebeveiligingsbeleid vastgesteld binnen Strukton. Beleid en technische maatregelen alleen zijn niet voldoende om de goede werking van de ICT-middelen en -voorzieningen te waarborgen. Ongewenst gebruik kan grote hinder en schade opleveren. Het Strukton ICT-gedragsprotocol voorziet in een aantal richtlijnen en geboden voor verantwoord gebruik van de ICT-middelen door de medewerker.

De essentie van het Strukton ICT-gedragsprotocol is als volgt samen te vatten:

a. **Zakelijk gebruik.** De beschikbaar gestelde ICT-middelen zijn primair bedoeld voor zakelijk gebruik. Beperkt privégebruik is toegestaan voor zover dit niet indruist tegen de gestelde regels, niet storend is voor de overeengekomen werkzaamheden en geen extra kosten voor Strukton tot gevolg heeft.
b. **Vertrouwelijkheid.** Medewerkers moeten zich er van bewust zijn dat men met vertrouwelijke bedrijfsgegevens te maken heeft. Het gebruik van ICT-middelen mag eventuele vertrouwelijkheid of gevoeligheid van gegevens niet schenden of strijdig zijn met wettelijke of contractuele beperkingen.
c. **Privacy.** Op zowel het gebruik als controle op het gebruik van ICT middelen is het Strukton Privacyreglement van toepassing.
d. **Overlast voorkomen.** Het gebruik van internet en e-mail is aan bepaalde regels en beperkingen gebonden. Hierbij gelden ook de gangbare omgangsvormen bij communicatie.
e. **Zorgvuldigheid.** De medewerker dient zorgvuldig om te gaan met de beschikbaar gestelde ICT-middelen en zich te houden aan de gestelde regels.

Voor het gebruik van social media (blogs, wiki’s of sociale netwerken als bijvoorbeeld LinkedIn, YouTube, Flickr, Twitter, Facebook etc.) door Struktonmedewerkers zijn een aantal richtlijnen opgenomen in dit gedragsprotocol. De volledige en meest recente versie van deze richtlijnen is te verkrijgen via Corporate Communications en op de intranetten van de verschillende werkmaatschappijen.

Het ICT-gedragsprotocol is niet vrijblijvend. De directie zal bij overtreding van dit gedragsprotocol tot sancties overgaan en passende arbeidsrechtelijke maatregelen nemen.

Artikel 1 Definities

Medewerker	Iedere persoon die voor of bij Strukton werkzaam is, op basis van arbeidsovereenkomst, overeenkomst van opdracht, inleen of anderszins.
ICT-middelen	De door of namens Strukton ter beschikking gestelde hardware, software en netwerkfaciliteiten, evenals de door of namens Strukton aangeboden voorzieningen t.b.v. elektronisch data- en spraakverkeer. Waaronder: desktop- en laptopcomputers, en de daarop geplaatste programmatuur, internettoegang, e-mail, maar ook printer, scanner, fax, PDA (elektronische agenda), (mobiele) telefoon en smartdevice.
Strukton	Strukton Groep nv of aan haar gelieerde ondernemingen, dochterondernemingen en combinaties of samenwerkingsverbanden daarvan met andere ondernemingen.
Beheerder	De ICT-verantwoordelijke van het bedrijfsonderdeel en/of de hiervoor aangewezen medewerkers.
Derden	Onder derden wordt verstaan iedereen die geen medewerker is van Strukton.
Beveiligings-incident	Een incident waarbij de reputatie van Strukton op het spel zou kunnen staan of de bedrijfsvoering buitenproportioneel kan worden verstoord, met het risico dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(middelen) worden aangetast of attractieve waardegoederen worden ontvreemd.
Internet-gebruik	Het uitwisselen of doorgeven van gegevens en/of berichten via E-mail, het bezoeken van internetsites, het binnenhalen (downloaden) van gegevens alsmede het binnenhalen van software en/of het gebruiken van software vanaf internet.
Smartdevice	Een draadloos apparaat, niet zijnde een PC, dat zich kenmerkt door computer functionaliteit. waarop applicaties beschikbaar zijn, waarmee via internet of wifi Strukton informatiesystemen kunnen worden benaderd. Hieronder vallen een daarvoor geschikte mobiele telefoon, Smartphone of Tablet.

Artikel 2 Privacy en controle

2.1 Gegevens die tot één persoon, of tot een beperkte groep personen herleidbaar zijn zullen niet worden geregistreerd, verzameld, gecontroleerd, gecombineerd dan wel bewerkt worden, anders dan in dit protocol is afgesproken.

2.2 Persoonlijke gegevens zullen alleen gebruikt worden voor het doel waarvoor ze verzameld zijn.

2.3 Het registreren van gegevens die tot één persoon of een zeer beperkte groep personen herleidbaar zijn wordt tot het minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van werknemers op de werkplek, zoals vastgesteld in het Privacyreglement van Strukton.

2.4 De inhoud van e-mail is in beginsel persoonlijk van aard. Alleen de medewerker kan anderen machtigen tot toegang tot de inhoud van zijn/haar e-mailverkeer. Voor het verlenen van support is het in bepaalde situaties echter nodig dat de medewerker toegang verleent tot zijn of haar mailbox aan een IT-medewerker van de support-organisatie. In zulke gevallen zal de medewerker deze toegang verlenen.

2.5 Het gebruik van applicaties, e-mail- en internet wordt op permanente basis centraal gemonitord en gelogd. Deze monitoring heeft in eerste aanleg een technische oorsprong om de werking van de systemen te kunnen beoordelen. Periodiek wordt hierover aan de betrokken werkmaatschappij gerapporteerd. Deze rapportage geschiedt op een niet tot personen herleidbare wijze.

2.6 Indien de rapportage daartoe aanleiding geeft kan op verzoek van de directie van een werkmaatschappij nadere informatie worden verstrekt. Het openen van e-mail en op persoonsniveau controleren van internetgebruik zal uitsluitend plaatsvinden bij duidelijk vermoeden van onrechtmatig gedrag. De beslissing hierover ligt bij de directie van de betrokken werkmaatschappij.

2.7 Binnen de beperkingen die door de wet en het Strukton Privacyreglement daaraan worden gesteld, zal Strukton de naleving van het protocol controleren
De bij controle betrokken functionarissen zullen de privacy van de betrokken medewerkers zoveel als redelijkerwijs verwacht mag worden respecteren en controles uitvoeren op een wijze waarop de privacy van betrokken medewerker(s) maximaal gewaarborgd is.

Artikel 3 Geldigheid Gedragsprotocol

3.1 Deze regeling, het Strukton ICT-gedragsprotocol, is van kracht voor alle medewerkers van Strukton. De directie van elke Strukton werkmaatschappij is verantwoordelijk voor de naleving van het gedragsprotocol.

3.2 Iedere medewerker dient zich te houden aan de in deze regeling vervatte en daaruit voortvloeiende instructies, geboden en verboden.

Artikel 4 Gebruik van de ICT-middelen

4.1 Het gebruik van de ICT-middelen door de medewerker is primair ten behoeve van het vervullen van zijn taak of functie. Voor zover dit niet indruist tegen de gestelde regels, niet storend is voor de overeengekomen werkzaamheden en geen extra kosten voor Strukton tot gevolg heeft, is beperkt privé gebruik toegestaan.

4.2 Strukton behoudt de bevoegdheid een medewerker de mogelijkheid tot het gebruik van ter beschikking gestelde ICT-middelen te ontzeggen.

4.3 Installatie van software op ICT-middelen geschiedt uitsluitend door de Beheerder. Uitzondering hierop is alleen toegestaan indien hiervoor uitdrukkelijk toestemming is verleend door de beheerder.

4.4 Het installeren van software zonder een geldige licentie is verboden.

4.5 Mede met het oog op beheer van licenties en de ondersteuning van de gebruikers kan de Beheerder controles uitvoeren ten aanzien van geïnstalleerde software, alsmede ter zake instructies geven. E.e.a. met inachtneming van het Strukton Privacyreglement.

4.6 Op alle Struktoncomputers en op het netwerk van Strukton aangesloten computers, dient een door Strukton goedgekeurd antivirusprogramma actief te zijn.

4.7 Met uitzondering van niet draagbare hardware geldt dat hardware nimmer onbeheerd achtergelaten dient te worden. In voertuigen mag hardware uitsluitend uit het zicht in een afgesloten kofferbak worden achtergelaten.

4.8 In geval van schade, vermissing of diefstal van ICT-middelen dient de Beheerder onverwijld op de hoogte worden gesteld. Waar mogelijk en relevant, zoals bij inbraak, dient bij de politie aangifte te worden gedaan en van het betreffende proces-verbaal een afschrift aan de Beheerder te worden overgelegd.

4.9 Reparaties aan en opening van apparatuur mag uitsluitend door de Beheerder geschieden.

4.10 Computers zijn door de Beheerder ingesteld om na 10 minuten inactiviteit in de schermvergrendelmodus te gaan. Bij het verlaten van de werkplek dient de medewerker handmatig de schermvergrendelmodus te activeren (toetsen combinatie ⊞-toets+L).

4.11 Afhankelijk van de locatie van een werkplek (kantoor, trein, etc), gaat mobiel computergebruik gepaard met andere risico's, waarvoor medewerkers bijbehorende beveiligingsmaatregelen dienen te treffen. Te denken valt aan het gebruik van kabelsloten of opbergen in af te sluiten kasten.

4.12 De medewerker is verantwoordelijk voor de back-up van lokaal opgeslagen data op de C- of D-schijf (periodieke back-up van centrale data is de verantwoordelijkheid van ICT). Het gebruik van de C- en D-schijf voor data opslag wordt overigens ontraden.

Artikel 5 Internet

5.1 Medewerkers zijn in beginsel uitsluitend gerechtigd internet voor zakelijke doeleinden, samenhangend met de werkzaamheden die de medewerker bij Strukton verricht, te gebruiken. Internetsites waarvan het vermoeden kan bestaan dat bezoek ervan mogelijk nadelige gevolgen voor de ICT-middelen tot gevolg kan hebben, mogen niet worden bezocht. Voor alle duidelijkheid, het is verboden internetsites te bezoeken die pornografisch en/of racistisch en/of ander kwetsend of aanstootgevend materiaal bevatten.

5.2 Strukton behoudt zich het recht voor internetsites voor gebruik te blokkeren. In dit geval zal een melding verschijnen dat de betreffende pagina is geblokkeerd. Indien de medewerker meent de pagina toch te moeten bekijken, kan de medewerker contact opnemen met zijn leidinggevende, die daartoe een verzoek zal indienen bij de Beheerder.

5.3 Strukton behoudt zich het recht voor de doorgifte van bepaalde typen bestanden te blokkeren, die de capaciteit van de internetverbinding onnodig kunnen belasten (mp3 - files, streaming media etc.) of schadelijk kunnen zijn voor het Struktonnetwerk (.exe-files, virussen, etc.).

5.4 Het downloaden van software vanaf internet en het gebruiken van software vanaf internet (SaaS) is slechts toegestaan met uitdrukkelijke toestemming van de Beheerder. Deze verboden zijn uitsluitend op de Beheerder niet van toepassing, mits deze doeltreffende maatregelen heeft getroffen om de continuïteit van de bedrijfsvoering te waarborgen.

5.5 Bij internetgebruik dient de medewerker zorg te dragen dat de rechten van derden (zoals auteursrechten, merkenrechten) niet worden geschonden.

5.6 Indien op een internetsite naam, bedrijfsgegevens en/of e-mailadres moeten worden achtergelaten om gegevens op te vragen of te verkrijgen, dan zal de medewerker dat uitsluitend doen als er een zakelijk te rechtvaardigen reden voor is. Ook zal de medewerker in dat geval aangeven dat die gegevens niet voor andere doeleinden mogen worden gebruikt. Bedrijfsgevoelige informatie zal nooit worden doorgegeven of op een internetsite worden achtergelaten.

Artikel 6 Intranet

6.1 Het intranet van werkmaatschappij van Strukton wordt als informatiemedium voor haar medewerkers gebruikt en als zakelijk communicatiemedium tussen Struktonbedrijven onderling. Wat in artikel 5 over internetgebruik is bepaald, geldt ook voor het gebruik van intranet.

Artikel 7 Richtlijnen voor gebruik social media [1]

7.1 Van Strukton medewerkers, die actief zijn op social media (blogs, wiki's of sociale netwerken als bijvoorbeeld LinkedIn, YouTube, Flickr, Twitter, Facebook etc.), wordt verwacht dat zij verstandig en zorgvuldig omgaan met deze media en geen vertrouwelijke of interne informatie plaatsen.

7.2 Bloggen over het werk(-en) bij Strukton gebeurt altijd eerlijk en transparant en met gebruik van de echte naam. Men dient aan te geven waar en in welke functie men werkzaam is en niet noodzakelijk spreekt namens Strukton.

7.3 Medewerkers dienen niet zelf te reageren op gesignaleerde negatieve berichten over Strukton, maar deze te melden bij het Hoofd Corporate Communications.

Artikel 8 E-mail

8.1 E-mail wordt in beginsel uitsluitend zakelijk gebruikt om het risico op imagoschade voor Strukton tot een minimum te beperken. Indien de gestelde beveiligingsklasse van gegevens *zeer vertrouwelijk* is wordt communicatie per telefoon of e-mail sterk ontraden.

8.2 Strukton behoudt zich het recht voor de doorgifte te blokkeren van berichten welke mogelijk virussen bevatten of gegevens waarvan de verspreiding of verzending onwenselijk is. In dit geval zal een melding verschijnen dat het betreffende bericht is onderschept. Indien de betreffende medewerker meent het bericht toch te moeten inzien, kan de medewerker contact opnemen met de Beheerder.

8.3 Het is iedere medewerker geboden dezelfde regels en beleefdheidsnormen in acht te nemen als gelden ten aanzien van telefonische en niet-elektronische communicatie.

8.4 Oproepen van derden om plaatjes, post, koopaanbiedingen, kettingbrieven of goedbedoelde (virus)waarschuwingen algemeen binnen Strukton te verspreiden dienen te worden genegeerd. Het is verboden dergelijke oproepen zelf te verspreiden.

8.5 In geval van viruswaarschuwingen moet (uitsluitend) de Beheerder worden geïnformeerd.

8.6 Het is verboden dreigende, seksueel intimiderende en/of racistische taal te gebruiken dan wel te verspreiden.

8.7 Alle e-mail zal een disclaimer bevatten volgens de door Strukton ter beschikking gestelde standaardtekst.

8.8 De door de medewerker te verzenden e-mail met bijlages zal een Strukton ingestelde maximale omvang hebben. Bij het adresseren van e-mail zal de medewerker het aantal geadresseerden zo veel mogelijk beperken.

8.9 Strukton zal voor de mailbox van de medewerker op de e-mailinfrastructuur een door Strukton te bepalen hoeveelheid schijfruimte ter beschikking stellen. De medewerker is zelf verantwoordelijk voor het regelmatig opschonen van zijn mailbox.

[1] Een uitgebreidere versie van de richtlijnen voor het gebruik van social media is te verkrijgen via Corporate Communications en op de intranetten van de verschillende werkmaatschappijen.

Artikel 9 Beveiligingsbeleid

9.1 Strukton beschikt over een formeel Informatiebeveiligingsbeleid. Relevante delen hiervan zijn opgenomen in dit ICT-gedragsprotocol. In de functieprofielen kunnen taken en verantwoordelijkheden van Struktonmedewerkers op het gebied van informatiebeveiliging worden opgenomen die daarmee een onderdeel van het arbeidscontract vormen. Indien nodig worden de voor de individuele medewerker specifiek geldende verplichtingen vermeld.

9.2 Op het gebruik van e-mail (zowel inkomend als uitgaand), intranet en internet zijn de geheimhoudingsverplichtingen voortvloeiend uit de arbeidsovereenkomst tussen de medewerker en Strukton van toepassing.

9.3 In het kader van het toegang verschaffen tot het Struktonnetwerk en applicaties (waaronder intranet) daarop, verkrijgt iedere gebruiker een gebruikersnaam en een wachtwoord. Instructies van de Beheerder met betrekking tot wachtwoorden en de eventuele wijziging daarvan dienen te worden opgevolgd.

9.4 De manager van de betreffende medewerker is verantwoordelijk voor het, in overeenstemming met het functieprofiel, bepalen van de juiste toegangsrechten en ziet erop toe dat eventuele functie- of taakwijzigingen van medewerkers direct tot uiting komen in hun toegangsrechten.

9.5 Medewerkers nemen goede beveiligingsgewoonten in acht bij het kiezen en gebruiken van hun wachtwoord(en), waardoor wachtwoorden moeilijk te raden zijn. Na gebruik loggen zij af. Zij veranderen het wachtwoord indien de vertrouwelijkheid van het wachtwoord wordt betwijfeld. Zij worden hierin ondersteund door de techniek. Medewerkers zijn in beginsel, tot het tegendeel blijkt, persoonlijk verantwoordelijk voor misbruik van hun account.

9.6 Alle medewerkers houden hun accountgegevens waaronder het wachtwoord en pincode geheim. Zij gebruiken hun persoonlijke account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Opgeslagen wachtwoorden en pincodes van medewerkers en derden zijn in geen geval leesbaar door anderen dan de betrokkene zelf. Het is verboden een wachtwoord mede te delen aan anderen dan de Beheerder.

9.7 Toegang tot het Struktonnetwerk is alleen toegestaan met computers, die zijn ingericht volgens Struktonstandaarden en -eisen of met uitdrukkelijke toestemming van de Beheerder.

9.8 Verouderde en niet meer gebruikte elektronische gegevensdragers zoals diskettes, tapes, USB-sticks, cd- en dvd-roms, moeten fysiek worden vernietigd.

9.9 Computerbestanden die worden ontvangen van derden worden eerst op aanwezigheid van virussen gecontroleerd.

9.10 Het is niet toegestaan om vertrouwelijke informatie buiten het Struktonnetwerk te verzenden of op te slaan. Onder vertrouwelijke informatie wordt verstaan alle informatie die als zodanig is aangeduid of informatie waarvan de medewerker weet of zou behoren te weten dat deze vertrouwelijk is.
Dit geldt voor e-mail (Hotmail, Gmail, etc.), het gebruik van diensten voor het verzenden van grote bestanden (Dropbox, WeTransfer, etc.) en andere diensten waarbij Strukton informatie buiten het Strukton netwerk wordt opgeslagen (Prezi, Google drive, etc).

9.11 Het is toegestaan om Strukton informatie in de vorm van e-mail op een Smartphone of Tablet (zakelijk of privé) op te slaan. Door Active Sync (push mail) te activeren, wordt informatie op het device opgeslagen.
Als er Strukton informatie (bijv. e-mail) op een Smartphone of Tablet staat, is het ICT gedragsprotocol van toepassing en moet op het device een minimale vorm van beveiliging worden toegepast, bestaande uit een wachtwoord. Dit wordt door het e-mail systeem afgedwongen.
Medewerkers die uit hoofde van hun functie met vertrouwelijke informatie te maken (kunnen) krijgen, is het expliciet **niet toegestaan** om informatie op een andere dan een Strukton device op te slaan. Deze groep mag alleen gebruikmaken van een Strukton device dat volledig door Strukton ICT wordt beheerd en waarop een hoger beveiligingsniveau wordt ingesteld. Het gebruik van een onbeheerd privé device is voor deze groep medewerkers uitgesloten.
Per werkmaatschappij is vastgesteld welke functies en medewerkers binnen deze groep vallen.

9.12 Computers die op een Struktonkantoor zijn aangesloten op het netwerk (via netwerkkabel of wifi) mogen niet gelijktijdig rechtstreeks met het internet zijn verbonden via een modem, PC-kaart of dongle voor mobiel dataverkeer of anderszins. Het gevaar bestaat dat hierdoor een onbeveiligde verbinding tussen het Struktonnetwerk en het internet wordt opgezet.

9.13 Als bij een incident de reputatie van Strukton op het spel staat, de bedrijfsvoering boven proportioneel wordt verstoord, de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(middelen) wordt aangetast of attractieve waardegoederen worden ontvreemd, betreft het een beveiligingsincident. Iedere medewerker van Strukton of ingehuurde derde is verantwoordelijk voor het signaleren van beveiligingsincidenten en meldt deze bij de daartoe bevoegde afdeling als regulier incident. Indien het een beveiligingsincident betreft over een persoon (zoals fraude of een overtreding van regels) wordt dit gemeld aan de direct leidinggevende die dit weer meldt aan de Stafgroep Informatiebeveiliging, waarbij de identiteit van de indiener wordt beschermd.

Artikel 10 Eigendom

10.1 Alle zakelijke gegevens en informatie, inclusief e-mailberichten, gegenereerd, gedragen of ontvangen door Strukton ICT-middelen, zijn eigendom van Strukton.

10.2 Ter beschikking gestelde ICT-middelen mogen zonder voorafgaande en schriftelijke toestemming van Strukton niet aan derden in gebruik worden gegeven. Evenmin mogen een of meer kopieën van programmatuur aan derden worden verstrekt.