Inleiding

Ambiq wil alles wat in haar vermogen ligt doen om de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatie- en communicatievoorziening te waarborgen.

In de meeste processen van informatieverwerking en –beheer vervullen medewerkers een cruciale rol. Medewerkers moeten daarom op een zorgvuldige en verantwoorde manier met ICT en met communicatiemiddelen omgaan. Immers, onzorgvuldige omgang met ICT- en communicatiemiddelen kan leiden tot grote risico's voor cliënten en kan ook reputatieschade voor Ambiq tot gevolg hebben. Vertrouwelijke informatie kan terechtkomen in onveilige omgevingen, kan worden misbruikt of mensen kunnen ongeautoriseerd toegang tot informatie krijgen. Daarnaast kan onzorgvuldige omgang met informatie- en communicatiemiddelen schade toebrengen aan het Ambiq netwerk; (en daarmee aan de continuïteit van de bedrijfsvoering) denk bijvoorbeeld aan virussen.

Deze gedragscode geldt voor alle ICT- en alle communicatiemiddelen waarover de medewerker kan beschikken.

De gedragscode heeft vooral tot doel dat de medewerker zich bewust is van de risico's die zijn verbonden aan het gebruik van ICT en (elektronische) communicatiemiddelen al dan niet in combinatie met vertrouwelijke informatie. De artikelen in deze gedragscode geven daarom een generieke omschrijving en bevatten geen limitatieve opsomming van (on)gewenste gedragingen. Medewerkers dienen die maatregelen te nemen die redelijkerwijs van hen verwacht mogen worden; er wordt een professioneel en integer handelen verwacht. Eventuele sancties richting medewerker behoren, zoals dat ook geldt voor andere situaties in de arbeidsverhouding, in juiste verhouding te staan tot de mate waarin niet aan deze verwachting is voldaan.

Bij twijfel over de reikwijdte of strekking van deze gedragscode of als er redenen zijn om af te wijken van deze gedragscode, dienen medewerkers te allen tijde voorafgaand aan het verrichten van de voorgenomen handelingen, goedkeuring te vragen aan MT van Ambiq.
Deze gedragscode omvat de volgende onderwerpen:

1. Gebruik en toegang Ambiq ICT-infrastructuur
    a. Toegang tot het Ambiq netwerk
    b. Gebruik van ICT-middelen
    c. Gebruik van informatie
2. Internet, e-mail en social media gebruik;

Het gebruik van mobiele communicatiemiddelen is in een afzonderlijk beleidsdocument vastgelegd.

Gedragscode

1. Definities

a. Informatie
   Alle gegevens, ongeacht de presentatievorm, waarover de medewerker de beschikking heeft en toegang tot heeft, inclusief gegevens die zijn afgeleid uit bewerking van eerdere gegevens.
b. Communicatiemiddelen
   Elk door Ambiq goedgekeurd en/of aan een medewerker(s) verstrekt ICT-middel ten behoeve van verzameling, vervaardiging, verwerking, transport of opslag van informatie, waaronder in ieder geval (mobiele) telefoon, computer, tablet, in- en externe netwerkfaciliteiten, analoge en digitale gegevensdragers. In geval van twijfel dienen medewerkers goedkeuring te vragen aan het managementteam van Ambiq.
c. Medewerker
   Een personeelslid, vrijwilliger of stagiaire van Ambiq dan wel een daarmee op basis van het verrichten van werkzaamheden gelijkgesteld (externe) persoon.
d. Ambiq netwerk:
   Het netwerk (bekabeld en Ambiq Wi-Fi) dat toegang geeft tot de informatiesystemen van Ambiq.
e. Ambiq Wi-Fi:

De zakelijke Ambiq Wi-Fi verbinding waarmee de Ambiq infrastructuur benaderd kan worden. Dit in tegenstelling tot cliënt- en/of gast netwerken

f. Cliënten- of gast netwerk(en):
Bekabelde of Wi-Fi netwerk die gebruikt kan worden door cliënten of gasten; dit netwerk staat los van het Ambiq netwerk.

g. Single Sign On:
De mogelijkheid om één keer in te loggen op het Ambiq netwerk en vervolgens applicaties kunnen starten zonder voor die applicaties een aparte gebruikersnaam en wachtwoord op te hoeven geven.

2. Gebruik en toegang tot de ICT-infrastructuur

a. Toegang tot het 'Ambiq netwerk'.
   i. Wachtwoorden zijn persoonsgebonden; het is nooit toegestaan om de gebruikersnaam en wachtwoord aan collega's of derden ter beschikking te stellen. De gebruiker is persoonlijk verantwoordelijk voor dat wat gedaan wordt onder zijn/haar gebruikersnaam.
   ii. Wijzigingen in toegang tot en rechten voor het Ambiq netwerk en applicaties, moeten door de leidinggevende van de medewerker worden aangevraagd (bijvoorbeeld bij in dienst, functie wisseling en uit dienst).
   iii. Externe medewerkers dit toegang moeten hebben tot het Ambiq netwerk, moeten een geheimhoudingsverklaring ondertekenen. Wanneer geheimhouding is geregeld in een (dienstverlenings)overeenkomst, hoeven externe medewerkers geen individuele geheimhoudings-verklaring te ondertekenen.
   iv. Beveiligingen mogen niet worden uitgeschakeld, gewijzigd of omzeild. Aanwezige procedures dienen te worden gevolgd en voorgeschreven beveiligingsmiddelen moeten worden gebruikt.
   v. Bij het verlaten van de werkplek vergrendelt de medewerker de werkplek; alleen na invoeren van het wachtwoord is de werkplek te ontgrendelen.
   vi. Het is niet toegestaan om gebruik te maken van het Ambiq netwerk met andere dan door Ambiq ter beschikking gestelde of goedgekeurde ICT-middelen.
   vii. Onbedoelde inbreuken op de ICT-beveiliging, van binnenuit of vanuit de buitenwereld dienen te worden gemeld bij systeembeheer en bij de coördinator Informatiebeveiliging.

b. Gebruik van ICT-middelen
   i. Medewerkers mogen door Ambiq ter beschikking gestelde communicatiemiddelen voor privédoeleinden gebruiken, mits dit gebeurt binnen redelijke grenzen, niet storend is voor de dagelijkse werkzaamheden en hierbij voldaan wordt aan de bepalingen van deze Gedragscode en eventuele nadere instructies van Ambiq. Medewerkers hebben een eigen verantwoordelijkheid om het privégebruik van door Ambiq ter beschikking gestelde communicatiemiddelen te beperken en/of te compenseren. Voor privé gemaakte kosten kunnen aan de medewerker doorbelast worden door middel van inhouding van het salaris.
   ii. Het downloaden en of verwijderen van software en applicaties (behoudens zogenaamde app's op mobiele devices) is niet toegestaan zonder toestemming van ICT. Installeren van software en applicaties op het Ambiq netwerk en/of op Ambiq ICT-middelen mag alleen door, of in opdracht van ICT worden uitgevoerd.
   iii. Door Ambiq verstrekte ICT-middelen worden nooit onbeheerd achtergelaten in bijvoorbeeld de auto, onbewaakte garderobes, etc.
   iv. Schade, te wijten aan schuld of nalatigheid van de medewerker, zal maximaal 1x worden vergoed door de werkgever (MITS de "bijgeleverde bescherming" structureel wordt toegepast). Alle schades nadien zullen op de werknemer worden verhaald middels een verrekening met de eerstvolgende salarisbetaling;
   v. Indien een door Ambiq verstrekt ICT-middel wordt gestolen of vermist, zal de medewerker dit direct melden bij de leidinggevende en bij de servicedesk en binnen 24 uur aangifte doen bij de politie. Een vervangend ICT-middel wordt

pas verstrekt nadat aangifte is gedaan en de leidinggevende van de medewerker toestemming geeft voor vervanging. Indien nodig kan er wel een tijdelijke oplossing worden verstrekt, indien werkzaamheden/functie van de medewerker dit noodzakelijk maken.

vi. Iedere medewerker heeft de beschikking over een beperkte hoeveelheid centrale persoonlijke (niet zijnde privé) dataopslag, die gebruikt kan worden voor het opslaan van tijdelijke, persoonlijke en concept bestanden. Formele Ambiq informatie mag niet op deze persoonlijke dataopslag worden opgeslagen, maar dient altijd in de daarvoor bestemde applicaties of op centrale (team) site te worden opgeslagen.

vii. Medewerkers voorkomen activiteiten waarbij (opzettelijk) een groot beslag wordt gelegd op door Ambiq beschikbaar gestelde ICT-middelen/ ICT-infrastructuur.

viii. Het is voor medewerkers niet toegestaan zelf wijzigingen aan te brengen in de ICT-infrastructuur, zoals het verplaatsen van thin clients/PC's, vaste telefoons, maken van aanpassingen in bekabeling, wijzigingen aanbrengen op laptops etc.

c. Gebruik van informatie
   i. Medewerkers gaan zorgvuldig om met vertrouwelijke informatie.
   ii. De medewerker is verantwoordelijk voor (vertrouwelijke) informatie op papier of die op de door de medewerker gebruikte ICT-middelen en/of opslagmedia staan. De medewerker neemt passende maatregelen om te voorkomen dat een onbevoegde toegang krijgt tot de informatie. Bij verlies of diefstal van ICT-middelen meldt de medewerker dit direct bij de leidinggevende en bij de servicedesk.
   iii. Er worden alleen de hoogstnoodzakelijke afdrukken gemaakt. Afdrukken met daarop vertrouwelijke (cliënt) gegevens worden zo snel mogelijk, maar uiterlijk bij het eerstvolgende bezoek aan kantoor, op locatie vernietigd of in het dossier van de cliënt opgeborgen.
   iv. Ambiq gegevens, al dan niet vertrouwelijk, zowel schriftelijk als opgeslagen in digitale vorm, worden bewaard binnen de centrale ICT-infrastructuur van Ambiq of op door management van Ambiq goedgekeurde opslagmedia. Het gebruik van public cloud opslag toepassingen zoals dropbox, zijn niet toegestaan.

3. Internet en e-mail

a. Medewerkers maken gebruik van e-mail, internet, social media en andere vormen van openbare communicatie volgens de wet en normen van fatsoen. Medewerkers gaan zorgvuldig te werk en voorkomen dat Ambiq door het gedrag van de medewerker wordt beschadigd.
b. Gebruik van e-mail en internet is hoofdzakelijk werk gerelateerd. Het is toegestaan om voor beperkte persoonlijke doeleinden internet te gebruiken. De werknemer dient zich te houden aan de opgestelde regels en procedures. Websites welke binnen een van de ongewenste categorieën (zie d.i) vallen, maar toch werk gerelateerd zijn dienen afgestemd te worden.
c. Voor de e-mail van (bijzondere) persoonsgegevens naar personen buiten Ambiq dient gebruik te worden gemaakt van onze beveiligde e-mailoplossing.
d. Ambiq houdt zich het recht voor om toegang tot bepaalde sites te beperken. Met name websites met een pornografische, racistische of discriminerende of een op entertainment gerichte inhoud kunnen worden geweerd.
e. Ambiq kan het recht tot gebruik van (een deel van) internet toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (dat deel van) niet toegestaan.
f. Bij misbruik of ongeoorloofd gebruik van internet of communicatiemiddelen wordt de leidinggevende ingelicht. Deze onderzoekt de melding, waarbij ICT eventueel logboeken en/of data kan aanleveren. In geval van misbruik wordt het managementteam op de hoogte gesteld.
g. Cliënten die internet of andere communicatiemiddelen gebruiken worden door medewerkers begeleid. Bij start van de behandeling wordt dit punt besproken. Gedurende de hulpverlening komt dit punt regelmatig terug in gesprekken tussen cliënt

en groepsleiding. Cliënten krijgen nooit, ook niet onder begeleiding, toegang tot het Ambiq netwerk.

h. De gebruikelijke gedragsregels (zie handboek 6.06.03) , zoals de regels die momenteel gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van Ambiq en voor het verzenden van post, zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen, Twitter, Facebook etc.)
i. Het is niet toegestaan om de e-mail van Ambiq (permanent) door te sturen naar privé e-mailadressen.
j. Het is niet toegestaan om door middel van e-mail:
    i. Berichten anoniem of onder fictieve naam te versturen
    ii. Dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en ketting email te verzenden of door te sturen. Wordt dergelijk materiaal ontvangen, moet dit doorgegeven worden aan de servicedesk.
    iii. Iemand via e-mail of internet lastig te vallen.

Controle

1. Om de veiligheid van de infrastructuur te waarborgen en toe te zien op een zorgvuldig gebruik in overeenstemming met deze ICT-gedragscode, worden van tijd tot tijd controles uitgevoerd. Het toezicht op het gebruik zal bestaan uit het steekproefsgewijs controleren van het gebruik van de ICT-infrastructuur.
2. De controle die uitgevoerd wordt, wordt gedaan met de piramide methode, wat betekent dat pas op basis van duidelijke signalen de volgende stap wordt genomen voor wat betreft de controle. De controle wordt uitgevoerd door de medewerker ICT in opdracht van de manager ICT. Wanneer daar aanleiding toe is, wordt de direct leidinggevende geïnformeerd. Er is niet altijd controle mogelijk op het gebruik van de ICT; bijvoorbeeld het ‘surf gedrag’ van medewerkers of cliënten is niet te achterhalen.
3. De controle m.b.v. de piramide methode wordt in de volgende fases verdeeld:
    a. Controle op Ambiq breed gebruik van infra, voor zover deze data te achterhalen is (bijvoorbeeld grootte van de mail store, totale kosten van mobiele telefonie, totale kosten van data abonnementen, aantal defecten aan middelen)
    b. Onderzoek naar gebruik van de ICT-infrastructuur door specifieke gebruikers. Hiertoe wordt overgegaan op het moment dat het Ambiq brede gebruik van de ICT-infrastructuur opvallend afwijkt van het gemiddelde/de verwachting.
    c. Onderzoek naar details van het gebruik van één gebruiker, indien het gebruik van de medewerker daar aanleiding toe geeft (bijvoorbeeld inhoud van e-mail, gebelde telefoonnummers, momenten van data verbruik). Dit (en eventueel verder) onderzoek wordt pas ingesteld na overleg met en akkoord van de leidinggevende van de medewerker en de manager ICT.
    d. Indien mocht blijken dat in strijd met deze regeling wordt gehandeld of indien daarvoor aanwijzingen zijn (zoals klachten, signalen van binnen of buiten de organisatie en systeemstoringen), dan kunnen gegevens van (de) betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt.
    e. De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.

Sancties

Bij handelen in strijd met deze regeling, het bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van internet, kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen. Hierbij gaat het om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst.