IT-code

AG Digipolis Antwerpen

1. Inleiding

De goede werking van het AG Digipolis Antwerpen, hierna 'AG DigAnt', en haar partners is onlosmakelijk verbonden met de doeltreffende en veilige werking van IT en de manier waarop medewerkers omgaan met de aan hen beschikbaar gestelde IT-middelen.

Deze IT-code wil een houvast bieden voor alle gebruikers van AG DigAnt. De IT-code bepaalt de waarden, normen en gedragsregels die van toepassing zijn op de IT-middelen van het AG DigAnt.

2. Doelgroep en toepassingsgebied

Alle IT-middelen[1] beschikbaar gesteld door DigAnt of gekoppeld met de omgeving van DigAnt en haar partners, vallen binnen het toepassingsgebied van deze IT-code.

De doelgroep onderhevig aan deze IT-code zijn alle interne en externe medewerkers, stagiairs, interims, leveranciers en derde partijen van DigAnt, hierna 'gebruikers', welke gebruik maken van deze IT-middelen.

3. Definities en referenties

Dit hoofdstuk verklaart termen die gebruikt worden doorheen het document en somt termen en referenties op.

3.1. Definities

Term	Beschrijving
IT-middelen	PC's, laptops, servers, smartphones, randapparatuur, netwerk, internet, intranet, e-mail, software, gebruikersaccounts,...
Gebruikers	Interne en externe medewerkers, stagiairs, interims, leveranciers en derde partijen van AG DigAnt
Beheerders	Gebruikers met verhoogde of administratorrechten. Gebruikers met lokale beheerdersrechten op hun eigen PC of laptop worden in deze IT-code niet beschouwd als beheerder. (Meer info zie Terminologie)

[1] zie Definities en referenties

3.2. Referenties en terminologie

zie security - wikipagina

4. Regels voor gebruikers

In deze IT-code trachten we zo compleet mogelijk te zijn, maar deze IT-code kan onmogelijk alle handelingen vatten. Daarom verwacht AG DigAnt van gebruikers dat ze steeds hun verantwoordelijkheid nemen om integer te werken en daarbij de principes uit de A-waarden en de geldende regelgeving wat betreft intellectuele eigendom, auteursrechten en privacy-wetgeving, respecteren.

Onderstaande regels zijn van toepassing voor alle gebruikers zoals gedefinieerd in Definities en referenties

4.1. Veilig gebruik van IT-middelen

1. Veiligheid is een taak van iedere gebruiker. Beveilig zowel de toestellen, de toepassingen als de bijhorende data. Respecteer het informatieveiligheidsbeleid en gebruik IT-middelen met zorg. Gebruikers zijn aansprakelijk voor alle handelingen die worden uitgevoerd met hun persoonlijke gebruikersnaam. Deel daarom nooit jouw gebruikersnaam en bijbehorend wachtwoord of pincodes, tokens,… en voorkom onrechtmatig gebruik. Respecteer steeds het paswoordbeleid[2].
2. Vermijd dat collega's of bezoekers toegang krijgen tot persoonsgegevens of vertrouwelijke informatie van AG DigAnt of haar partners. Laat je IT-middelen daarom nooit onbeheerd achter en vergrendel ze steeds als je ze niet gebruikt. Vermijd dat afgedrukte documenten rondslingeren op het werk, bij remote werken of thuiswerken. (Voor meer info, zie de clean desk policy[3]).
3. Gebruik geen (illegale) software waarvan je niet zeker bent dat je over de juiste licenties beschikt of die de beveiliging en performantie van de IT-infrastructuur in gedrang kan brengen.
4. Gebruik jouw IT-middelen in een vertrouwde omgeving. Vermijd connectie met ongekende of onbeveiligde wifi-netwerken en gebruik enkel vertrouwde toestellen voor jouw activiteiten voor AG DigAnt.
5. Wees voorzichtig met internet en e-mail: denk twee keer na vooraleer je een link aanklikt of een bijlage opent. Let op waar je jouw gebruikersnaam, wachtwoord of andere vertrouwelijke informatie ingeeft of achterlaat.
6. Meld veiligheidsincidenten (bv. vermoeden van misbruik, verdachte e-mail, eigenaardig gedrag) en verlies of diefstal van IT-middelen onmiddellijk aan de helpdesk en informeer jouw leidinggevende. Pas de nodige discretie toe over gemelde incidenten en volg de meldingsprocedure voor een security-incident of datalek[4].

[2] zie Definities en referenties
[3] zie Definities en referenties
[4] zie Definities en referenties

7. Tenzij het tot jouw opdracht behoort en mits voorafgaande toestemming is het niet toegestaan de beveiliging van IT-middelen uit te testen of in opspraak te brengen.
8. Toegang tot data en applicaties wordt enkel gegeven voor geautoriseerde gebruikers via de geldende procedures. Toegang moet steeds kaderen binnen de professionele doeleinden, met respect voor de deontologische waarden en conform de relevante wetgeving.

9. Bescherm jouw IT-middelen tegen diefstal. Laat deze niet onbeheerd achter op vrij toegankelijke plaatsen of zichtbaar in jouw auto.

4.2. Goed beheer van IT-middelen

1. De door AG DigAnt beheerde IT-middelen worden voorzien van een standaardconfiguratie. Wijzingen aan hardware, besturingssysteem, configuratie en naamgeving verlopen via de helpdesk. Voor software die je zelf installeert, sta je in voor de licentie, het regelmatig updaten en de veiligheid.
2. IT-middelen niet in beheer van AG DigAnt, mogen enkel gekoppeld worden met het bedrijfsnetwerk[5] indien ze voldoende beveiligd zijn en na registratie via de helpdesk.
    a. IT-middelen die je gebruikt voor AG DigAnt of haar partners, beheer je steeds zoals een goede huisvader. Daarbij sta je in voor:
        i. de goede zorg, het onderhoud en het up to date houden van jouw toestel.
    b. Wanneer je jouw IT-middelen niet meer gebruikt voor AG DigAnt of haar partners, draag je minimaal de aan AG DigAnt gerelateerde informatie over en vervolgens verwijder je zelf op afdoende en aantoonbare wijze de gegevens op de persoonlijke opslaglocaties.
3. Voor IT-middelen in werkplek 2.0 behoudt AG DigAnt zich het recht om het privégebruik te beperken en/of de keuze voor werkplek 2.0 te ontzeggen en desgevallend de vergoeding terug te vorderen bij een ernstig vermoeden van misbruik, fraude of schending van de richtlijnen.

4.3. Gebruik van internet

1. Toegang tot internet is in de eerste plaats bestemd voor professionele doeleinden binnen je opdracht als medewerker van AG DigAnt. AG DigAnt laat echter occasioneel gebruik toe voor privé doeleinden, op voorwaarde dat dit gebruik redelijk is, in geen enkel opzicht de goede werking van AG DigAnt belemmert en geen inbreuk vormt op deze IT-code.
2. Het bezoeken van seksistische, pornografische, racistische of andere extreme sites is niet toegelaten.
3. Het is niet toegelaten gegevens te downloaden of te verspreiden die beschermd zijn door het recht op intellectuele eigendom, met schending van de toepasselijke wetten of van onbetrouwbare bronnen (zoals spelletjes, films, enz.). Het is niet toegelaten om gebruik te maken van websites die spelletjes/games of gokspelen aanbieden.
4. Het bekijken of beluisteren van streaming media mag geen negatieve invloed hebben op professionele activiteiten van de medewerker of de performantie van de IT-infrastructuur.
5. Regels rond het gebruik van sociale media (Twitter, Facebook, Instagram, internet fora e.d.) zijn bepaald in het standpunt van AG DigAnt rond sociale media[6].

[5] zie Definities en referenties
[6] zie Definities en referenties

4.4. Gebruik van e-mail

1. Het gebruik van e-mail is in de eerste plaats bestemd voor professionele doeleinden binnen je opdracht als medewerker van AG DigAnt. AG DigAnt laat echter occasioneel gebruik toe voor privé doeleinden, op voorwaarde dat dit gebruik redelijk is, in geen enkel opzicht de goede werking van AG DigAnt belemmert en geen inbreuk vormt op deze IT-code.
2. Het is aangeraden om "privé" te vermelden in het onderwerp van jouw privé e-mails en om privé e-mails te bewaren in een aparte map "privé" van jouw mailbox.
3. Het is niet toegestaan persoonlijke financiële verplichtingen aan te gaan vanuit jouw professionele mailbox of persoonlijke voorwerpen te koop aan te bieden.
4. Het is niet toegestaan deel te nemen aan kettingbrieven, spamming of discussiefora, tenzij voor professionele doeleinden.
5. Het is niet toegestaan e-mails te versturen waarbij je tracht jouw identiteit te verbergen of te vervalsen.
6. Het is niet toegestaan e-mails te versturen of te bewaren met onrechtmatige en/of ongepaste inhoud (bv. obsceen, beledigend, discriminerend, racistisch, politiek, pornografisch, seksistisch, enz.) tenzij verkregen in het kader van de behandeling van een dossier.
7. Als medewerker ben je aansprakelijk voor de inhoud van jouw e-mails. Vergewis je er dus steeds van dat je de toegang tot jouw e-mail afschermt.

4.5. Privégebruik van IT-middelen

Het occasioneel gebruik van de IT-middelen van AG DigAnt voor privé doeleinden is alleen mogelijk als het gebruik redelijk en niet storend is voor de operationele werking, de performantie en veiligheid van het netwerk en infrastructuur mogen niet in het gedrang komen.

Als je toch privébestanden bewaart op IT-materiaal van AG DigAnt, geef dit dan duidelijk aan door bijvoorbeeld een map 'privé' te voorzien. Bewaar geen privébestanden op de netwerkschijven van AG DigAnt.

5. Regels voor beheerders

Onderstaande regels zijn van toepassing voor beheerders zoals gedefinieerd in Definities en referenties.

5.1. Integriteit van beheerders

1. Beheerdersrechten worden enkel toegewezen aan geautoriseerde interne of externe medewerkers (zie onderstaand punt Passend toegangsbeheer voor meer informatie rond geautoriseerde medewerkers).
2. Vertrouwelijke of persoonsgegevens mogen niet geraadpleegd of verspreid worden indien dit niet noodzakelijk is in het kader van de taak. Beheerders moeten gepast omgaan met de informatie en kennis die ze opdoen.
3. Om de integriteit van de beheerders te bewaken kunnen activiteiten van beheerders gelogd worden.

4. Beheerders hebben een brede en diepe kennis van hun vakgebied en onderhouden hun kennis geregeld in de vorm van opleidingen, certificaten en andere.

5.2. Operationele activiteiten

1. Beheerderstaken mogen enkel uitgevoerd worden op basis van een specifieke, gedocumenteerde en geautoriseerde opdracht. Zorg ook bij hoogdringendheid steeds voor een melding en registratie.
2. Beheerders implementeren en volgen de regels op die van kracht zijn.
3. Interventies op afstand op het IT-materiaal van eindgebruikers moeten steeds worden aangekondigd en geregistreerd.
4. Bij het aanmaken, aanpassen of verwijderen van een account moet de beheerder rekening houden met geldende procedures, naamconventie en andere afspraken rond het beheren van accounts.
5. Beheerders kijken regelmatig de logging en monitoring activiteiten na om de operationele werking te garanderen.
6. Toegekende beheerdersrechten mogen enkel gebruikt worden voor taken die niet met gewone gebruikersrechten mogen worden uitgevoerd.

5.3. Beschermen van informatie

1. Beheerders respecteren de geldende wetgeving. Bij vermoeden van inbreuk op de wetgeving dient de beheerder deze direct te rapporteren aan de DPO.
2. Beheerders nemen technische en organisatorische maatregelen om de veiligheid van de informatie waarmee ze in aanraking komen, te waarborgen.
3. Veranderingen aan configuraties kunnen risico's met zich meebrengen. Beheerders moeten hier bewust mee omgaan en waar nodig documenteren.
4. Bij vermoeden van ongeautoriseerde handelingen op systemen of applicaties moet een beheerder dit onmiddellijk rapporteren aan zijn leidinggevende en de Security Officer informeren. In samenspraak met AG DigAnt moeten de nodige maatregelen getroffen worden om verdere impact te beperken en eventuele reeds geleden schade ongedaan te maken.

5.4. Passend toegangsbeheer

1. Beheerders kunnen enkel beheerdersrechten krijgen als ze deel uitmaken van de functiegroep die verantwoordelijk is voor het beheer en onderhoud van systemen, netwerk, databases en applicaties.
2. De beheerdersrechten worden beperkt tot de rechten noodzakelijk voor het uitvoeren van het toegewezen takenpakket. (least privilege-principe)
3. Beheerders mogen in geen beding gebruikerstaken uitvoeren onder service- of systeemaccounts.
4. Beheerders mogen de rechten van gewone gebruikersaccounts niet opwaarderen tot accounts met beheerdersrechten.

6. Individuele controle

6.1. Recht op controle

Binnen het wettelijk kader heeft AG DigAnt het recht om de werkmiddelen van gebruikers te controleren. Daarbij moet het recht op privacy en gegevensbescherming van de gebruikers gerespecteerd worden.

6.2. Voorwerp van controle

AG DigAnt kan controles doen van:

- devices
- het gebruik van e-mail;
- het gebruik van internet;
- het gebruik van andere professionele apps zoals bijvoorbeeld Slack, Yammer,...
- de informatie en bestanden die gebruikers publiceren op het intranet of internet;
- de informatie en bestanden die gebruikers raadplegen of opslaan op verschillende opslagmedia zoals bijvoorbeeld mappen op computers, servers, document management systemen,...

6.3. Doel van de controles

Controle door AG DigAnt is alleen mogelijk als een van de volgende vijf doelen wordt nagestreefd:

1. **het voorkomen en vaststellen van ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden.** Dat zijn feiten als:
    - het hacken van computers, waaronder het op illegale manier kennis nemen van persoonsgegevens of vertrouwelijke bestanden;
    - het raadplegen van sites die
        - zich tegen de grondbeginselen van de democratie en de rechtsstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;
        - anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
        - een gevaar voor verslaving vormen zoals goksites en pornografische sites;
        - de privacy en gegevensbescherming van iemand aantasten.
2. **het beschermen van bepaalde informatie.** Bepaalde informatie is niet geschikt om algemeen gedeeld te worden. Een controle door AG DigAnt is mogelijk ter bescherming van die informatie.
3. **het verzekeren van de veiligheid, de performantie of de goede technische werking van de IT-systemen** van AG DigAnt. Daar hoort de controle op de bijbehorende kosten en de fysieke bescherming van de IT-omgevingen (installaties) van AG DigAnt bij.
4. **het te goeder trouw naleven van deze IT-code;**
5. **het verzekeren van de bedrijfscontinuïteit** bijvoorbeeld bij overlijden, onvoorziene afwezigheid of vertrek van een werknemer.

6. Als een **wettelijke bepaling** het toestaat of oplegt, kan AG DigAnt de gegevens voor dit doel gebruiken, inkijken en herleiden tot de bepaalde gebruiker, bijvoorbeeld als AG DigAnt gevraagd wordt mee te werken bij een gerechtelijk onderzoek.

6.4. Soorten van controle

De manier waarop gecontroleerd wordt is afhankelijk van het doel van de controle. Er zijn drie soorten om te controleren, telkens meer ingrijpend dan de vorige:

1. permanente globale controle
2. occasionele globale controle
3. individuele controle

6.4.1. Permanente globale controle

Een permanente globale controle is het automatisch monitoren of bewaren van elektronische communicatiegegevens. Het gaat om niet-geïndividualiseerde gegevens die niet gelinkt worden aan een persoon.

6.4.2. Occasionele globale controle

Een occasionele globale controle is het verzamelen en de inzage door AG DigAnt van globale online communicatiegegevens die tijdens een beperkte periode werden gegenereerd en betrekking hebben op een groep van gebruikers.

Een occasionele globale controle is beperkt tot de tijd die nodig is om eventuele misbruiken te voorkomen of vast te stellen.

6.4.3. Individuele controle

Het voorwerp van de individuele controle van IT-middelen, de doelen en voorwaarden van deze soort van controle zijn in lijn met de aanbeveling van de Gegevensbeschermingsautoriteit. Vooraleer wordt overgegaan tot een individuele controle is er steeds een onderzoeksopdracht met goedkeuring vanuit de directie van AG DigAnt nodig.

Voorwerp van de controle

Bij een individuele controle, controleert AG DigAnt afhankelijk van de context:

- wie, welke websites heeft bezocht, wanneer en voor hoe lang;
- wie bepaalde communicaties heeft verzonden, de geadresseerden en het volume ervan. AG DigAnt kan ook de verzonden werkgerelateerde e-mails lezen. Persoonlijke e-mails of bestanden worden best in een aparte map “Privé” bewaard.

7. Naleving en sancties

Niet-naleving van deze IT-code kan in het geval van interne medewerkers aanleiding geven tot disciplinaire acties, in overeenstemming met in de rechtspositieregeling Deel 2 - Arbeidsreglement.

In het geval van externe medewerkers, interims, stagiairs of leveranciers kan de contractuele overeenkomst opgeschort of verbroken worden.

Mogelijke uitzonderingen op dit beleid zijn slechts toegelaten mits grondige motivatie en formele goedkeuring.

8. Aanvaarding

Voor de interne medewerkers is de IT-code als bijlage aan de arbeidsovereenkomst toegevoegd en door de ondertekening ervan verklaar je als gebruiker of beheerder dat:

1. ik mij bewust ben van van de opgenomen regels;
2. ik mij engageer tot het naleven van de regels;
3. ik mijn toestemming verleen aan AG DigAnt om gebeurlijke controles te verrichten voor de doeleinden zoals beschreven in deze IT-code en conform de privacywetgeving.

Voor alle andere externe partijen is de ondertekening van deze IT-code vereist en verklaar ik als gebruiker en/of beheerder dat:

1. ik mij bewust ben van van de opgenomen regels;
2. ik mij engageer tot het naleven van de regels;
3. ik mijn toestemming verleen aan AG DigAnt om gebeurlijke controles te verrichten voor de doeleinden zoals beschreven in deze IT-code en conform de privacywetgeving.

Naam en voornaam:	
ad-account:	
Organisatie (indien niet Digipolis):	
Opdrachtnummer:	
Datum:	
Handtekening:	

Digitaal ondertekend terug te bezorgen aan :